

#### UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

#### CENTRO UNIVERSITARIO UAEM VALLE DE MÉXICO

Aprendizaje incremental para la tarea de reconocimiento de dígitos con Redes Neuronales Artificiales

#### **TRABAJO DE TESIS**

Que para obtener el Título de

#### **INGENIERO EN SISTEMAS Y COMUNICACIONES**

Presenta

C. Fragoso García Sandra C. González Hernández Luis Ángel

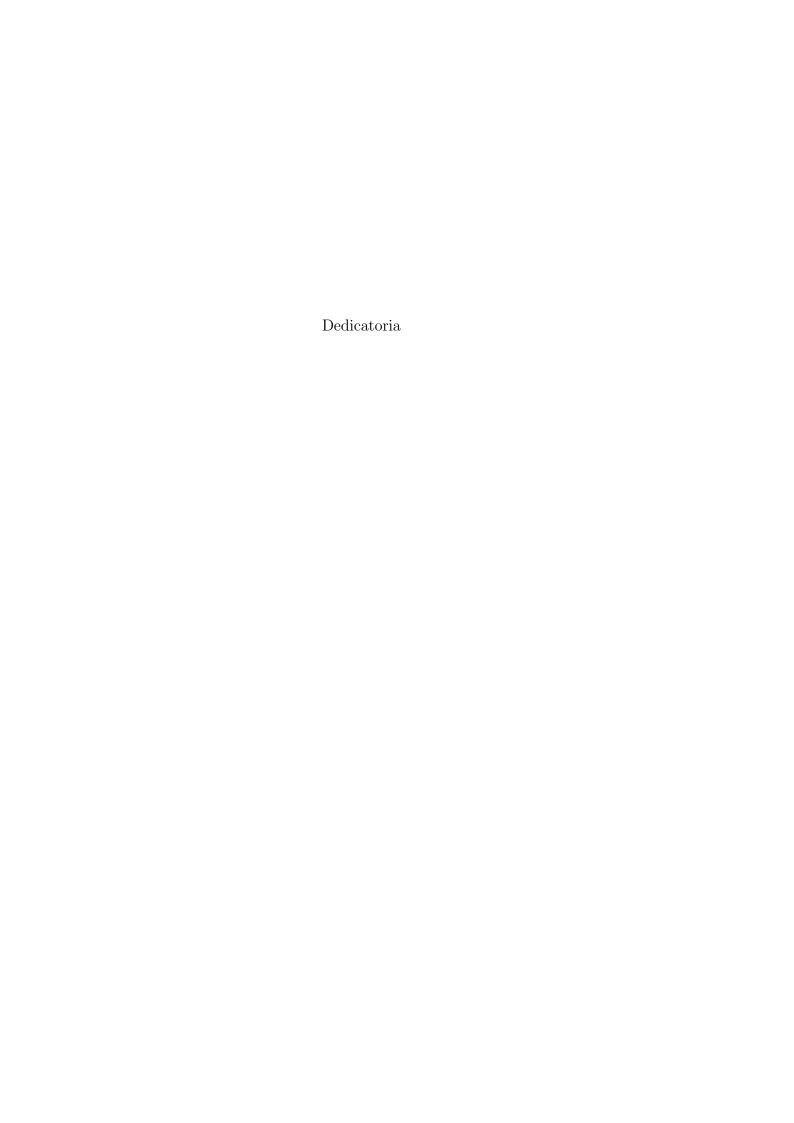


Centro Universitario UAEM Valle de México

Atizapán de Zaragoza, Edo. de Méx. Septiembre 2023

#### Resumen

El aprendizaje incremental es un área de la Inteligencia Artificial la cual permite agregar nuevo conocimiento a un modelo (e.g. Redes Neuronales Artificiales) sin la necesidad de entrenar el modelo con toda la información histórica de la tarea en cuestión [1]. En el presente trabajo de investigación se ocupará el modelo de Redes Neuronales Artificiales enfocada en la clasificación de dígitos escritos a mano usando el algoritmo de entrenamiento de backpropagation, con redes Multi capa Perceptron y duplicación de pesos múltiples simulando memoria a corto y largo plazo para mejorar los resultados presentados en [1].



# Agradecimientos

Sus agradecimientos

# Índice general

1.	Introducción	1
2.	Planeamiento del Problema	3
3.	Objetivos	6
	3.1. Objetivos Específicos	6
4.	Preguntas de Investigación	7
5.	Justificación	8
6.	Delimitación	11
7.	Revisión de la Literatura	12
	7.1. Redes Neuronales Artificiales	12
	7.1.1. Función de Activación	13
	7.2. Aprendizaje Incremental	14
	7.2.1. Algoritmos de Aprendizaje Incremental	15
8.	Metodología	18

# Índice de figuras

7.1.	Red Neuronal Artificial Básica	12
7.2.	Función Escalonada	14
7.3.	Dos enfoques tradicionales del aprendizaje incremental	15

# Índice de tablas

# Lista de Acronimos

### Introducción

La inteligencia artificial (IA) es una área del conocimiento que se enfoca en poder hacer máquinas que se enfocan en comportamiento y razonamiento humano, para que en momento dado, se pueda interactuar con una máquina. Así mismo, también es posible pensar que mucho del desarrollo en el área de inteligencia artificial, es el poder tener mejores herramientas que ayuden a las actividades diarias.

En este sentido, un área de la IA es el llamado Aprendizaje Máquina, donde se estudian algoritmos que permiten aprender de forma auomática una tarea. Así, una de las técnicas más conocidas en la actualidad, dentro del área de IA son las Redes Neuronales Artificiales (RNAs), siendo técnicas que realizan procesos matemáticos para poder aprenderse tareas a resolver. Algunas áreas en las que son útiles las RNAs son en el aprendizaje de tareas no lineales, como la predicción de la capacidad de la red 5G, basada en el tráfico diario de este [2] o clasificación, por ejemplo la clasificación de metales y rocas por medio de RNAs y lógica difusa [3].

Las RNAs están formadas por neuronas artificiales que simulan a las biológicas. Así los procesos químicos que suceden en el cerebro, se simulan computacionalmente a través de señales que viajen a través de las neuronas artificiales, de aquí en adelante simplemente se referirá a ellas como "neuronas". Las neuronas en una RNA cuentan con una

estructura distribuida en paralelo, presentando una buena habilidad de aprendizaje [4].

Dentro del aprendizaje máquina cuando una técnica, por ejemplo RNA, se enfoca en aprender una tarea, se conoce como algoritmo lineal sin memoria, siendo uno de los métodos más empleados desde el inicio de las RNAs [5]. Sin embargo, si es necesario incorporar nueva información del problema, es necesario volver a entrenar todo el modelo, considerando toda la información existente, esto es, la anterior y la nueva que acaba de llegar, es ahí donde nace el concepto de Aprendizaje Incremental, siendo un área enfocada en poder incorporar información del problema en cuestión, sin tener que volver a re-entrenar todo el modelo.

Derivado del aprendizaje incremental se desprende el concepto de memoria dentro de la IA, analizando como un algoritmo de aprendizaje máquina puede olvidar la información que se usó en un entrenamiento previo al entrenar con información más reciente. Si se hace la analogía con los humanos, la memoria es un factor importante para estudiar considerando la perdida de información aprendida, así, este es un problema biológico, el cual tanto afecta a los humanos como a las máquinas. Por ello, se han elaborado distintos experimentos para poder combatir esta problemática. Uno de estos es el caso de [1], el cual propone el manejo de RNAs con pesos dobles, donde la primer capa de pesos esta enfocada a comportarse como memoria a corto plazo, y la segunda como memoria a largo plazo. Los experimentos mostrados en [1] permiten notar un mejora en tareas de aprendizaje incremental, teniendo menos pérdida de información en comparación de implementaciones anteriores como el algoritmo Learn++ [6, 7].

Así, el presente trabajo de investigación esta enfocado en poder explorar nuevas configuraciones. Así, el presente trabajo de investigación esta enfocado en poder explorar nuevas configuraciones de pesos duplicados para poder extender el trabajo previamente presentado en [1]. de pesos duplicados para poder extender el trabajo previamente presentado en [1].

#### Planeamiento del Problema

Las Redes Neuronales Artificiales tienen la habilidad de poderse aprender una tarea y poder hacer o resolver tareas de predicción o clasificación básicamente. En este sentido, con algoritmos de aprendizaje como el Backpropagation, permite ajustar los pesos de una RNA para que esta pueda empezar a resolver una tarea particular. No obstante, muchas de las tareas que se resuelven en la vida diaria, van generando mas información con el tiempo, por ejemplo, el comportamiento de un una serie financiera, o bien la predicción del clima en una determinada región. Así, se tiene el aprendizaje incremental, siendo un método poco explorado enfocado en poder aprender nueva información del problema, sin tener que volver a entrenar todo el modelo con la información anterior y la nueva que acaba de llegar, esto es, en los modelos actuales de aprendizaje máquina, si se usa un conjunto de datos para entrenar un modelo en específico, dicho modelo es funcional para dicho conjunto de datos y la información que ello representa. Sin embargo, si es necesario incorporar nueva información al modelo, es necesario recolectar dicha información nueva, agregarla a la que se tenia anteriormente, y volver a entrenar todo el modelo para que éste pueda incorporar la nueva información.

De esta forma, una red ya entrenada con un primer conjunto de datos  $d_1$  se desea entrenar con un nuevo conjunto de datos del mismo problema  $d_2$ , al entrenar la red con  $d_2$  se perderá en conocimiento aprendido por  $d_1$ . Si no se desea utilizar un modelo de

aprendizaje incremental, se tendría que juntar el conjunto  $d_1$  y  $d_2$  en un solo conjunto y volver a entrenar la RNA para así poder incorporar el nuevo conocimiento  $(d_2)$  a la RNA. Si se desea utilizar el método de aprendizaje incremental, se puede entrenar en un primer momento a la red con el conjunto  $d_1$ , posteriormente con  $d_2$  teniendo poca perdida de información de  $d_1$ . Si más adelante llega mas información del problema  $(d_3)$  que se desee incorporar a la base de conocimientos de la RNA, entonces solo habrá que entrenar la RNA con  $d_3$  usando el modelo incremental para tener una pérdida mínima de información de  $d_1$  y  $d_2$ .

De esta forma, el presente trabajo tomará como base la investigación de [1], en donde utiliza una configuración de pesos dobles (a una RNA se duplican todos sus pesos), donde a una capa de pesos duplicados se enlaza con una tasa de aprendizaje alta, para simular un rápido aprendizaje, y por ende simular lo que sería memoria a corto plazo. En su contraparte, la segunda capa de pesos duplicados, se enlaza con una tasa de aprendizaje baja para aprender lentamente un problema, simulando la memoria a largo plazo. Es decir, al momento de aprender una tarea nueva, una capa de pesos aprenderá muy rápido la nueva tarea (tasa alta de aprendizaje) y por ende olvidará más rápidamente los datos ya aprendidos anteriormente, por otro lado, la segunda capa de pesos duplicados, aprenderá muy lentamente los nuevos datos que llegan, y por ende olvidando poco la información que anteriormente se aprendió. Considerando ello y también que la RNA trabaja en conjunto con ambas capas de pesos duplicados, se pondera la salida de la RNA para que pueda contemplar la información nueva que se acaba de agregar a la RNA en ambas capas, así como la información que se acaba de olvidar de ambas capas de pesos.

El problema principal del aprendizaje incremental mostrado en [1], es que entre más conjuntos de datos nuevos que lleguen, mas se olvidaran los primeros conjuntos que se aprendieron, lo cual no es tan útil si se contempla que en el futuro de una RNA podrán existir 10 o 20 etapas de entrenamiento incremental con nuevos conjuntos de datos que

se vayan recolectando.

Por ello es indispensable poder explorar nuevas configuraciones de RNAs que permitan mejorar los métodos actuales para permitir una menor cantidad de olvido conforme llegue nueva información al modelo. Donde al igual que en trabajos anteriores, el presente trabajo se basará en conceptos de memoria a corto y largo plazo, y en lugar de hacer una copia de los pesos actuales y tener dos tasas de aprendizaje, una rápida para simular la memoria a corto plazo, y otra tasa de aprendizaje para simular la memoria a largo plazo, se explorará por hacer mas copias de los pesos, teniendo más tasas de aprendizaje que operen en cada una de dichas copias.

## Objetivos

Diseñar una red neuronal artificial para aprendizaje incremental basada en el principio de la memoria a corto y largo plazo, buscando usar más de dos capas de pesos duplicados para el reconocimiento de dígitos, y con una menor pérdida de información de trabajos previos.

#### 3.1. Objetivos Específicos

- 1. Implementar el algoritmo mostrado en [1] para el reconocimiento de dígitos con aprendizaje a corto y largo plazo con los parámetros que ahí se indican.
- 2. Obtener el conjunto de datos de Optical Digits, limpiar los datos y prepararlos según lo indicado con [1].
- 3. Separar el conjunto de entrenamiento y de prueba de acuerdo a lo que se explica en el artículo de Bullinaria y probar el primer código implementado en miras de comprobar los resultados previamente mostrados en [1].
- 4. Tomar como base el algoritmo implementado, y extenderlo para permitir mas de dos pesos duplicados, aplicando el conjunto de datos previamente mostrado.
- 5. Comparar ambas implementaciones en busca de una reducción significativa de las tasas de aprendizaje con respecto a trabajos previos en la literatura.

# Preguntas de Investigación

- 1. ¿Existen trabajos más recientes sobre aprendizaje incremental?
- 2. La memoria a corto y largo plazo, representa dos extremos, pero ¿será posible subdividir más esa clasificación, para que más puntos intermedios puedan mejorar la memoria a corto y largo plazo, al mismo tiempo que el rendimiento en el aprendizaje incremental?
- 3. ¿El uso del aprendizaje incremental va a hacer que el tiempo de entrenamiento sea más rápido o al contrario?

#### Justificación

Las redes neuronales permiten el aprendizaje automático y la resolución de distintos problemas, pero como se comentó anteriormente, las técnicas de aprendizaje máquina, tienen una deficiencia que es al momento de aumentar los nuevos bloques de datos que llegan para aprender, se obtiene un deterioro en el rendimiento de aprendizaje de información y olvido de la información anterior [1].

Los resultados que se han obtenido no han funcionado a la perfección, la memoria a corto plazo olvida poco pero va olvidando, y lo ideal sería que no olvidara. Biológicamente, los humanos pueden aprender nuevas tareas, o información nueva de un problema, y no olvida de forma significativa lo que anteriormente aprendió, no obstante, eso no pasa actualmente con las RNA y en general con cualquier algoritmo de aprendizaje máquina. En otro sentido, los humanos ya tienen cierta configuración en el cerebro que les permite aprender como se hace actualmente, y se puede afirmar que por el momento no hay ningún procedimiento (ya sea quirúrgico o no) que permita modificar la estructura del cerebro para aprender mas y olvidar menos.

No obstante, computacionalmente nada puede impedir que se experimente con más configuraciones y llegar al punto en donde toda la información que ingrese a un modelo (por ejemplo RNAs) se acumule, y si no hay problema de almacenamiento, que ésta se

siga acumulando y que no olvide, esto podría ser bueno en diversas situaciones.

Desde un punto de vista computacional, si llega nueva información y no se ocupa aprendizaje incremental, esto implicará volver a entrenar todo el sistema con la información anterior y la actual (por ejemplo,  $d_1$  y  $d_2$ ) y considerando que una de las desventajas que tienen la RNAs es que el entrenamiento es un cuello de botella, siendo este donde se lleva la mayor parte de cómputo y por consiguiente de energía. Lo mencionado anteriormente implica que volver a entrenar con toda la información acumulada, gastará más energía y tiempo, que si solo se entrena con la nueva información que llega al modelo. En su contraparte, existe una gran variedad de herramientas, las cuales permiten codificar una red neuronal artificial con librerías ya preexistentes, para esta investigación solo se expondrán 2 empresas, siendo estas las más importantes: Microsoft y Google. La primera cuenta con la plataforma de Azure que renta una maquina virtual donde se puede programar en Python, y la segunda, cuenta con Google Colab que de igual forma brinda una máquina virtual para realizar experimentos de Maching Learning, la única diferencia contra Azure es que dicha herramienta es gratuita, y una similitud que tienen es que en ambas herramientas se puede programar en el mismo lenguaje.

Como se puede observar, las herramientas mencionadas permiten la programación en Pyhton, y esto se debe a que dicho lenguaje es una herramienta de software libre que no requiere licencia, es relativamente fácil poder depurar un código y permite acelerar más el desarrollo de aplicaciones, a diferencia de otros lenguajes más estructurados como C o Java, además tiene más librerías para el desarrollo de Maching Learning, por ejemplo, TensorFlow, Numpi, entre otras.

TensorFlow es una librería de Python que permite construir y entrenar redes neuronales para detectar patrones y razonamientos usados por los humanos, en la presente investigación se usará dado a que favorece la creación de una RNA, permite la elaboración de cualquier tipo de algoritmo de Machine Learning, cabe mencionar que también se puede usar para Deep Learning, facilita la adquisición de datos modelos de capacitación, predicciones y refinamiento de resultados, está disponible para el uso en computadores personales, pero es recomendado usarlo en su propio editor en la nube que es Colab.

Keras es un framework de alto nivel para el aprendizaje, escrito en Python y capaz de correr sobre los frameworks TensorFlow, por esta razón se usará para la presente investigación, pues facilita los procesos de experimentación rápida, y ya que al ejecutarse en TensorFlow, por consiguiente se puede ejecutar en Colab.

### Delimitación

En la presente investigación solamente se utilizará redes neuronales del tipo perceptrón multicapa, donde cabe mencionar que este no es el único tipo de red que existe, i.e., también se tiene Redes Neuronales Convolucionales (RNC), Redes Neuronales Recurrentes (RNR) o bien Redes de Base Radial (RBR) [8]. Así mismo, no se abordará el uso de técnicas d eoptimiación como lo son los algoritmos genéticos, y unicamente se limitará a explorar la mejora en rendimiento al tener más de dos capas duplocadas de pesos en la red con aprendizaje incremental. Así mismo, no se abordarán modelos como las redes profundas u otro conjunto de datos y se limitará el trabajo a lo antes mencionado.

#### Revisión de la Literatura

#### 7.1. Redes Neuronales Artificiales

Las redes neuronales artificiales (RNA) son modelos computacionales de la Inteligencia Artificial los cuales contienen simples unidades de procesamientos llamadas neuronas. Ellas se inspiran en el cerebro humano, tomando como base la conectividad entre neuronas y el aprendizaje que pueden tener. Un perceptron o neurona (artificial) solamente resuelve problemas lineales y tiene la siguiente forma:

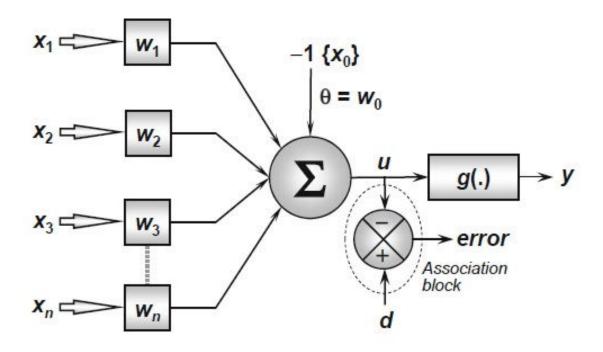


Figura 7.1: Red Neuronal Artificial Básica

Donde  $\Sigma$  es la representación matemática de la neurona.,  $x_1, x_2, \ldots, x_n$  son las variables de entrada a la red.  $w_1, w_2, \ldots, w_n$  son los pesos con los cuales se van a podnerar las entradas, es decir multiplicar cuando la información entra en la neurona. Posterior a multiplicar el peso por la entrada correspondiente, se suman todos esos valores  $w_1x_1 + w_2x_2 + w_3x_3$ .

Al revisar esta formula, se puede observar que se parece a la operación de una regresión la cual es:  $y = w_0 + w_i x_i$ , de esta forma, internamente la neurona realiza una regresión lineal. En su contraparte, el parámetro que permite a la neurona trazar una recta cruzando el eje y en el plano cartesiano (eje de las ordenadas), a ello se conoce como sesgo (del inglés bias), este valor se agrega a la conexión, el cual usualmente se le da un valor de 1. Agregando este nuevo valor a la fórmula, queda de la siguiente manera:  $y = \Sigma w_i x_i + w_0 b$ , donde b es el sesgo.

Un inconveniente del uso de una sola neurona para experimentos es que solo va a resolver ejercicios parecidos a la puerta lógica AND u OR.

Existen problemáticas de solo usar una sola neurona e.g problemas de tipo compuerta XOR.

Para solucionarlo se usan dos o más neuronas, además de la función de activación, que es la que permite pasar la informaicón de una neurona a otra, en un rango especificado, y la cual se describirá en la siguiente sección.

#### 7.1.1. Función de Activación

Dicho método se utiliza cuando el modelo de RNA contiene dos o más neuronas. Esta función lo que provoca es dar al modelo una salida no lineal, para eso la segunda fórmula presentada es distorcionada para quedar de la siguiente manera:  $f(w_1x_1+w_2x_2+w_3x_3+b_0)$  para el caso de 3 entradas.

Al hablar de funciones de activación se deben de comentar las más comunes, como lo es la función escalonada.

Tenemos la función escalonada, la cual se representa con la siguiente formula:

$$f(x) = \begin{cases} 0 : x < 0 \\ 1 : x \ge 0 \end{cases}$$

Su representación grafica queda de la siguiente manera:

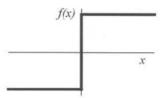


Figura 7.2: Función Escalonada

#### 7.2. Aprendizaje Incremental

Con el pasar de los años la tecnología a evolucionado, eso quiere decir que el Aprendizaje Automático se ha actualizado y que la cantidad de datos va aumentado con más frecuencia.

Se puede verificar como Üna tarea de aprendizaje es incremental si los ejemplos de entrenamiento usados para resolverla están disponibles en horas extras, generalmente uno a la vez" [5], si los resultados no se necesitan de manera urgente, este tipo de trabajos serán resueltos por algoritmos de aprendizaje no incremental.

Una área donde esto es de mucha utilidad es la *Robótica* porque este necesita estar en constante entrenamiento [5].

Dicha forma de aprender fue inspirada en la forma en que el humano aprende y esta más rápida, fue por esto que fue adoptada por el aprendizaje máquina.

Con el paso del tiempo se ha convertido en un paradigma del aprendizaje automático, aquí el aprendizaje toma el lugar de nuevos ejemplos para juntarlos y conforme van aprendiendo estos toman el lugar de los ejemplos ya aprendidos [4].

#### 7.2.1. Algoritmos de Aprendizaje Incremental

El algoritmo de aprendizaje incremental puede definirse como aquel que cumple los siguientes criterios: 1) Ser capaz de aprender y actualizarse con cada nuevo dato etiquetado o no etiquetado. 2) Conservar los conocimientos adquiridos previamente. 3) No debe requerir el acceso a los datos originales. 4) Generar una nueva clase o cluster cuando sea necesario. Dividir o fusionar los clusters cuando sea necesario. 5). Ser de naturaleza dinámica con el entorno cambiante [9].

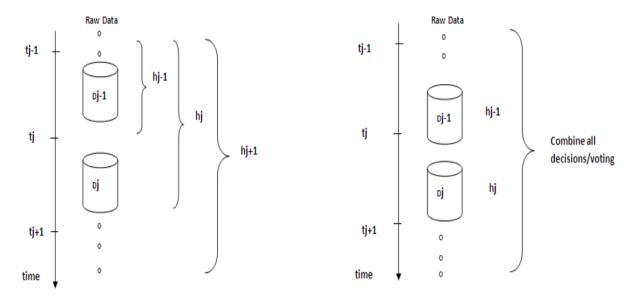


Figura 7.3: Dos enfoques tradicionales del aprendizaje incremental.

1 Metodología de acumulación de datos. 2 Metodología de aprendiza je por conjuntos.

Como se observa en la Figura 11, en el primer método, cuando se recibe una nueva porción de datos Dj, se descarta hj-1 y se desarrolla una nueva hipótesis hj, basada en todos los datos disponibles acumulados hasta el momento. Y en el segundo método, cuando se recibe una nueva porción de datos Dj, se desarrolla una única hipótesis nueva o un conjunto de hipótesis nuevas basadas en los nuevos datos. Por último, se puede utilizar un mecanismo de votación para combinar todas las decisiones de las diferentes hipótesis y obtener la predicción final.

Por ejemplo, si se deja que Dj-1 represente la porción de datos recibida entre el

tiempo tj-1 y tj, y que la hipótesis hj-1 se desarrolle sobre Dj-1.

El sistema aprenderá información de forma adaptativa cuando se reciba una nueva porción de datos Dj. En el método de aprendizaje por conjuntos, se desarrolla una nueva hipótesis hj o un conjunto de hipótesis H:h1, i1,2,...,M, basadas en los nuevos datos. A continuación, se utiliza el mecanismo de votación para combinar todas las decisiones de las diferentes hipótesis y llegar a la predicción final. La mayor ventaja de este enfoque es que no se requiere almacenar los datos vistos anteriormente, el conocimiento se ha almacenado en la serie de hipótesis desarrolladas a lo largo de la vida de aprendizaje.

Conocimiento en el momento t:

Dt es un trozo de datos con n instancias (i=1,...,n)

(xi,yi) es una instancia en el espacio de características m-dimensional X

 $Yi \in Y = 1,...,K$  clases

Función de distribución Df

Una hipótesis ht, desarrollada por los datos basados en Dt con Pt

La nueva entrada estará disponible en el momento (t+1)

Algoritmo de aprendizaje:

- 1. Encontrar la relación entre Dt y Dt+1
- 2. Actualizar la función de distribución inicial Dt+1
- 3. Aplicar la hipótesis ht a Dt+1 y calcular el pseudoerror de ht
- 4. Refinar la función de distribución para Dt+1
- 5. Se desarrolla una hipótesis por los datos basados en Dt+1 con Pt+1
- 6. Repetir el procedimiento cuando se reciba la siguiente porción del nuevo conjunto de datos.

Resultado: La hipótesis final.

## Metodología

El primer paso a realizar, es recrear el código mostrado en [1], el describe la implementación de una red neuronal multicapa usando el algoritmo de entrenamiento back-propagation en el lenguaje de programación Python. Así mismo, se utilizará el conjunto de datos de Optical Digits, en donde se tendrá que preprocesar los datos, para eliminar registros inválidos.

Posteriormente, se implementará una extensión del código, donde se experimentará con mas de dos capas de pesos duplicados para mejorar la tasa de olvido de información al momento de usar el aprendizaje incremental. Para ello se explorará incrementando gradualmente el número de capas de pesos duplicados.

Finalmente, cuando los resultados se obtengan se realizará una comparación, de los resultado del algoritmo base con los resultados del algoritmo extendido.

### Bibliografía

- [1] J. A. Bullinaria, "Evolved dual weight neural architectures to facilitate incremental learning.," in *IJCCI*, pp. 427–434, 2009.
- [2] B. Zhao, T. Wu, F. Fang, L. Wang, W. Ren, X. Yang, Z. Ruan, and X. Kou, "Prediction method of 5g high-load cellular based on bp neural network," in 2022 8th International Conference on Mechatronics and Robotics Engineering (ICMRE), pp. 148–151, IEEE, 2022.
- [3] L. A. C. Salazar, D. J. M. Aldana, and J. A. C. Montes, "Implementación de redes neuronales y lógica difusa para la clasificación de patrones obtenidos por un sónar," in 2013 II International Congress of Engineering Mechatronics and Automation (CI-IMA), pp. 1–6, IEEE, 2013.
- [4] Y. Liu, "Yuan liu incremental learning in deep neural networks," 2015.
- [5] C. G. Giraud-Carrier, "A note on the utility of incremental learning," AI Commun., vol. 13, pp. 215–224, 2000.
- [6] A.-J. Li, "An improved algorithm for incremental learning learn++," in 2008 International Conference on Wavelet Analysis and Pattern Recognition, vol. 1, pp. 310–315, IEEE, 2008.
- [7] R. Elwell and R. Polikar, "Incremental learning of concept drift in nonstationary environments," *IEEE Transactions on Neural Networks*, vol. 22, no. 10, pp. 1517– 1531, 2011.

- [8] P. Royo, "Qué son las redes neuronales y cuál es su aplicación en el marketing," 2021.
- [9] R. Ade and P. Deshmukh, "Methods for incremental learning: a survey," *International Journal of Data Mining & Knowledge Management Process*, vol. 3, no. 4, p. 119, 2013.