

6. INTRODUCCION A MACHINE LEARNING

José J. Martínez P.

josejesusmp@gmail.com

Mayo 2023

6.1 Introducción

Machine Learning es un término que ya se venía utilizando desde el siglo pasado. Sin embargo, ahora se ha convertido en un término comodín que utiliza mucha gente sin conocer su significado real y dependiendo del ambiente y de la formación de la gente le dan diferentes significados, debido a su utilización. Aunque, su florecimiento no es muy viejo, solo se logró hasta 2005, cuando G. Hinton, publicó un artículo en el que mostraba cómo al entrenar una red neuronal profunda, se podían reconocer dígitos escritos a mano, con una precisión del 98%. Como se ha mencionado, la historia de las redes neuronales ha sido una historia de amores y desamores y a finales de los 90s se había abandonado su investigación en estas redes. Con este artículo se demostró que con Deep Learning era posible lograr cosas que ninguna otra técnica de ML había hecho. El entusiasmo se extendió a muchas otras áreas de aplicación y digamos que estamos viviendo el auge de ML, que va a perdurar bastante.

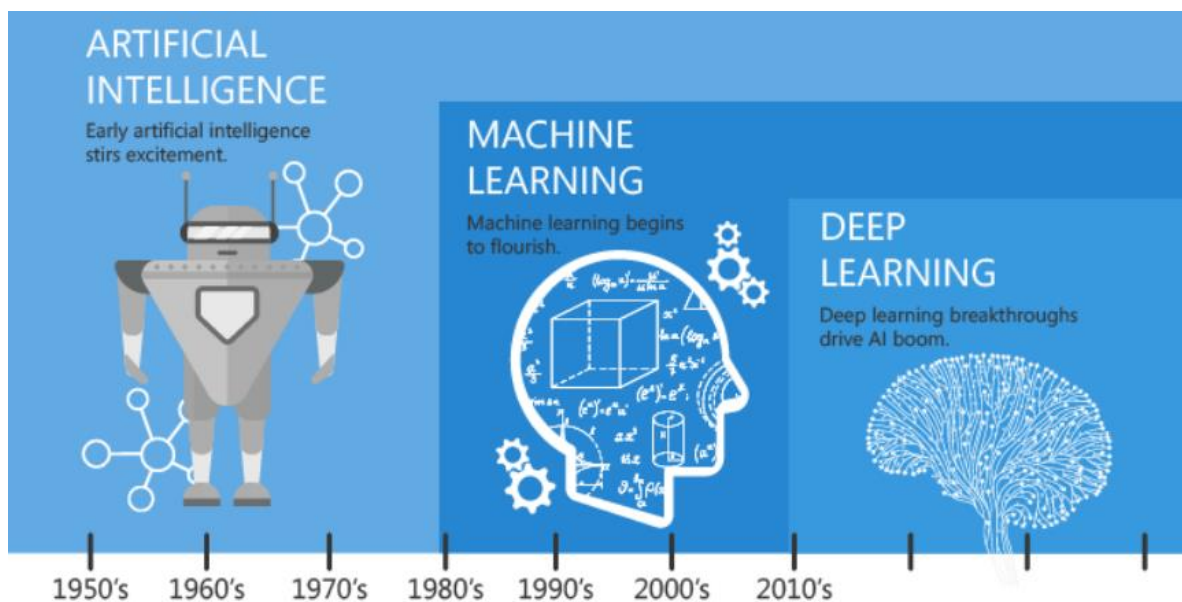


Figura 6.1. Una línea de tiempo de Inteligencia Artificial, Machine Learning y Deep Learning.

La gráfica de la figura 6.1, refleja en el tiempo los desarrollos que marcan la situación actual de la IA. Desde los 80s se comenzó a trabajar en ML, especialmente enfocado hacia el reconocimiento de objetos o patrones, con base en el concepto de atributos o parámetros (features), sin embargo, con Deep Learning de alguna manera se dispara su utilización, llevando al reconocimiento de los datos, como la fuente de conocimiento, pues en ellos está la información real, válida, de la interacción de humanos y máquinas con el ambiente. Una vez se logran integrar estos conceptos, se encuentra que hay otras técnicas básicas para enfrentar los mismos y otros problemas, especialmente K-NN Nearest, SVM (Support Vector Machine) y árboles de decisión.

Supongamos el siguiente problema: traducir un texto de un idioma a otro y solucionarlo con las técnicas actuales de programación. Para hacer un programa de computador que realice esta tarea, primero, hay que estudiar la gramática de ambos lenguajes, con el fin de codificar sus reglas; algo que no es tan simple. Luego incluir los diccionarios de ambos lenguajes, incluir también la codificación de las búsquedas y seleccionar las palabras más apropiadas en el lenguaje de destino; otra tarea de programación complicadas.

Pero hay más, ¿cómo trabajar con palabras homógrafas u homónimas? Por ejemplo, la palabra “can” en inglés, puede ser el verbo poder o puede ser simplemente una lata, en español. Todo depende del contexto. ¿Pero cómo codificamos apropiadamente ese contexto? Realmente la solución de este tipo de problemas, bajo ese concepto de programación es extremadamente difícil y por esto los traductores de lenguajes, antes de ML eran muy pobres.

Ahora las cosas han cambiado. Se encontró que la solución de muchos problemas complejos se encuentra en los datos. Usando una cantidad gigantesca de datos provenientes de diferentes fuentes en la web, Google tiene un modelo pre-entrenado que va mejorando sus resultados, de manera tan sorprendente, que en algunos casos superan el nivel de un traductor humano.

Ahora, se han desarrollado cientos de aplicaciones, que silenciosamente le dan poder a cientos de productos que usamos regularmente; desde mejores recomendaciones hasta búsquedas por voz. Es por esto que, nos pueden surgir algunas preguntas:

- ¿Qué es ML?
- ¿Dónde comienza y termina ML?
- ¿Qué significa exactamente, que una máquina aprenda algo?
- Si descargo una copia de Wikipedia ¿aprendió algo mi computador?
- ¿Se volvió inteligente repentinamente el computador?

6.2 ¿Qué es ML?

Veamos varias definiciones de ML:

- “ML es el campo de estudio que le da a los computadores la habilidad para aprender sin que sean explícitamente programados”. Arthur Samuel 1959.
- “ML es la ciencia o el arte de programar los computadores, de manera que puedan aprender a partir de los datos”.
- Una simple: “Sistemas que mejoran su comportamiento con respecto a una tarea con más y más experiencia o datos”
- “Se dice que un programa de computador aprende de la experiencia **E**, con respecto a alguna tarea **T**, con alguna medida de comportamiento **P**, si su comportamiento sobre **T**, medido por **P**, mejora con la experiencia”. Más orientada a la ingeniería. Tom Mitchel 1998.
- Otra forma de ver ML. En la gráfica 6.1, se puede observar, ML en comparación con la programación tradicional tomando como ejemplo encontrar la raíz cuadrada de un número.

En el caso de la programación tradicional podemos programar el método de Newton y hallar la solución. En el caso de ML, tendríamos muchos ejemplos con resultados correctos de la raíz cuadrada y a través de regresión podríamos encontrar la solución.

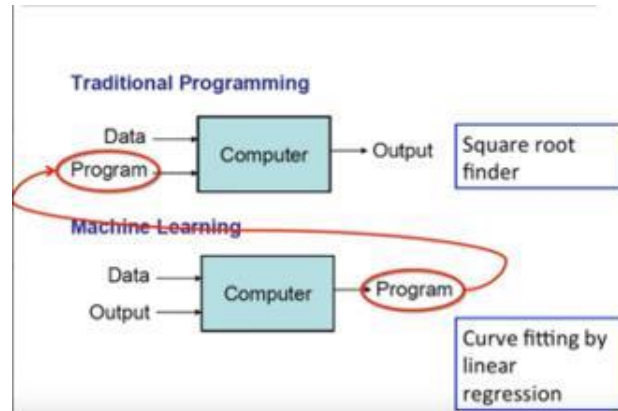


Figura 6.2. Programación tradicional versus ML.

Para tener una mayor claridad, vamos a trabajar alrededor de un ejemplo que es el filtro que tienen los sistemas de correo electrónico para detectar correos engañosos, que se conocen como filtros SPAM. El filtro spam que usa nuestro correo, es un programa de ML, que, con base en instancias de emails marcados como spam, observa qué mensajes del correo marca o no como spam; y con que, instancias de correos normales, aprende cómo filtrar mejor el spam. Esas instancias de emails que usa el sistema para aprender se llaman el conjunto de entrenamiento, o dataset.

Volviendo a la última definición de ML, la tarea T del filtro Spam es marcar los correos que llegan como spam, correo no deseado, cuando esos correos presentan ciertas características que el filtro Spam las tiene clasificadas como comunes a todos los correos spam. La experiencia E, es el conjunto, dataset, de correos buenos y malos que tiene el sistema y del cual aprende, que ha ido recabando el sistema de correo de la interacción permanente con sus usuarios en todo el mundo. Mientras que P, es la predicción que hace sobre un determinado correo de que es spam o no, también se conoce como el comportamiento del sistema, que depende de que tan bien hace la predicción y se le asigna una precisión que se usa mucho en problemas de clasificación. Para esto se usa la Matriz de Confusión, figura 6.3.

Matriz de Confusión		Predice	
		Positivo	Negativo
Real	Positivo	VP	FN
	Negativo	FP	VN

VP: Verdadero Positivo

FN: Falso Negativo

FP: Falso Positivo

VN: Verdadero Negativo

$$Precisión = \frac{VP + VN}{VP + VN + FP + FN}$$

Figura 6.3. Matriz de Confusión, permite encontrar la precisión de un sistema de clasificación por ML.

6.3 Porque el uso de ML

Volvamos a nuestro ejemplo del filtro Spam y digamos que vamos a escribir este programa, el filtro spam usando técnicas de programación tradicional. Siguiendo unos pasos básicos de Ingeniería de Software, primero debemos enterarnos cómo son los correos no deseados, cómo es la forma de los encabezados, del tema y del contenido. Aparecen palabras como “gratis”, “regalo”, “tarjeta de crédito”, etcétera.

De manera que con base en toda esta información encuentre estas palabras y algunos patrones que casi siempre se presentan en los correos spam. De manera que entro a programar para que cada una de estas palabras y patrones, permitan que mi programa detecte los correos no deseados.

Puede ser que mi filtro Spam funcione correctamente durante un determinado tiempo. Esto lo pueden advertir quienes producen los correos Spam y van a buscar otras palabras y otros patrones, para burlar mi filtro. Al hacerlo, mi filtro deja de funcionar un tiempo, hasta cuando me dé cuenta de que está dejando pasar correos spam.

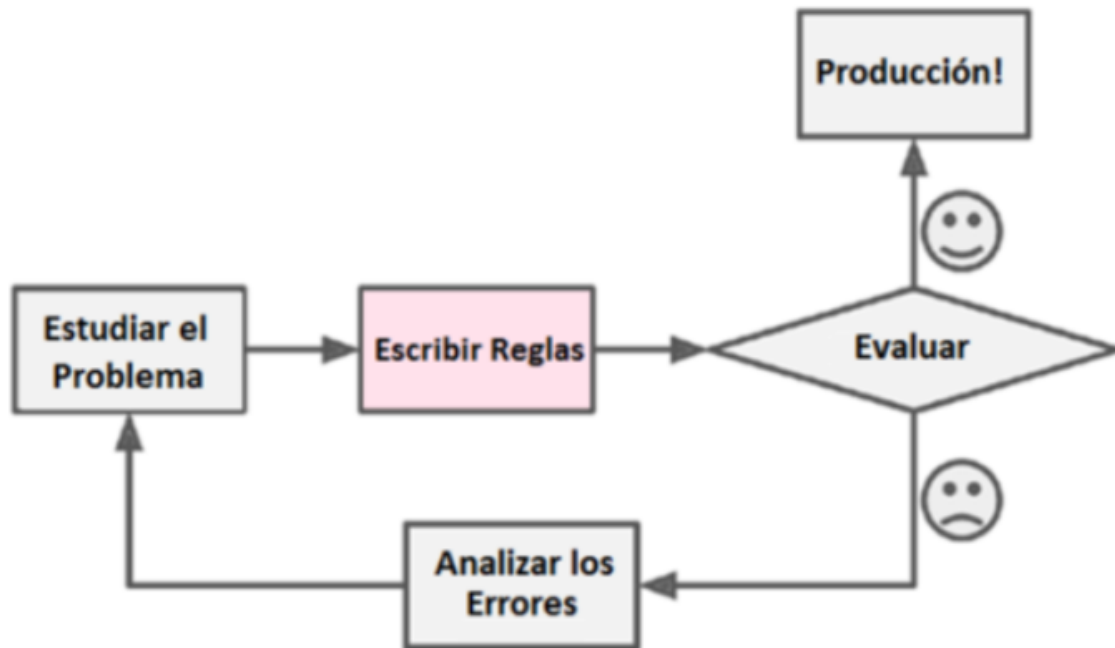


Figura 6.4 Enfoque de programación tradicional

Ahora las nuevas palabras pueden ser “pandemia”, “soledad”, “ayuda”, “anticovid”. Entonces, después de haber logrado esta tarea, con su correspondiente gasto de tiempo, incluyo en mi programa estas nuevas palabras y filtros. Pero nuevamente quienes producen los spam buscan nuevas formas de que sus correos sean aceptados como correos buenos. De manera que después de un análisis, tendría que volver a actualizar mi programa filtro. Llegamos a la conclusión que definitivamente esta no es la mejor manera de mantener un filtro actualizado y funcionando permanentemente.

En contraste, un filtro de spam basado en técnicas ML, aprende automáticamente qué palabras y frases son buenos predictores de spam, detectando patrones inusualmente frecuentes de las palabras en ejemplos spam, comparados con los ejemplos normales. El programa es mucho más corto, más fácil de mantener y probablemente más preciso. De manera que un filtro spam basado en ML se dará cuenta automáticamente que “pandemia”, “soledad” se han vuelto inusualmente frecuentes en los emails marcados por los usuarios como spam y comenzará a marcarlos sin necesidad de reprogramarlo.

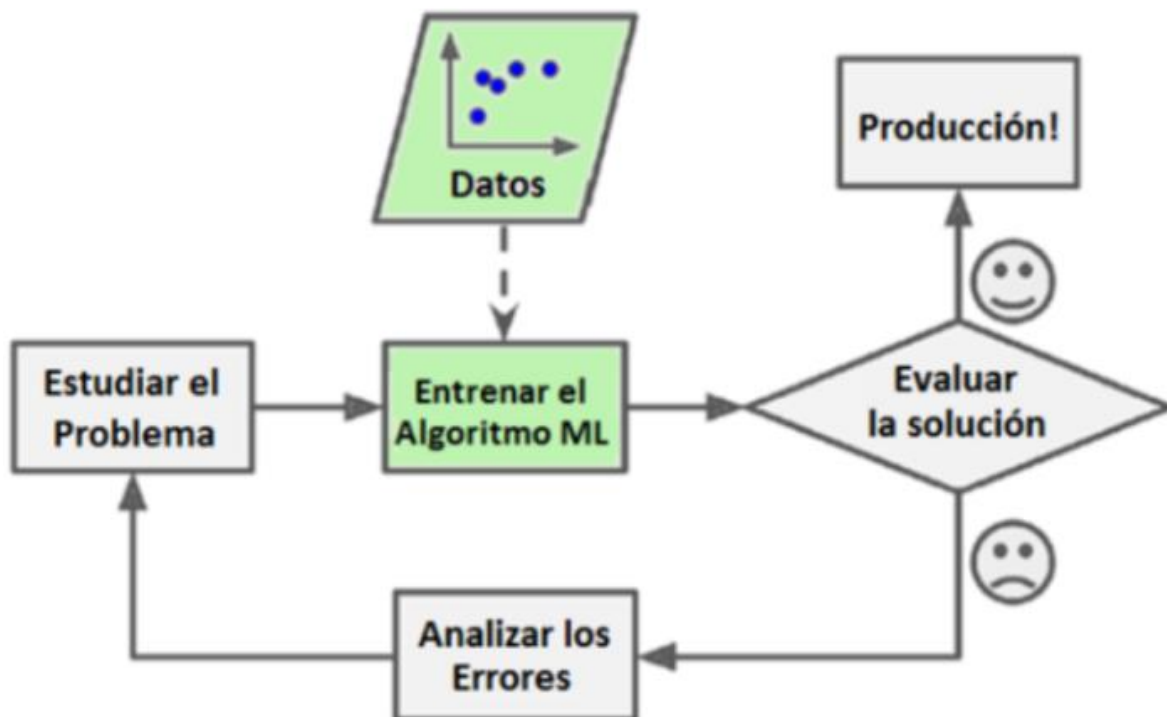


Figura 6.5. Enfoque de programación con ML.

En la figura 6.5, se puede observar cómo es la programación ML. El primer paso, lo mismo que en la programación tradicional se estudia el problema, pero luego se cambia y se entrena un algoritmo de ML, que es realmente un modelo, se evalúa su solución hasta cuando el modelo funcione bien y se lanza a producción. Sin embargo, en la medida en que los spams van cambiando, los usuarios van marcando que correos son no deseados, el modelo va aprendiendo y se va ajustando permanentemente a las nuevas formas de spam. Así, la actualización del filtro es automática.

Además, ML puede ayudar al aprendizaje humano. Los algoritmos de ML se pueden inspeccionar para ver lo que han aprendido, aunque en algunos algoritmos esto pueda ser algo complicado. Así, para el caso del filtro, cuando el modelo ya se ha entrenado con suficientes spams, es fácil inspeccionar y ver las listas de palabras y combinaciones de palabras que pueden ser los mejores predictores de spam.

Aplicar técnicas de ML para cavar en grandes cantidades de datos, puede ayudar a descubrir patrones que no eran inmediatamente evidentes, lo que se conoce como "*minería de datos*". Otra área donde sobresale ML es en problemas que o son muy complejos, para el enfoque tradicional, o simplemente no hay un algoritmo conocido.

En resumen, ML es ideal para:

- Solucionar problemas para los cuales existen soluciones que requieren mucho refinamiento o largas listas de reglas: un algoritmo ML generalmente puede simplificar el código y comportarse mejor que el enfoque tradicional de programación.

- Solucionar problemas complejos: para los cuales se usan fundamentos de enfoques tradicionales que no son una buena solución.
- Ambientes fluctuantes: un sistema ML puede adaptarse a nuevos datos.
- Sacar ideas sobre problemas complejos con gran cantidad de datos.

6.4 Aplicaciones de ML

Son muchas las áreas de aplicación de ML, que dejan abierta a muchos nuevos desarrollos en diferentes campos, tanto para la predicción o regresión, como para clasificación:

1. **Reconocimiento de imágenes.** Es una de las aplicaciones más comunes de ML, por la cantidad de utilidad que tiene en campos que van desde la robótica, la seguridad hasta los sistemas de recomendación por imágenes.
2. **Reconocimiento de voz.** Incluye paso de voz a texto, en robótica para comandos por voz, identificación de voz, análisis de sentimientos, síntesis de voz y otras. Este componente es clave para muchas aplicaciones.
3. **Predicción de tráfico.** Las vías del mundo están cada vez más congestionadas y los costos en tiempo y dinero de tener personas y mercancías varadas, es muy alto. De manera que cuando se quiere predecir una ruta hay sistemas confiables que lo hacen como “wase”, que funciona en tiempo real, con base en toras tecnologías y empresas que proveen estos servicios satelitales.
4. **Recomendación de productos.** O, Sistemas de Recomendación, se usan mucho en comercio electrónico como en Amazon, AliExpress, Netflix. Una vez uno ha seleccionado un producto las redes sociales lo invaden a uno de información referente al producto.
5. **Vehículos autónomos.** Los carros autónomos ya están en prueba en varios lugares del mundo, lo mismo que muchos robots móviles en empresas industriales. También en aviónica, drones, y para exploración espacial, robots que en determinadas circunstancias funcionan de manera autónoma.
6. **Filtros spam y para programas malignos (malware).** Como lo vimos en nuestro ejemplo, la llegada de correos mal intencionados, pueden inducir a generar problemas al usuario, lo mismo puede suceder con cualquier otro tipo de información textual, como puede ser la publicidad engañosa. Por otro lado, poder filtrar los programas engañosos o virus, son de mucha utilidad para el usuario normal.
7. **Asistente personal virtual.** Sistemas que ayudan a la toma de decisiones gerenciales leyendo información directamente de las bases de datos empresariales, haciendo promedios y resúmenes para adecuarlas al ambiente. También en herramientas de negociación.
8. **Detección en línea de fraudes.** Las transacciones en línea son permanentes y se utilizan en todo el mundo, aquí la utilización de ML hace estas transacciones confiables y seguras.
9. **Negocios en mercado de valores.** El uso de ML en mercado de valores esta muy extendido. Aquí la variable tiempo es fundamental, en algunos negocios de Fintech.
10. **Diagnóstico médico.** ML se comienza a utilizar en diagnóstico médico, especialmente apoyados en tomografías. Ayuda en diagnóstico y hallazgo de tumores de seno y cerebrales. Aquí es importante destacar la riqueza que hay en las historias clínicas, que se tiene de todos los usuarios de los servicios médicos, de cuya riqueza todavía no se tiene conciencia. Es posible

que ya haya equipos para este tipo de diagnóstico que directamente incluyan hardware especializado con Deep Learning, para diagnóstico rápido.

11. **Traducción automática de lenguajes.** Hoy en día viajar a cualquier parte del mundo puede ser una experiencia más enriquecedora contando con equipos manuales de traducción automática en tiempo real a precios muy cómodos. Esta es una aplicación de ML, muy importante porque permite con la facilidad de comunicación entre los seres humanos.

12. **Inteligencia Artificial Creativa.** Es un tipo de IA que puede generar o crear una amplia variedad de datos en forma de texto, imágenes, videos, audio y modelos 3d.

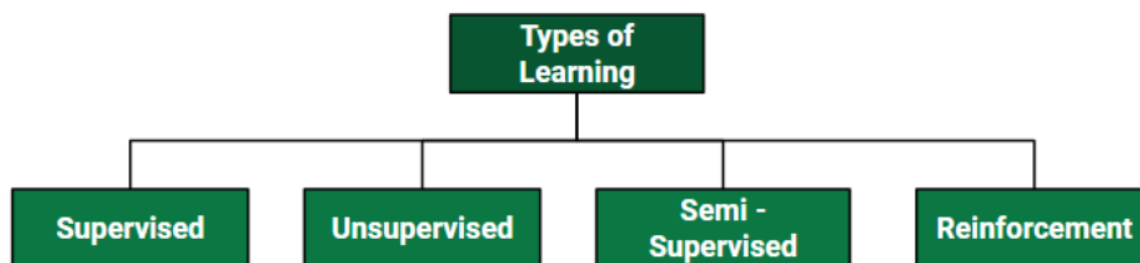
Todas estas aplicaciones están soportadas por herramientas como RNA, Deep Learning y Redes Convolucionales. Otras herramientas muy utilizadas son K-NN Nearest, SVM y árboles de decisión.

6.5 Algoritmos en ML

Estos algoritmos se presentan en el Apéndice.

6.6 Tipos de aprendizaje en ML

Ya hemos hablado algo de aprendizaje cuando estudiamos el aprendizaje supervisado para el algoritmo de retropropagación en RNAs. Además, por el tipo de aprendizaje se permite de cierta manera una clasificación de algoritmos de ML. Hay cuatro categorías importantes de aprendizaje: aprendizaje supervisado, aprendizaje no supervisado, aprendizaje semi-supervisado y aprendizaje reforzado RL.



6.6.1 Aprendizaje supervisado

En el aprendizaje supervisado el conjunto de entrenamiento con el que se alimenta el algoritmo incluye las soluciones deseadas llamadas rótulos o labels.

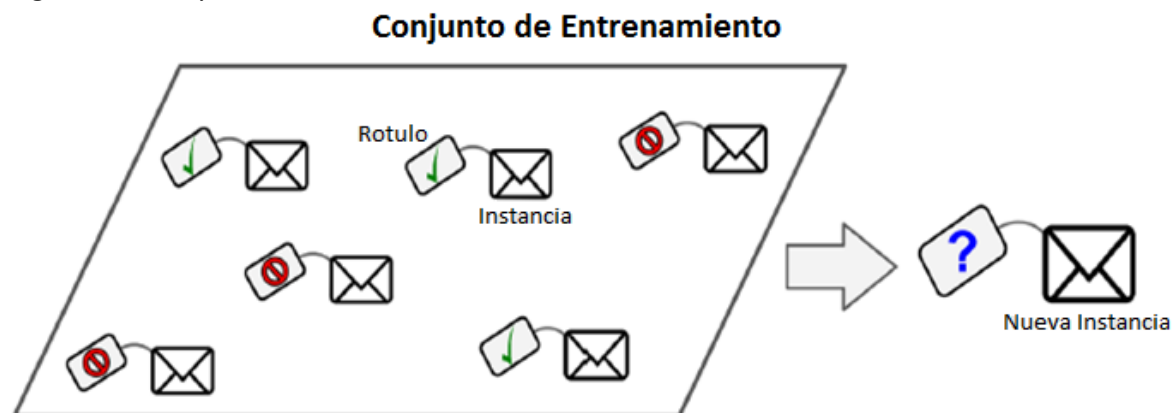


Figura 6.6. Un conjunto de entrenamiento rotulado para clasificación de spam

Los modelos se ajustan a los datos de entrenamiento que comprenden las entradas y las salidas. Se usan para hacer predicciones sobre conjuntos de prueba en los que solo se proveen las entradas y las salidas del modelo se comparan con las variables rótulo almacenadas, lo que sirve para estimar la bondad del modelo.

Hay aprendizaje supervisado en la clasificación del spam. Este es un buen ejemplo ya que se entrena con muchos emails junto con su clase: spam o normal, así aprende cómo clasificar los nuevos emails. En la figura 6.6, el filtro se ha entrenado con un conjunto de entrenamiento, que incluye correos normales y correos no deseados, cuando llega un correo nuevo, el filtro lo clasifica.

Otra tarea es predecir un valor numérico objetivo, como el precio de un carro. Sí se tiene un conjunto de datos con características como: kilometraje, edad, marca, y otros, llamados predictores, se puede hacer un modelo de regresión para entrenar el sistema.

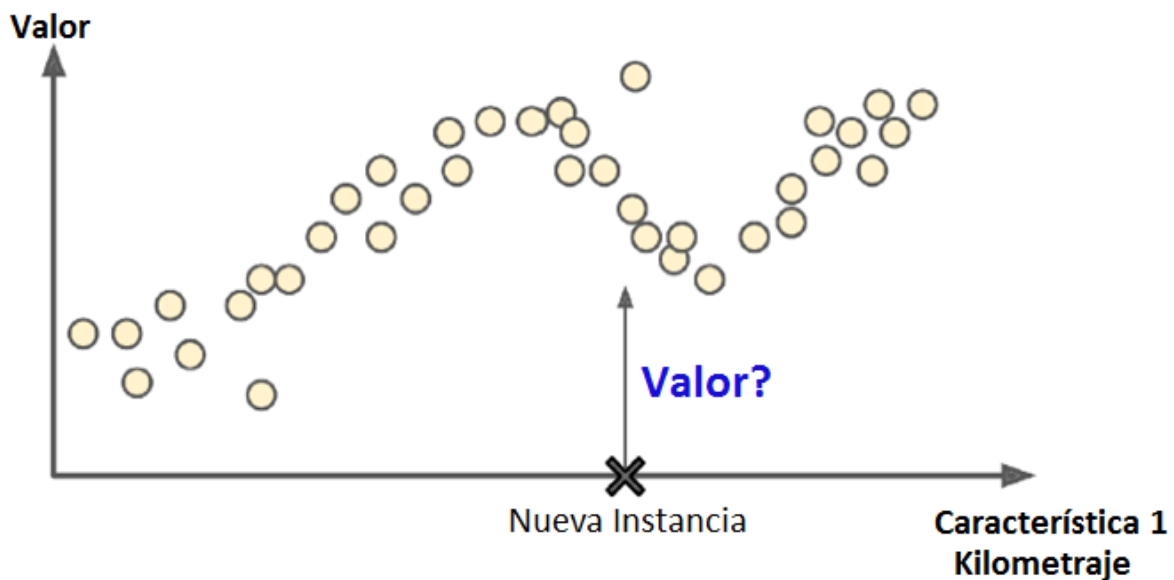


Figura 6.7. Un conjunto de entrenamiento rotulado para regresión.

En la figura 6.7, se tiene un modelo de regresión ajustado con el conjunto de entrenamiento, en este caso con sola una característica (feature), el kilometraje, para predecir el valor de un carro. En general hay varias características de entrada.

6.6.2 Aprendizaje no supervisado

Como se puede adivinar, un aprendizaje no supervisado se realiza con un conjunto de entrenamiento que no está rotulado, el sistema trata de aprender sin un instructor. En la figura 6.8, se puede apreciar un conjunto de datos sin rótulo. El agrupamiento (clustering) es un concepto importante en aprendizaje no supervisado, se trata de encontrar una estructura o patrón en un conjunto de datos no categorizado.

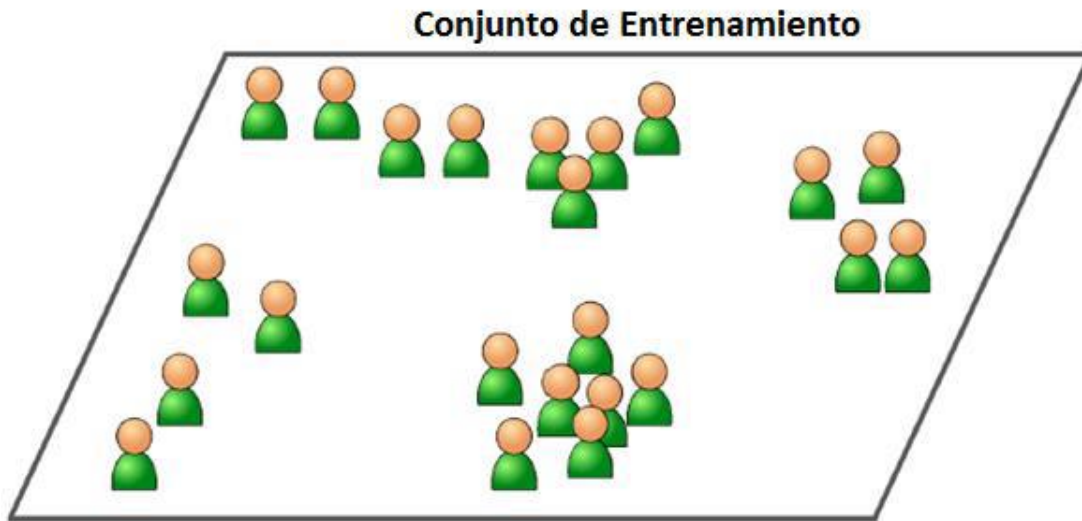


Figura 6.8. Un conjunto de entrenamiento rotulado para aprendizaje no supervisado.

Los algoritmos de visualización también son buenos ejemplos de aprendizaje no supervisado. Al alimentarlos con datos complejos y sus rótulos, estos algoritmos sacan una representación 2D o 3D de sus datos, que se puede plotear fácilmente. Y tratan de preservar la estructura y la manera en qué se puede comprender cómo están orientados y organizados los datos y quizá encontrar patrones no sospechados.

Supongamos que usted tiene una cantidad de datos correspondientes a huevos y quiere correr un algoritmo de clustering para tratar de detectar grupos por tamaños de huevos: jumbo, AA, A y B. En el conjunto de datos no hay rótulos que le digan al algoritmo a qué grupo pertenece un determinado huevo, el algoritmo encuentra esos grupos sin ayuda. Este es un ejemplo de agrupamiento.

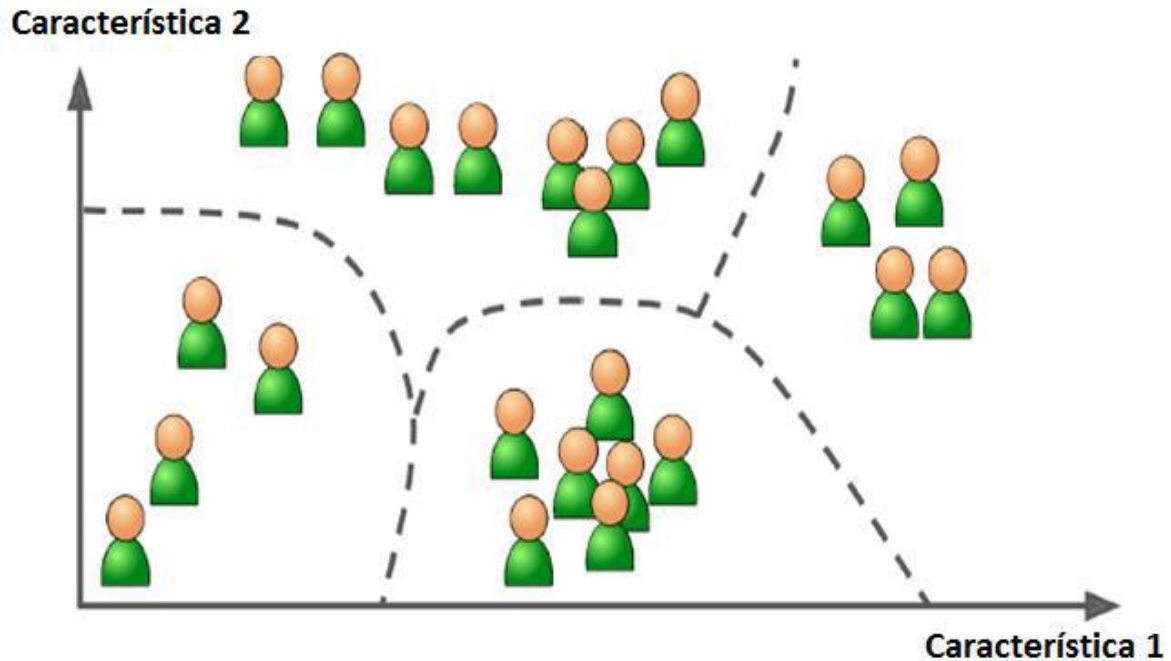


Figura 6.8. Agrupamiento, resultado de entrenamiento con aprendizaje no supervisado.

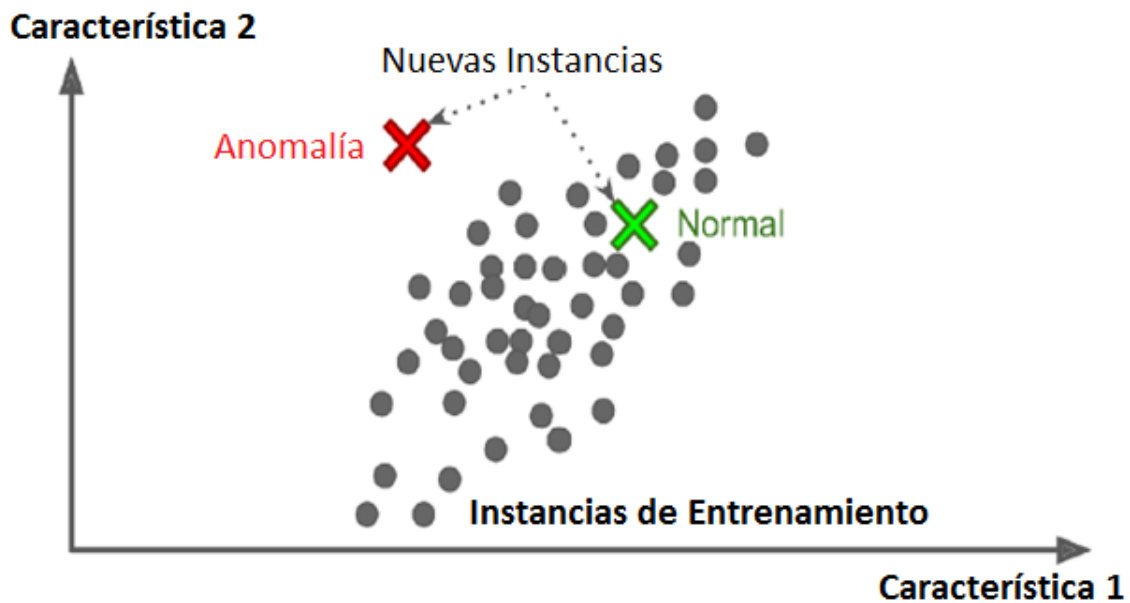


Figura 6.9. Detección de anomalías.

Otra tarea no supervisada es la detección de anomalías, por ejemplo, detectar transacciones inusuales en tarjetas de crédito para prevenir el fraude; encontrar defectos de fábrica o eliminar valores atípicos en los datasets para alimentar otro algoritmo de ML. En la figura 6.9, se puede observar cómo al llegar una nueva instancia de una transacción comercial, el algoritmo puede detectar si la transacción es válida o se trata de una anomalía, es decir de un fraude.

Sin embargo, la rotulación en algunas aplicaciones, es difícil y costosa en esfuerzo en tiempo ya que puede requerir trabajo de anotadores humanos a veces con experiencia y entrenamiento en el dominio del específico. Esto es especialmente cierto para aplicaciones que incluyen aprendizaje de gran número de rótulos de clases y a veces con similitudes entre ellas. Se utilizan algoritmos K-NN, SVM entre otros.

6.6.3 Aprendizaje semi-supervisado

El aprendizaje semi-supervisado (SSL) es una técnica de ML una pequeña parte de datos rotulados y cantidades de datos no rotulados para entrenar un modelo predictivo. Su importancia se debe a lo costoso de la rotulación.

Algunos servicios de almacenamiento de fotos, como Google fotos son buenos ejemplos de este tipo de aprendizaje. Una vez usted descarga las fotos de su familia allí, este reconoce automáticamente la persona que aparece en diferentes fotografías.

Característica 2

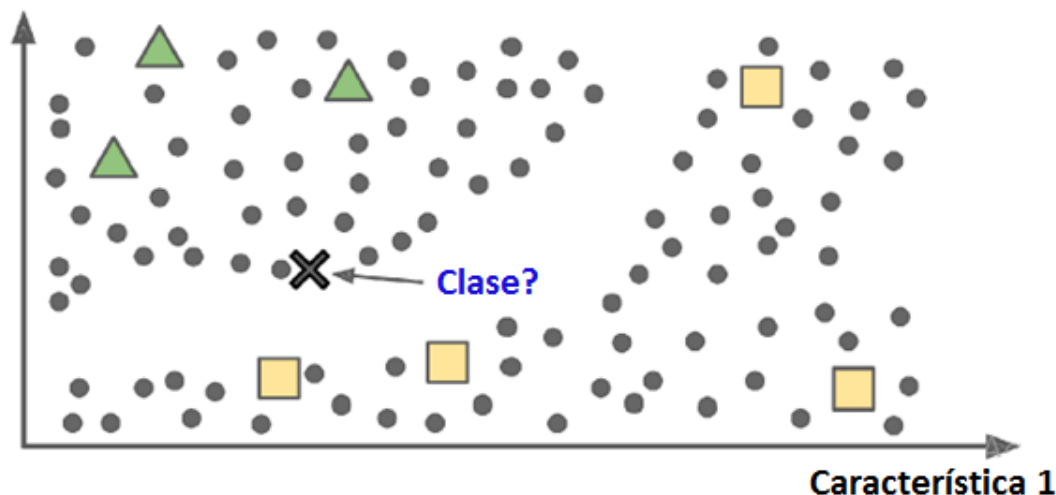


Figura 6.10. Aprendizaje semi-supervisado.

También son varios los proyectos de este tipo que ha desarrollado y está desarrollando FaceBook. Un algoritmo bastante popular es representar los datos rotulados y no rotulados en forma de grafo y luego aplicar un algoritmo de propagación de rotulos. Este difunde rotulaciones hechas por un humano a través de toda la red del data set. <https://www.altexsoft.com/blog/semi-supervised-learning/>.

6.6.4 Aprendizaje reforzado

El aprendizaje reforzado es un enfoque de ML en el cual se entrenan agentes para tomar una secuencia de decisiones. En el aprendizaje reforzado, el sistema de aprendizaje se llama "agente".

Para el entrenamiento, el agente observa el ambiente, toma decisiones y ejecuta acciones. El agente recibe una retroalimentación en términos de recompensas de retorno dependiendo de si la acción fue exitosa o penalidades si no lo fue. Debe aprender por sí mismo cuál es la mejor

estrategia, llamada política, para obtener la mayor recompensa. En el tiempo, una política define qué acción debe escoger el agente cuando está en una situación dada.

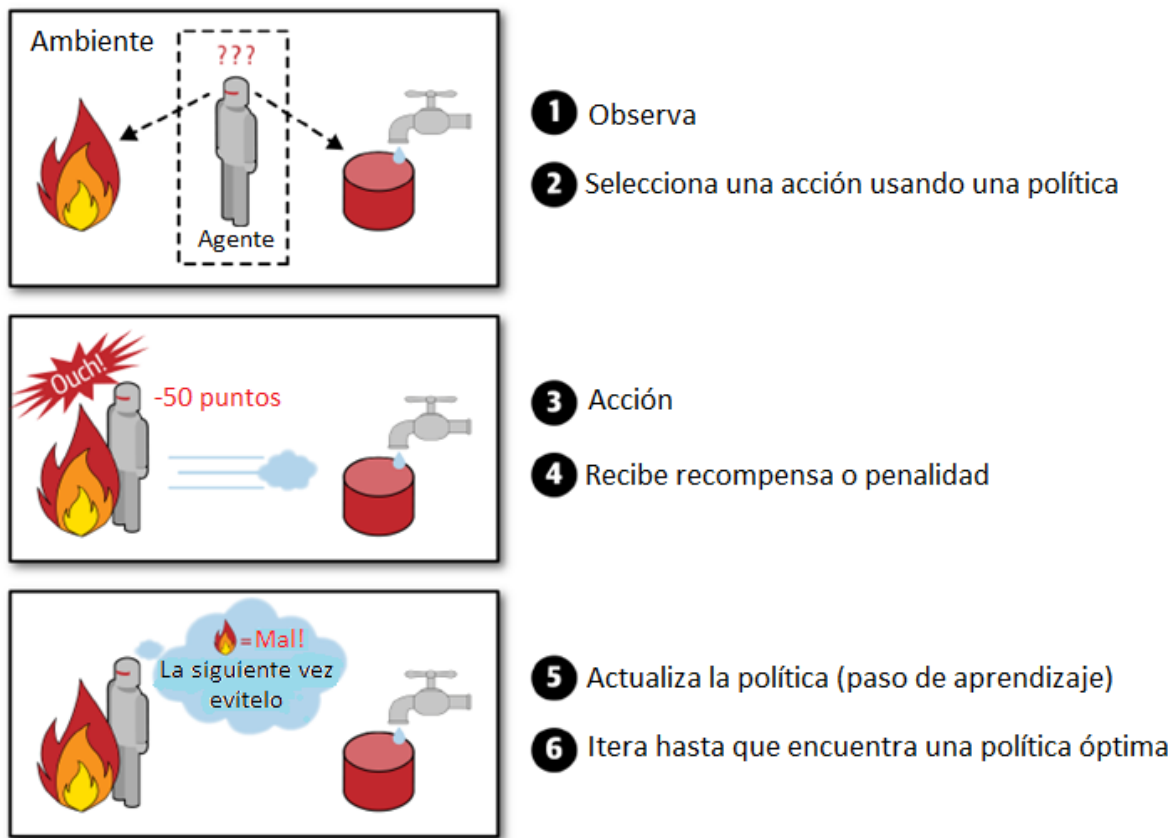


Figura 6.11. Aprendizaje reforzado.

Al principio, el agente no conoce nada sobre el ambiente, por lo que toma las acciones de forma aleatoria. Si una acción trae una recompensa positiva, el agente deberá aprender a escoger esa acción más frecuentemente, mientras que, si una acción lleva a una penalidad, el agente tenderá a escoger esa acción menos frecuentemente. Así, **el agente aprenderá a escoger las acciones que maximicen la suma de recompensas recibidas**, que se conoce como **retorno**.

Hay tres tipos de algoritmos de aprendizaje por refuerzo:

- **Q-Learning**. El más importante, calcula el refuerzo 'por estados y acciones. Se usa cuando hay un número finito de estados y acciones.
- **Iteración de política**. Calcula el refuerzo por estados y acciones siguiendo dos pasos: evalúa la política en un paso, seguido por un paso de mejora en la política. Hay un agente y un dominio de estados y acciones. La tarea es encontrar una política que cause el refuerzo para incrementar cada estado inicial, sin causar el refuerzo de ningún otro estado sucesor para disminuirlo. Se usa cuando hay un número infinito de estados y acciones.
- **Iteración de valor**. Calcula el refuerzo para estados y acciones usando una señal de refuerzo determinada por una función de refuerzo. Se usa cuando conocemos una ecuación de ambiente y se necesita encontrar una función acción-valor que es una Q-

función que nos da el refuerzo para cada estado y acción. Se debe tener información completa sobre la ecuación de transición del ambiente.

Ver ejecución del juego Bong, en un Notebook de Jupyter.

6.7 Los datos

En el capítulo 1, hablamos de la utilización de los datos como una estrategia para realizar IA, lo que se puede observar directamente en ML. Para resaltar la importancia de los datos, vamos a hablar sobre la irrazonable efectividad de los datos.

En un artículo famoso publicado en 2001, de M. Banko y E. Brill de Microsoft, mostraron que algoritmos muy diferentes a ML, incluyendo los más simples, se comportan casi idénticamente bien, alrededor de la solución de un problema complejo una vez se tengan los datos suficientes: eliminar la ambigüedad en los lenguajes naturales. La idea de que los datos son más importantes que los algoritmos para solucionar problemas complejos fue popularizada por P. Norving, en el artículo “La irrazonable efectividad de los datos”.

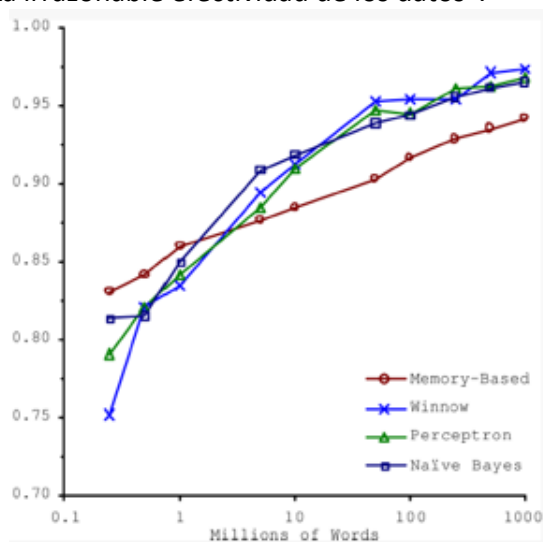


Figura 6.12. La irrazonable efectividad de los datos.

Sin embargo, se debe observar que los datos de entrenamiento de tamaño pequeño y de tamaño medio, son aún bastante comunes; y no es siempre fácil y/o barato obtener datos de entrenamiento. Ni se deben olvidar los algoritmos.

6.7.1 Problemas con los datos

Es importante resaltar el aspecto de la calidad de los datos pues juega un papel fundamental en el desarrollo de los modelos de ML. La mala calidad de los datos puede dar lugar a predicciones incorrectas, modelos defectuosos y resultados inexactos. Hay necesidad de tener datos de calidad para que los sistemas de IA, produzcan resultados precisos y significativos.

- **Datos de entrenamiento no representativos.** Con el fin de hacer una buena generalización, es crucial que los datos de entrenamiento sean representativos de los

nuevos casos que se quieren generalizar. Esto es más difícil de lo que parece: si la muestra es muy pequeña puede ser no representativa, pero aun los grandes muestreos pueden ser no representativos, si el muestreo es defectuoso.

- **Datos con calidad pobre.** Si los datos de entrenamiento están llenos de valores atípicos, errores y ruido, se hará más difícil y poco probable que el sistema detecte patrones subyacentes. El esfuerzo que se haga para depurar los datos de entrenamiento es bastante provechoso. Recordemos la Ciencia de Datos. Este es el trabajo al que más le dedican tiempo los científicos de datos.
- **Datos sesgados.** Es un problema implícito a muchos datasets, consiste en que desde la fuente de generación de los datos ya existe un sesgo o predisposición. Es el caso que se veía en el libro “Armas Matemáticas de Destrucción”, donde la política, la economía, la educación y la cultura, influyen en el comportamiento de la gente llevando a la producción de datos sesgados.

El último es uno de los problemas más graves con los que se enfrenta la tecnología ML, el problema está en que hasta cuando la herramienta no está en funcionamiento, sus problemas no se pueden detectar, precisamente, porque las personas que los debieran detectar están imbuidas dentro del mismo sistema.

6.8 Lenguajes y librerías

Para el desarrollo de aplicaciones ML, es preciso tener conocimientos de programación, de estructuras de datos, de manejo de memoria y mínimo de un lenguaje de programación. Además, hay muchas librerías que se ofrecen para diferentes lenguajes de programación para hacer ML, por lo que es muy fácil para personas con los conocimientos básicos señalados.

Por otra parte, en concepto de otros expertos, no hay un mejor lenguaje para ML, cada uno es bueno en determinado campo. Por ejemplo, la mayoría de los ingenieros de ML prefieren usar Python para problemas de lenguaje natural NLP, mientras que para análisis de sentimientos prefieren usar Python o R, y algunos probablemente van a usar Java, para otras aplicaciones de ML como seguridad y detección de amenazas.

Python

En estos momentos hay más de 8 millones de desarrolladores alrededor del mundo que usan Python. Según Spectrum de la IEEE, es el primer lenguaje utilizado, en este último año.

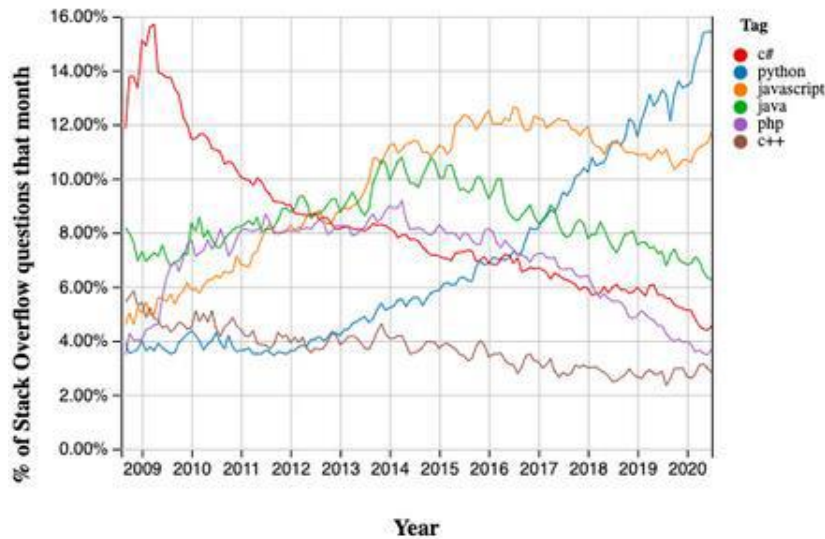


Figura 6.13. Uso de lenguajes de programación. Fuente Stack Overflow

R

Con más de dos millones de usuarios, 12000 paquetes en el repositorio CRAN, aproximadamente 206 grupos Meetup, más de 4000 preguntas sobre programación R cada mes, R es un lenguaje para escribir ML de estadísticos para estadísticos.

6.9. Panorama de ML

Los desarrollos que han conllevado a la reciente aparición de herramientas de IA Generativa, han llevado a replantear algunas consideraciones sobre el ML. Un benchmark o prueba de referencia es una medida de calidad que permite evaluar un desempeño contra otro. Así para evaluar el comportamiento de herramientas de ML existen una serie de data sets benchmark, uno de los primeros fue MNIST ya mencionada con números escritos a mano.

En un artículo de 2021, de Pott, Kiela et al., se presenta un gráfico de cómo la IA Generativa ha ido superando diferentes benchmarks, comprándola con el comportamiento humano para superar esos benchmarks. El grafico parte de los 90s en el eje X; y en el eje Y, toma una medida normalizada del estimado del comportamiento humano que es la línea roja, en cero.

Así el reconocimiento de números escritos a manos MNIST que se lanzó en los 90s, tomó aproximadamente 20 años sobrepasar el estimado del comportamiento humano. Switchboard tiene una historia similar se lanzó en los 90s, su problema es pasar de voz a texto; tomó aproximadamente 20 años pasar la línea roja. ImageNet tiene una historia más reciente, se lanzó en 2009, tomó 10 años alcanzar el punto de saturación; y a partir de aquí realmente se ha acelerado el paso de la línea roja, así SQUAD 1.1, para responder preguntas, lo solucionó en 3 años. La respuesta fue SQUAD 2.0, que se solucionó en menos de 2 años.

Y luego el benchmark GLUE, que es un conjunto grande de tareas destinado a probar el estrés de los mejores modelos. Cuando se anunció a muchos de los científicos del campo les preocupó que

fuera muy difícil para los modelos actuales. Pero GLUE se saturó en menos de 1 año. La respuesta fue SuperGlue destinado a ser mucho más difícil y también se saturó en menos de 1 año.

Benchmarks saturate faster than ever

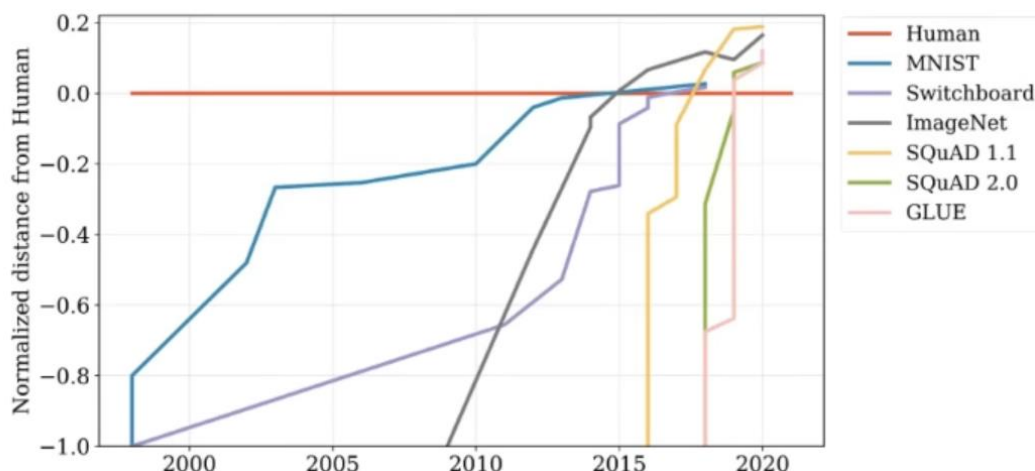


Figura 6.14. Cada vez es más rápido que las nuevas herramientas, saturan los benchmarks.

Esta es una historia notable de progreso indudable. Incluso si usted tiene dudas sobre las medidas del comportamiento humano, incluso aquí vemos un rápido incremento en la tasas de cambio. Y ahora 2021 fue hace años en la historia de la IA. Específicamente en términos de NLU, Natural Language Understanding.

Como se puede observar ML es el paradigma de momento, que posiblemente dure bastante tiempo. El hecho de que su fortaleza está basada en la disponibilidad de conjuntos de datos bien conformados, lleva a pensar que esta puede ser su debilidad. Como ya se ha visto, los problemas en el dataset pueden llevar a que el modelado con ML sea un completo desastre.

Para el desarrollo de un proyecto de ML, se deben seguir los siguientes pasos:

1. Definir el objetivo del proyecto
2. Definir el criterio de evaluación
3. Evaluar la solución actual
4. Obtener un dataset confiable y con los datos suficientes
5. Seleccionar el modelo
6. Analizar los errores del modelo
7. Aplicar el modelo para el objetivo planteado

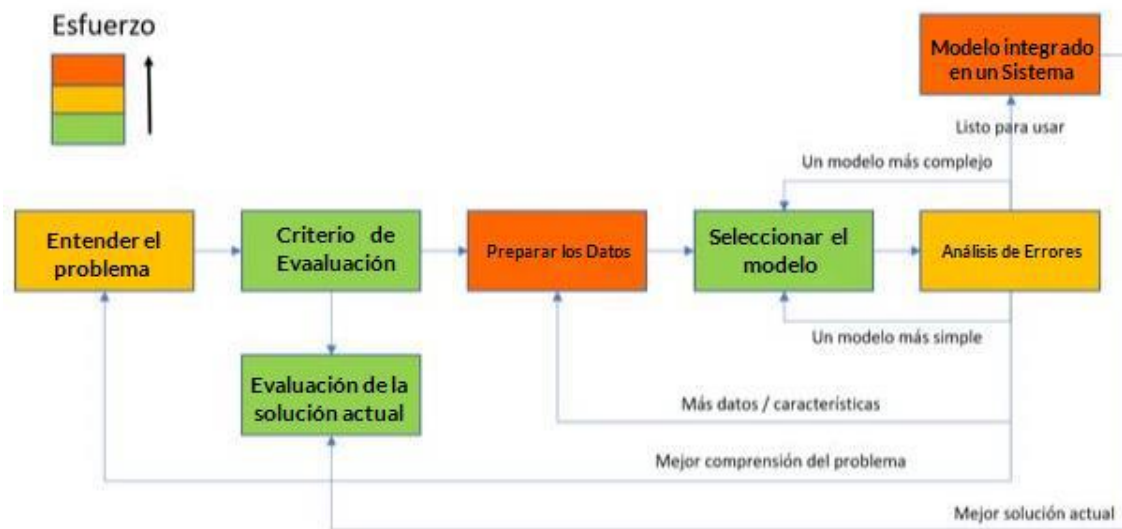


Figura 6.14, modelo para la implementación de sistemas de ML

6.10. ML oscura

Como la base de los algoritmos de ML son los datos, hechos ya pasados, sus resultados son conservadores, GPT-3 está entrenada con datos hasta del 2021. Funcionan en el pasado, por lo que, en muchos casos, son incapaces de predecir los cambios culturales y los gustos.

Veamos un caso en Amazon, con experiencia en IA, donde ha habido problemas. Según un reporte de Reuters, este gigante del e-commerce tenía un sistema interno que usaba IA para examinar las aplicaciones, que hacen las personas interesadas en trabajar con Amazon. Después de algunas quejas se encontró que una herramienta de reclutamiento de personal tenía prejuicios contra las mujeres degradándolas consistentemente. Este sistema fue descartado por Amazon, luego de observarse estos comportamientos.

Como se ha visto, los sistemas de ML funcionan con datos históricos, en los que se han mantenido estos prejuicios, generalmente llevando a que se perpetúen los prejuicios existentes. En este caso el prejuicio estaba en los ambientes de trabajo dominados por hombres. El otro problema especialmente en IA Generativa, con uso universal, no se tiene datos válidos de la periferia sobre muchos aspectos, llevando a respuestas demasiado pobres e inexactas.

Otra manera en que se implementan prejuicios de género y raza se debe a cómo, de manera inconsciente, los desarrolladores hacen las implementaciones con estos sesgos. Este es un problema muy complicado de resolver y la única solución es a través de una muy buena educación, consideración que las empresas de desarrollo en general no son conscientes.

En Colombia, por ejemplo, el ICBF se ha apoyado en el software "BETTO" para tomar decisiones con respecto a la contratación de entidades para el cuidado de niños en condiciones de vulnerabilidad. BETTO, según el gobierno del momento, es una estrategia, una política, y un vehículo de transparencia para la contratación en el ICBF. BETTO incorpora IA, con la capacidad de utilizar algoritmos de control en las plataformas de ciberseguridad, para dar certeza en los procesos de contratación administrativa.

Sin embargo, varias ONG, que habían trabajado durante varios años en esta tarea con el ICBF, no fueron contratadas, debido a que BETTO escogió otras entidades para su contratación. Según la directora del ICBF del momento, fue BETTO quien tomó la decisión, lo que según ella garantiza la idoneidad del proceso. El desconocimiento, la ignorancia y el miedo a enfrentarse a cierto tipo de herramientas hace que las persona le deleguen la responsabilidad de decisiones importantes al “sistema”, algo realmente inconcebible pero real.

En su libro, Cathy O’Neal, “Armas Matemáticas de Destrucción”, plantea que estamos viviendo en la edad del algoritmo, que las decisiones que afectan nuestras vidas no las toman los humanos sino los modelos matemáticos. En teoría esto lleva a una mayor equidad, pues en principio, todos somos juzgados por las mismas reglas. Pero en la práctica ocurre todo lo contrario, los modelos son opacos, no están regulados, son incontestables. Esto lleva a un refuerzo en la discriminación.

Supongamos que ustedes se gradúan, generalmente van a trabajar en el desarrollo de un proyecto. En poco tiempo ven la necesidad de salir de la casa y adquirir un apartamento pequeño. Van al banco donde le consignan su salario y manifiestan su interés de compra con el fin de conocer todas las condiciones para que le presten para una hipoteca. Y comienzan los problemas, si bien su ingreso es alto, no tiene contrato a término indefinido, no tiene experiencia crediticia y otros. Las reglas de la banca actual no permiten que se le otorgue un préstamo, estas reglas se llevan a los algoritmos, perpetuando la discriminación.

En el libro “THE BOOK OF WHY”, j Pearl y D. Mackenzie, Planten el problema de ML en el sentido que llevan a que características (features) altamente correlacionados se asumen como relaciones causa efecto, llevando a veces a resultados completamente desatinados.

6. 11 IA Generativa

Es un tipo de IA que crea una amplia variedad de datos y lo hace a partir de patrones aprendidos de datos existentes. La IA generativa es capaz de producir contenido altamente realístico y complejo que imita la creatividad humana, a partir de indicaciones (prompts) hechas por personas que pueden no tener ningún nivel de tecnología IA, convirtiéndose en una herramienta valiosa para muchas industrias.

Algunos avances recientes en el campo como GPT (Generative Pre-trained Transformer) han impactado el ambiente mundial llevando a fuertes cuestionamientos sobre su uso especialmente en ambientes educativos. El modelo utilizado Transformer, basado en redes neuronales feedforward, ha revolucionado el campo debido a la capacidad de extensión de su atención.

Como se ha visto, la IA Generativa, está influyendo en mucha gente, por lo que se debe poner especial atención a los posibles problemas que pueda generar, en diferentes campos de la actividad humana. Una cultura que tome la decisión de trabajar con IA Generativa debe considerar algunos aspectos importantes (tomados de <https://www.techtarget.com/searchenterpriseai/tip/Generative-AI-ethics-8-biggest-concerns>):

- **Contenido dañino.** Al crear automáticamente contenido basado en indicaciones (prompts) hechas por los humanos, pueden producir mejoras en la productividad, pero también pueden dañar de manera intencional o no intencional. La IA Generativa debe ayudar no reemplazar a humanos o procesos.

- **Derechos de autor y problemas legales.** Entre los muchos datos con que se han entrenado estas herramientas está internet, cuando crean imágenes o líneas de código, las fuentes son desconocidas lo que puede ser problemático para una compañía farmacéutica que confía en una fórmula, lo que puede generar problemas de propiedad intelectual.
- **Violaciones a la privacidad de los datos.** En su entrenamiento estas herramientas pueden incluir información personal, que es difícil de eliminar, como en el caso de otros buscadores.
- **Divulgación de información sensible.** Estas herramientas democratizan las capacidades de la IA haciéndola más accesible. Combinar accesibilidad y democracia, podría eventualmente llevar a divulgar información sensible, por ejemplo de pacientes, exponiéndolos a campañas de productos.
- **Papeles y moral de la fuerza de trabajo.** La IA puede hacer mucho del trabajo diario que hacen muchos trabajadores con conocimiento como escribir, crear contenido, codificar. Aunque el desplazamiento y reemplazo de trabajadores ha sido continuo desde la implementación de herramientas de IA, se ha aumentado con la aparición de tecnologías de la IA Generativa.
- **Procedencia de los datos.** Esta tecnología consume tremendos volúmenes de datos que pueden manejarse inadecuadamente, de origen cuestionable, usados sin consentimiento o con parcialidades. Se pueden amplificar niveles adicionales de imprecisión por influencers sociales y los propios sistemas de IA.
- **Falta de explicabilidad e interpretabilidad.** Muchos sistemas de IA Generativa, agrupan hechos de manera probabilística, volviendo al camino en que la IA aprendió a asociar elementos de datos. Estos detalles no siempre se revelan cuando se usan aplicaciones como Chat-GPT, por lo que en consecuencia se cuestiona la confiabilidad de los datos.

A continuación una charla con Chat-GPT sobre IA

Problemas del uso de la IA en la sociedad del tercer mundo

ChatGPT

El uso de la inteligencia artificial (IA) en la sociedad del tercer mundo puede presentar algunos problemas y desafíos específicos. Algunos de estos problemas pueden incluir:

1. **Acceso limitado a la tecnología:** En muchos países del tercer mundo, el acceso a la tecnología de la IA puede ser limitado debido a factores como la falta de infraestructura de tecnología de la información, el alto costo de la tecnología o la falta de personal calificado para utilizarla.
2. **Desigualdades económicas:** El uso de la IA puede agravar las desigualdades económicas en los países del tercer mundo, ya que las empresas y los individuos más adinerados pueden tener más acceso a la tecnología y pueden beneficiarse más de ella que aquellos con menos recursos.
3. **Riesgos para el empleo:** La IA puede reemplazar a algunos trabajadores en algunas industrias, lo que puede crear problemas de empleo en los países del tercer mundo.

4. Problemas de priv

Falto terminar el punto 4

ChatGPT

Lo siento, dejé la pregunta incompleta. Aquí está la pregunta completa:

"Problemas del uso de la IA en la sociedad del tercer mundo"

4. Problemas de privacidad y seguridad: El uso de la IA puede plantear problemas de privacidad y seguridad en los países del tercer mundo, especialmente si no se cuenta con leyes y regulaciones adecuadas para proteger la privacidad y seguridad de los datos. Además, puede ser más difícil proteger la privacidad y seguridad de los datos en los países del tercer mundo debido a factores como la falta de infraestructura de tecnología de la información o la falta de personal calificado para proteger los datos.

Porque no considera los problemas politicos?

Lo siento, no mencioné los problemas políticos en mi respuesta anterior. En efecto, el uso de la inteligencia artificial (IA) en la sociedad del tercer mundo también puede plantear problemas políticos. Algunos ejemplos de estos problemas pueden incluir:

1. Control del gobierno: El gobierno de algunos países del tercer mundo puede utilizar la IA para controlar a la población y restringir la libertad de expresión y otros derechos fundamentales.
2. Desigualdades políticas: El uso de la IA puede agravar las desigualdades políticas en los países del tercer mundo, ya que algunos grupos pueden tener más acceso a la tecnología y pueden beneficiarse más de ella que otros.
3. Corrupción: El uso de la IA puede ser utilizado para facilitar la corrupción en los países del tercer mundo, especialmente si no se cuenta con leyes y regulaciones adecuadas para prevenir la corrupción.
4. Influencia extranjera: La IA puede ser utilizada por gobiernos y empresas extranjeras para influir en la política de los países del tercer mundo.

Como se puede ver, los problemas con la IA Generativa tienen que ver mucho con la falta de educación y formación de las personas. La gente debe ser crítica de lo que le dicen y valorar con su juicio todas las soluciones que le dan estas herramientas.

6.11. Ejercicio

1. Con base en la figura 6.1, tome una ecuación determinada, por ejemplo una raíz cuadrada o cúbica, o un seno, genere un data set con muchos valores. Usando una herramienta de ML, encuentre el resultado de un determinado valor.

2. Diseñe e implemente un sistema de almacenamiento de datos, para la entrada de productos para una pequeña bodega, utilizando la voz. Ver el siguiente link:
<https://cloud.google.com/speech-to-text/pricing>.
3. Desarrolle un problema de su escogencia.

6.11 Bibliografía

Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, Concepts, Tools, and Techniques to Build Intelligent Systems, **Aurélien Géron**.

Machine Learning in Robotics, 5 Modern Applications, Daniel Fegguella,
<https://emerj.com/ai-sector-overviews/machine-learning-in-robotics/>

Cathy O'Neal, Armas Matemáticas de Destrucción, 1972

J. Pearl y D. Mackenzie, THE BOOK OF WHY, The New Science of Cause and Effect, Basic Books, 2018.