République Algérienne Démocratique et Populaire
الجمهورية الجزائرية الديمقراطية الشعبية
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
وزارة التعليم العالي و البحث العلمي

ECOLE NATIONALE SUPÉRIEURE D'INFORMATIQUE

المدرسة الوطنية العليا للإعلام الآلي
(المعهد الوطني للتكوين في الإعلام الآلي سابقا)
École nationale Supérieure d'Informatique
ex. INI (Institut National de formation en Informatique)

Mémoire de fin d'études

pour l'obtention du diplôme d'Ingénieur d'État en Informatique

Option : Systèmes Informatiques (SQ)

Optimisation des architectures en deep learning en utilisant les techniques de plongement de graphes

Réalisé par :
M. Kacemi Souhib
M. Taibi Mohamed Kamel Eddine

Encadré par :
M. Ait Ali Yahia Yacine (ESI)
Mme. Amrouche Karima (ESI)

Soutenu le 20 Septembre 2023, Devant le jury composé de :

Mme. Fatima Benbouzid-Si Tayeb :	ESI	- Président
M. Hachemi Nabil Dellys :	ESI	- Rapporteur
Mme. Sara Ghorab :	ESI	- Examinateur

Promotion : 2022/2023

Dédicace

“

À mes chers parents,

À mes chers frères et soeurs et leurs enfants,

À tous mes amis,

À mes professeurs,

Merci.

”

- Souhib

Remerciements

Nous tenons à exprimer nos profondes gratitudes pour tous ceux qui ont contribué à la réalisation de ce mémoire de master.

Nos sincères remerciements vont à nos directeurs de mémoire qui nous ont offert un encadrement de qualité, un soutien inestimable et des conseils judicieux tout au long de ce parcours académique.

Nous tenons également à remercier tous les enseignants qui nous ont prodigué leur savoir et leurs compétences pour que nous puissions réussir dans nos études.

Nous exprimons également nos profonds remerciements à **M. Ali TFAILY** et **M.Souhib KACEMI** pour leur support et leurs orientations.

Nos remerciements s'adressent également à nos familles et nos amis pour leur soutien, leur encouragement et leur amour indéfectibles.

Enfin, nous sommes reconnaissants envers toutes les personnes qui ont contribué, de près ou de loin, à l'aboutissement de ce travail de recherche. Merci infiniment pour votre précieuse aide et vos précieux conseils tout au long de cette aventure.

Résumé

La maintenance prédictive est cruciale aujourd'hui pour anticiper les pannes avant qu'elles ne surviennent, permettant ainsi de réduire les coûts et le temps de maintenance. Les moteurs électriques, largement utilisés dans l'industrie, les transports et les usines, sont sujets à de nombreux défauts électriques et mécaniques, rendant leur maintenance coûteuse mais indispensable.

Ce mémoire explore l'application du machine learning pour la maintenance prédictive des moteurs électriques. La qualité des données est un élément clé du machine learning. Pour enrichir notre jeu de données sur différents moteurs présents sur le marché, nous utilisons l'intelligence artificielle générative pour créer des données similaires aux données réelles, sous forme de séries temporelles. Des techniques avancées telles que les auto-encodeurs variationnels (VAE), les réseaux adverses génératifs (GAN) et les grands modèles de langage (LLM) sont employées pour générer ces données.

Le travail réalisé a permis de produire des séries temporelles très proches des données réelles, lesquelles sont utilisées par un modèle de classification pour prédire de manière fiable si un moteur va tomber en panne ou non. Les résultats obtenus démontrent que notre solution est capable de générer des données de haute qualité et de prédire efficacement les pannes des moteurs électriques, offrant ainsi une approche prometteuse pour la maintenance prédictive dans divers secteurs industriels.

Mots clés : Apprentissage profond, Apprentissage automatique, Réseaux neuronaux profonds, Maintenance prédictive, Séries temporelles, Réseaux adverses génératifs (GAN), Auto-encodeurs variationnels (VAE), Grands modèles de langage (LLM)

Abstract

Predictive maintenance is crucial today for anticipating failures before they occur, thereby reducing costs and maintenance time. Electric motors, widely used in industry, transportation, and factories, are subject to numerous electrical and mechanical faults, making their maintenance costly but indispensable.

This thesis explores the application of machine learning for the predictive maintenance of electric motors. Data quality is a key element of machine learning. To enrich our dataset on various motors available on the market, we use generative artificial intelligence to create data similar to real data, in the form of time series. Advanced techniques such as variational autoencoders (VAE), generative adversarial networks (GAN), and large language models (LLM) are employed to generate these data.

The work carried out has produced time series very close to real data, which are used by a classification model to reliably predict whether a motor will fail or not. The results obtained demonstrate that our solution is capable of generating high-quality data and effectively predicting electric motor failures, thus offering a promising approach for predictive maintenance in various industrial sectors.

Keywords : Deep learning, Machine learning, Deep neural networks, Predictive maintenance, Time series, Generative adversarial networks (GAN), Variational autoencoders (VAE), Large language models (LLM)

Table des matières

Table des figures

Liste des tableaux

Liste des sigles et acronymes

AI	*Artificial Intelligence*
GenAI	*Generative Artificial Intelligence*
ReLU	*Rectified Linear Unit*
ANN	Artificial Neural Network
DL	*Deep Learning*
ML	*Machine Learning*
GAN	*Generative Adversarial Networks*
LLM	*Large language models*
VAE	*Variational Autoencoders*
CNN	*Convolutional Neural Networks*
RNN	*Recurrent Neural Network*
LSTM	*Long Short-Term emory*
MDP	*Markov Decision process*
NLP	*Natural language Processing*
GD	*Gradient Descent*
MLP	*MultiLayer Perceptron*

Introduction générale

L'apprentissage profond, ou deep learning, est une branche de l'intelligence artificielle (IA) qui a transformé de nombreux secteurs et industries, en particulier ces dernières années. Grâce à ses capacités avancées, l'apprentissage profond a permis des avancées significatives dans des domaines tels que la reconnaissance d'image, la compréhension du langage naturel et la génération de données. En tant que composant essentiel de l'intelligence artificielle générative, l'apprentissage profond est utilisé pour créer divers types de données, y compris des textes, des images, des données tabulaires et des données séquentielles.

Les architectures d'intelligence artificielle générative, telles que les GANs (Generative Adversarial Networks), les LLMs (Large Language Models) et les autoencodeurs variationnels (VAE), jouent un rôle crucial dans la génération de données synthétiques. Ces modèles sont particulièrement efficaces pour augmenter les ensembles de données existants, ce qui est essentiel pour entraîner d'autres modèles de machine learning avec des ensembles de données plus diversifiés et représentatifs.

Un domaine d'application particulièrement intéressant est celui des moteurs électriques, qui sont largement utilisés aujourd'hui et jouent un rôle crucial dans divers secteurs de l'industrie, notamment le transport. Ces moteurs, provenant de multiples fabricants et marques, nécessitent une maintenance prédictive pour garantir leur bon fonctionnement et prolonger leur durée de vie. Cependant, la diversité des marques et des modèles de moteurs pose un défi en termes de collecte de données suffisantes et variées pour chaque type de moteur.

Dans ce contexte, l'IA générative peut être utilisée pour générer des données synthétiques qui couvrent un large éventail de moteurs électriques. En généralisant sur toutes les variétés de moteurs existants, l'IA générative permet d'augmenter les ensembles de données, ce qui est crucial pour entraîner des modèles de classification et de prédiction plus précis et robustes. Ces modèles peuvent ensuite être utilisés pour effectuer une maintenance prédictive efficace, réduisant ainsi les temps d'arrêt et les coûts de maintenance.

Ce travail se concentrera sur l'application de l'IA générative pour la génération de données de type séries temporelles. Nous viserons à généraliser ces données pour qu'elles représentent une large gamme de moteurs électriques. L'objectif final est de faciliter la maintenance prédictive de ces moteurs en utilisant des ensembles de données augmentés et diversifiés, permettant ainsi d'améliorer la fiabilité et l'efficacité des systèmes de maintenance.

Dans cet article, nous présentons les méthodes d'intelligence artificielle générative dans le contexte de l'augmentation de dataset pour la maintenance prédictive. Nous utilisons notamment les réseaux adversatifs génératifs (GAN) et les modèles de diffusion. Les GAN, qui sont généralement composés d'un générateur et d'un discriminateur, permettent de générer des données synthétiques où le générateur crée des données et le discriminateur évalue la qualité de ces données. Par ailleurs, nous abordons les modèles de diffusion qui génèrent des données à partir d'un bruit gaussien. Nous détaillons les différentes étapes nécessaires pour générer des séries temporelles et discutons des méthodes d'évaluation pour apprécier la qualité des données générées par ces modèles. En outre, nous appliquons des techniques de traitement du signal pour visualiser les données dans le domaine fréquentiel.

Nous commençons par une revue de la littérature sur l'apprentissage profond et les différentes architectures existantes. Nous y présentons également des modèles génératifs tels que les autoencodeurs variationnels (VAE), les GAN et les modèles de langage de grande taille (LLM). Le dernier chapitre de cette revue bibliographique est consacré aux bases de la maintenance prédictive, aux composants des moteurs électriques, ainsi qu'aux techniques de traitement du signal comme la transformation de Fourier rapide (FFT).

partie I

Etude bibliographique

Chapitre 1

Apprentissage profond

1.1 Introduction

L'apprentissage profond (*deep learning* en anglais) est une branche de l'intelligence artificielle (IA) qui s'intéresse à la résolution des problèmes intuitifs, c'est-a-dire des tâches qui sont faciles à réaliser par les humains mais difficiles à décrire formellement. Ce sont des problèmes qui semblent automatiques, comme la reconnaissance des mots parlés ou des visages dans les images. L'apprentissage profond permet aux ordinateurs d'apprendre des concepts complexes en rassemblant de l'expérience. Cela permet d'éviter la spécification formelle des connaissances dont l'ordinateur a besoin [Goodfellow et al. 2016].

L'apprentissage profond utilise des réseaux de neurones profonds pour résoudre ces problèmes. Ces réseaux sont des modèles computationnels qui imitent le fonctionnement du cerveau humain [McCulloch et al. 1943, Rosenblatt 1958]. Ils sont constitués de plusieurs couches de neurones artificiels cachées qui traitent les données d'entrée.

Il existe trois grandes catégories d'apprentissage automatique : *supervisé*, *non-supervisé* et *semi-supervisé*. Dans l'apprentissage supervisé, on utilise un ensemble de données étiquetées, tandis que dans l'apprentissage non-supervisé, on ne dispose pas d'un ensemble de données étiquetées. L'apprentissage semi-supervisé est une combinaison d'apprentissage supervisé et non-supervisé. Dans l'apprentissage semi-supervisé, un ensemble de données est étiqueté, mais la majorité des données sont non étiquetées [Goodfellow et al. 2016, Bishop 2016].

Dans l'apprentissage profond, plusieurs types d'architecture existent, chacune adaptée à des tâches spécifiques. Parmi les plus courants, on trouve : les *réseaux de neurones convolutionnels* (CNN), les *réseaux de neurones récurrents* (RNN), les *réseaux de neurones générateurs adversaires* (GANs) et les *réseaux de neurones de transformation* (Transformer) [Goodfellow et al. 2016].

Dans ce chapitre, nous allons expliquer brièvement les différentes notions en relation avec l'apprentissage profond, telles que les couches du réseau, les fonctions d'activation, les types de réseaux, les connexions et les poids, le processus d'apprentissage et les types d'apprentissage.

1.2 Réseau de neurones artificiels

Un réseau de neurones artificiels (*Artificial Neural Network* en anglais) est un modèle de traitement de l'information construit de couches de neurones interconnectées qui traitent les données d'entrée en les transmettant à travers des poids de connexion qui peuvent être ajustés par un processus d'apprentissage [Aggarwal 2018]. Ce réseau s'inspire du fonctionnement des neurones biologiques du cerveau.

Chaque neurone dans les couches cachées du réseau reçoit des signaux d'entrée à partir des neurones précédents, les somme, et les transmet aux neurones de la couche suivante à travers une fonction d'activation. Les réseaux de neurones peuvent avoir plusieurs couches cachées, qui permettent de modéliser des relations non linéaires complexes entre les données d'entrée et de sortie. Ces réseaux neuronaux peuvent compter jusqu'à 150 couches, d'où le nom "profond". [Goodfellow et al. 2016].

Les réseaux de neurones peuvent faire des prédictions précises sur des données nouvelles qui ne sont pas vues pendant l'entraînement. Ils peuvent donc apprendre des relations complexes entre les données d'entrée et de sortie, ce qui leur permet de généraliser et de prédire les sorties pour de nouvelles données. Cependant, la qualité des prédictions dépend fortement de la qualité et de la quantité des données d'entraînement. Si les données d'entraînement sont mauvaises ou insuffisantes, les prédictions pour de nouvelles données peuvent être inexactes [Goodfellow et al. 2016].

Les réseaux de neurones artificiels sont généralement caractérisés par :

- **Traitement parallèle** : les réseaux de neurones sont capables d'effectuer plusieurs calculs simultanément. Cela les rend bien adaptés aux tâches nécessitant des calculs à grande échelle, telles que la reconnaissance d'images, la reconnaissance de la parole, et la traduction automatique [Goodfellow et al. 2016].
- **Apprentissage hiérarchique** : les modèles d'apprentissage profond sont généralement structurés en plusieurs couches . Chaque couche possède un niveau d'abstraction différent. Cela permet au modèle d'apprendre des motifs et des relations complexes dans les données, et plus le réseaux est profond, plus la capacité du modèle à découvrir ces relations est grande [Goodfellow et al. 2016].
- **Grandes quantités de données** : les modèles d'apprentissage profond nécessitent de grandes quantités de données pour s'entraîner efficacement. En effet, les modèles comportent un grand nombre de paramètres qui ne peuvent être réglés qu'à partir d'une grande quantité de données [Goodfellow et al. 2016].

1.3 Connexions et poids

Un réseau de neurones est constitué de nœuds et des connexions entre eux [Aggarwal 2018]. Chaque nœud possède un **ensemble d'entrées** (qui sont souvent les sorties des nœuds de la couche précédente), un **poids** et une valeur ajoutée appelée le **biais**. Dans

les réseaux neuronaux, le biais est un paramètre supplémentaire qui est ajouté à chaque neurone pour ajuster sa sortie. Il permet au réseau de déplacer la fonction d'activation horizontalement[Goodfellow et al. 2016].

Lorsque des signaux entrent dans un neurones, chaque signal est multiplié par le poids associé à son entrée, puis additionné avec les autres résultats. Le biais est ensuite ajoute au résultat final et ce dernier est transmet vers les entrées des neurones de la couche suivante en passant par une fonction d'activation (voir la figure 1.1) [McCulloch et al. 1943].

On peut dire que la taille du réseau de neurones est définie par le nombre de ses paramètres et le nombre de ses couches, qui sont des variables appelées **hyperparamètres**. Par contre, les poids et le bais sont des paramètres entraînables. Au début de l'entraînement, on affecte à ces deux paramètres des valeurs aléatoires, et au fur et à mesure, les valeurs de ces deux paramètres sont ajustées et modifiées afin d'obtenir les bonnes valeurs [Aggarwal 2018, Goodfellow et al. 2016].

1.4 Fonction d'activation

Un neurone dans le réseau artificiel calcule la somme pondérée de ses entrées et la valeur résultante de cette opération passe par une fonction appelée **fonction d'activation** (ou **fonction de transfert**) avant d'être transférée vers les neurones de la couche suivante. La sortie de neurone est donc calculée selon la formule 1.1 [McCulloch et al. 1943].

$$y = f\left(\sum_{i=1}^{n} w_i x_i + b\right) \tag{1.1}$$

Où :

w_i : le poids associé à l'entrée i
x_i : la valeur associée à l'entrée i
n : le nombre total d'entrées
b : le biais (constante entraînable ajoutée)
f : la fonction d'activation
y : la sortie du neurone

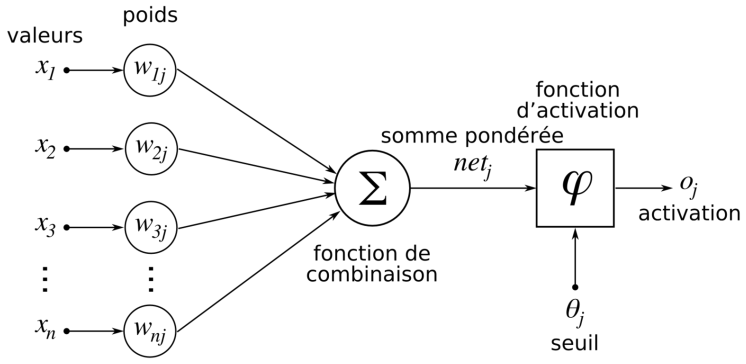

FIG. 1.1 : Le fonctionnement d'un neurone artificiel [McCULLOCH et al. 1943].

La fonction d'activation est utilisée pour introduire de la non-linéarité dans le modèle, permettant ainsi de modéliser des relations complexes entre les données d'entrée et de sortie [GOODFELLOW et al. 2016]. Les propriétés d'une fonction d'activation doivent être vérifiées dans un problème d'apprentissage profond. Ces propriétés sont :

- **Non-linéarité** : lorsque la fonction d'activation est non linéaire, il est possible de prouver qu'un réseau neuronal à deux couches peut approximer n'importe quelle fonction continue sur un domaine compact à une précision arbitraire, ce que l'on appelle le **théorème d'approximation universelle** [GOODFELLOW et al. 2016].
- **L'intervalle** : lorsque l'intervalle des valeurs est fini, l'apprentissage de manière générale est plus efficace.
- **Différentiabilité** : cette propriété est importante quand les méthodes d'optimisation sont basées sur le gradient, car elles cherchent à optimiser l'apprentissage en se basant sur la différentiabilité de la fonction.
- **Monotonie** : Une fonction d'activation est monotone si sa sortie augmente (ou diminue) à mesure que son entrée augmente. Cela garantit que le gradient de la fonction est toujours positif ou négatif, simplifiant ainsi l'apprentissage.
- **Efficacité en termes de calcul** : les fonctions d'activation doivent être efficaces en termes de calcul, afin que le réseau puisse être utilisé dans des applications en temps réel, sans ralentir le processus de l'apprentissage.

Parmi les fonctions d'activation les plus couramment utilisées dans les réseaux de neurones, on peut citer :

- **La fonction Sigmoïde** : si la probabilité d'un résultat est comprise entre 0 et 1, la fonction sigmoïde est le meilleur choix. Cette fonction est largement utilisée grâce à son intervalle et sa différentiabilité.

$$\sigma(x) = \frac{1}{1 + e^{-x}} \tag{1.2}$$

- **La fonction Unité linéaire rectifiée (ReLU)** : c'est une fonction qui possède une dérivée et permet la rétropropagation (backpropagation) tout en étant efficace

sur le plan informatique. Cependant, elle n'active pas les neurones en même temps, et c'est considéré comme désavantage pour cette fonction.

$$ReLU(x) = \max(0, x) \tag{1.3}$$

- **La fonction Tangente hyperbolique (Tanh)** : cette fonction est très identique à la fonction d'activation sigmoïde. Sa plage de sortie est comprise entre -1 et 1. Avec cette fonction, plus l'entrée est grande, plus la valeur de sortie sera proche de 1, et plus l'entrée est petite, plus la sortie sera proche de -1.

$$tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \tag{1.4}$$

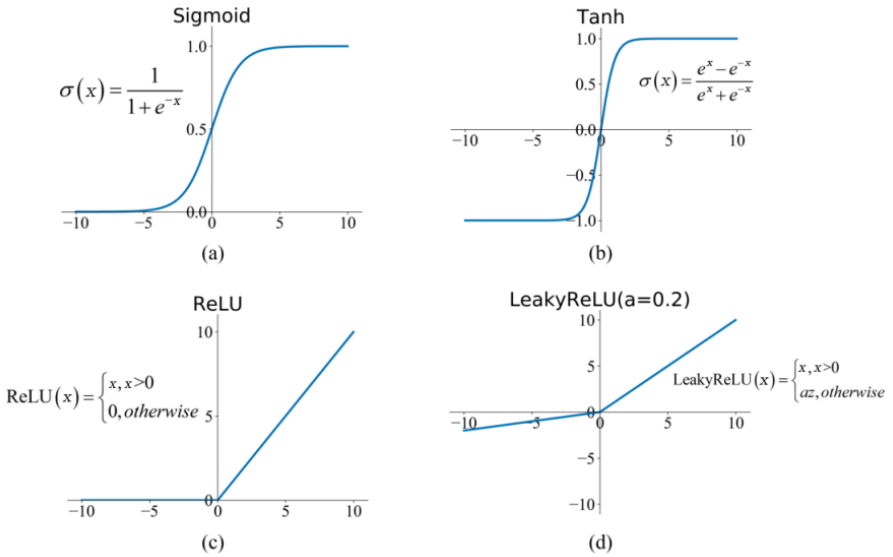

FIG. 1.2 : Les fonctions d'activations couramment utilisées [Junxi FENG et al. 2019].

1.5 Couches dans un réseau de neurones

Une couche (*layer* en anglais) est une succession verticale des neurones. Mathématiquement, elle est vue comme une composition de deux fonctions h et g où g est une fonction linéaire et h une fonction d'activation non linéaire. Cette composition de fonction est définie par l'équation 2.2 [GOODFELLOW et al. 2016].

$$y = h(g(x) + b) \tag{1.5}$$

Une couche intermédiaire est donc l'ensemble des nœuds verticaux qui sont connectés à la couche précédente et à la couche suivante. La connectivité entre les couches détermine la manière dont les informations circulent sur le réseau. La façon de connexions des nœuds entre eux est différente d'une architecture à une autre [GOODFELLOW et al. 2016], et c'est ce qui détermine le type d'une couche :

- **Couche entièrement connectée** : tous les neurones d'une couche sont connectés à tous les neurones de la couche suivante.
- **Couche partiellement connectée** : certains neurones ne sont pas connectés aux neurones de la couche suivante.

Les couches sont le composant principal des réseaux de neurones. Elles ont plusieurs caractéristiques qui définissent leur comportement et influencent les performances globales du réseau. Ces caractéristique sont les suivants :

- **La matrice de poids** : Dans une couche d'un réseau de neurones, la matrice de poids est une matrice de paramètres qui représente les connexions entre les neurones d'entrée et les neurones de sortie de cette couche [Aggarwal 2018]. Elle définie la puissance des connexions entre les neurones des différentes couches. Chaque ligne de la matrice correspond aux poids associés à un neurone d'entrée particulier, et chaque colonne correspond aux poids associés à un neurone de sortie particulier,La taille de la matrice de poids dépend du nombre de neurones d'entrée et du nombre de neurones de sortie dans la couche.

  La forme générale de la matrice de poids dans un réseau de neurones peut être exprimée comme suit :

$$W = \begin{bmatrix} w_{1,1} & w_{1,2} & \dots & w_{1,m} \\ w_{2,1} & w_{2,2} & \dots & w_{2,m} \\ \dots & \dots & \dots & \dots \\ w_{n,1} & w_{n,2} & \dots & w_{n,m} \end{bmatrix} \tag{1.6}$$

  où $w_{i,j}$ représente le poids de la connexion entre le neurone i de la couche actuelle et le neurone j de la couche suivante et *(n, m)* représente la dimension de la matrice.

  La matrice de poids est crucial pour la performance du réseau neuronal, puisqu'elle détermine la capacité du réseau d'apprendre et généraliser les motifs a partir des données en entrées.

- **Type de couche** : Les couches forment les blocs de construction de base des réseaux de neurones. Elle permettent d'effectuer des calculs complexes et d'apprendre des relations qui existent entre données d'entrée et de sortie. Dans le réseau neuronal, il existe trois types de couches différents :
  - **Couche d'entrée** : Cette couche est responsable de la réception des données d'entrée et de leur transmission à la couche suivante (la première couche parmi les couches cachées).
  - **Couche cachée** : Cette couche traite les entrées de la couche précédente et génère des valeurs de sortie qui sont transmises à la couche suivante. Les réseaux de neurones peuvent avoir plusieurs couches cachées, chacune effectuant différentes opérations sur les entrées.
  - **Couche de sortie** : Cette couche produit la sortie finale du réseau de neurones, qui peut être une classification, une régression ou un autre type de prédiction.

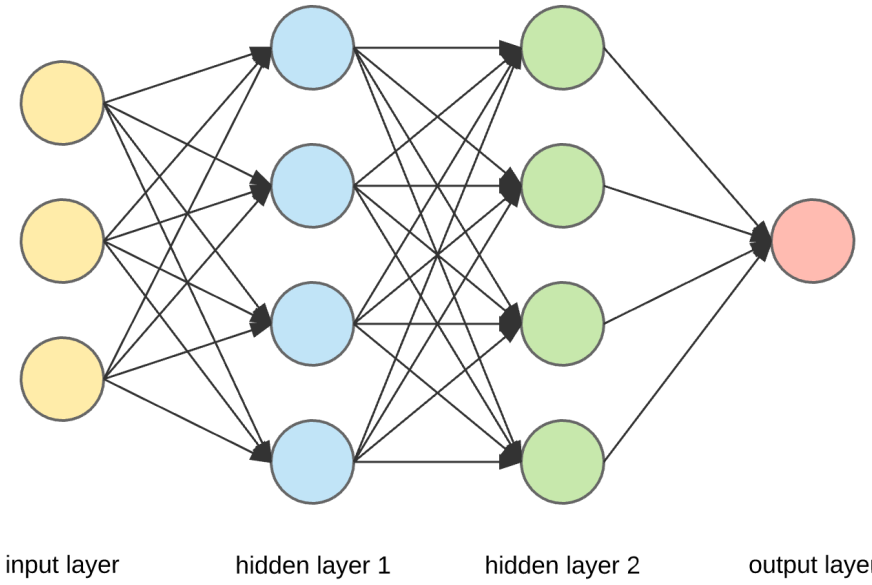

FIG. 1.3 : Schéma simple d'un réseau de neurones feedforward [MUNIASAMY et al. 2020].

1.6 Types de réseaux de neurones

Dans l'apprentissage profond, il existe plusieurs classes de réseaux de neurones, chacune avec sa propre architecture, caractéristiques, algorithme d'apprentissage et application. Dans cette section, nous allons présenter les différentes architecture de réseaux de neurones.

1.6.1 Réseaux feedforward

Les réseaux feedforward (ou réseaux entièrement connectés) sont un des types de réseau de neurones artificiels où les informations circulent dans une seule direction, de l'entrée vers la la sortie [GOODFELLOW et al. 2016]. Ils sont composés d'une succession de couches interconnectées, où chaque neurone d'une couche est connecté aux neurones de la couche suivante. Dans un Réseau de ce type, les données sont introduites dans la première couche du réseau (couche d'entrée), puis elles traversent plusieurs couches cachées avant d'atteindre la couche de sortie (*la figure 1.4 est un schéma simple d'un réseau feedforward*).

Les réseaux feedforward sont indépendants de la structure, c'est-à-dire il n'existe pas d'hypothèses particulières à faire sur l'entrée, ce qui les rend largement applicables. Cependant, ils ont tendance à être moins performants que les réseaux à usage spécial. Les réseaux feedforward sont couramment utilisés dans les applications d'apprentissage supervisé. Ils peuvent également être utilisés dans des applications d'apprentissage non supervisé [AGGARWAL 2018].

1.6.2 Réseaux de neurones récurrents (RNN)

Les réseaux de neurones récurrents (RNN) sont des architectures conçus pour fonctionner avec des données séquentielles, telles que : la reconnaissance de la parole, la recon-

naissance de la voie, l'analyse de séries chronologiques et le traitement du langage naturel [Goodfellow et al. 2016]. Les principales caractéristiques des RNN sont :

- **Connexions récurrentes** : Les connexions dans les réseaux récurrents sont des connexions récurrentes qui permettent à l'information de persister au fil du temps. Cela signifie que la sortie du réseau à un pas de temps est réinjectée en entrée du réseau au pas de temps suivant.
- **État caché** : Les réseaux RNN maintiennent un état caché qui représente la mémoire du réseau. Cet état est mis à jour à chaque pas de temps en fonction de l'entrée courante et de l'état caché précédent.
- **RNN bidirectionnels** : Les réseaux RNN bidirectionnels traitent la séquence d'entrée dans les sens avant et arrière, ce qui permet de capturer le contexte des pas de temps passés et futurs.

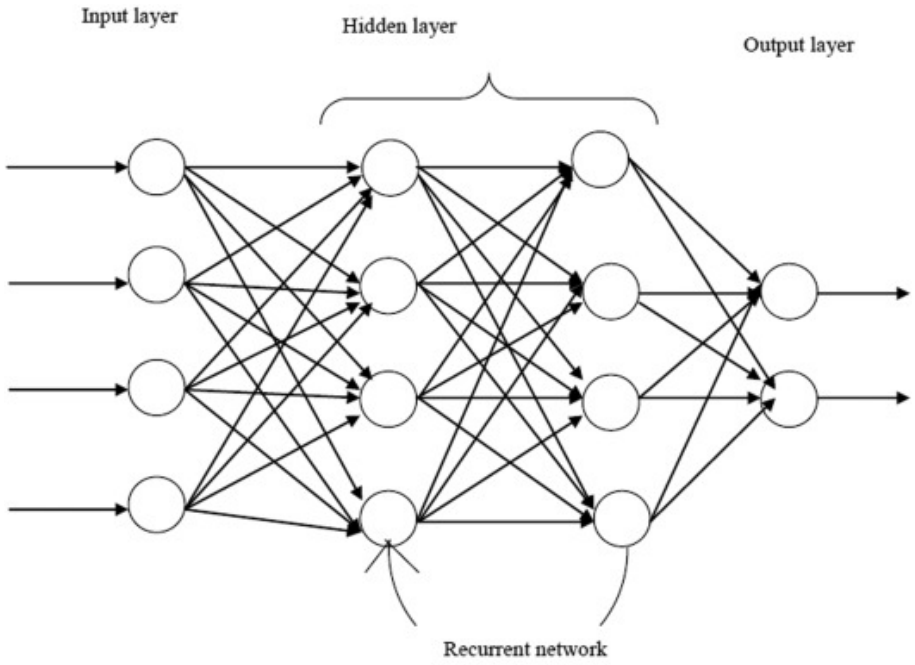

Fig. 1.4 : Exemple d'un réseau de neurones récurrent [Kumaraswamy 2021].

La capacité à conserver une mémoire des pas de temps précédents et à gérer les dépendances à long terme rend les réseaux récurrents utiles pour les tâches qui nécessitent de comprendre le contexte de la séquence d'entrée.

Réseaux récurrents à mémoire courtet long terme (LSTM)

Les réseaux de neurones récurrents à mémoire longue à court terme, ou Long Short-Term Memory (LSTM) en angalis , représentent une amélioration significative des réseaux de neurones récurrents traditionnels, conçue pour résoudre les problèmes d'évanouissement et d'explosion du gradient. Introduits par Hochreiter et Schmidhuber en 1997 dans [Hochreiter et al. 1997], les réseaux LSTM intègrent des cellules mémoire capables

de stocker et de conserver des informations tout au long du traitement d'une séquence. Ces cellules mémoire permettent de transporter des informations importantes grâce à trois types de portes : la porte d'entrée, la porte de sortie et la porte d'oubli. Ces portes jouent un rôle crucial en décidant quelles informations doivent être ajoutées, conservées ou oubliées.

Porte d'Entrée : décide quelles nouvelles informations doivent être stockées dans la cellule de mémoire. Elle est définie par :

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i) \tag{1.7}$$

où σ représente la fonction sigmoïde, W_i est le poids associé à la porte d'entrée, h_{t-1} est l'état caché précédent, x_t est l'entrée actuelle, et b_i est le biais.

Porte d'Oubli : contrôle quelles informations anciennes doivent être effacées de la cellule de mémoire. Elle est définie par :

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f) \tag{1.8}$$

où σ est la fonction sigmoïde, W_f est le poids associé à la porte d'oubli, h_{t-1} est l'état caché précédent, x_t est l'entrée actuelle, et b_f est le biais.

Porte de Sortie : décide quelles informations de la cellule de mémoire sont utilisées pour calculer l'état caché actuel. Elle est définie par :

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o) \tag{1.9}$$

où σ est la fonction sigmoïde, W_o est le poids associé à la porte de sortie, h_{t-1} est l'état caché précédent, x_t est l'entrée actuelle, et b_o est le biais.

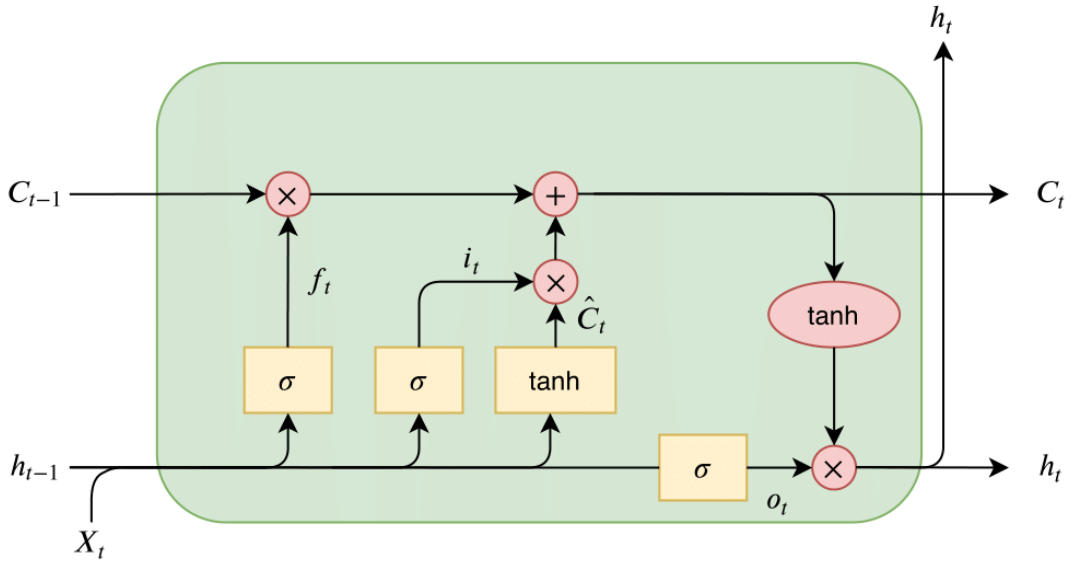

FIG. 1.5 : Architecture d'un bloc LSTM [FAWAZ et al. 2019].

1.6.3 Réseaux de neurones convolutifs (CNN)

L'architecture des réseaux de neurones convolutifs (CNN) est une architecture spéciale qui est bien adaptée à la tâche de classification d'images. Ces réseaux comportent trois types de couches : **convolutives**, **pooling** et **d'activation** [Goodfellow et al. 2016].

Les couches convolutives sont appliquées à l'image en entrée pour l'extraction des caractéristiques importantes de l'image. Ensuite, ces dernières traversent des couches d'activation, qui sont responsables de l'application d'une fonction d'activation non-linéaire à ces caractéristiques. Les couches d'activation sont suivies de couches de pooling qui réduisent la taille de l'image. Les couches de pooling sont elles même suivies par une couche entièrement connectée qui donne la classification de l'image (la sortie finale du modèle) [Goodfellow et al. 2016].

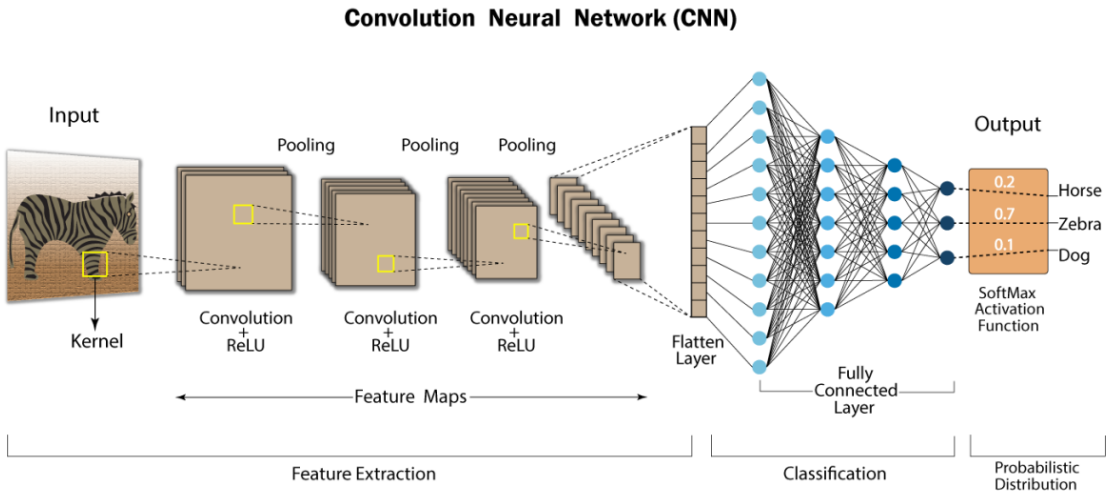

Fig. 1.6 : Le fonctionnement d'un réseau neuronal convolutif [Alharbi et al. 2021].

Couche convolutive

Une couche convolutive est un élément constitutif des réseaux de neurones convolutifs (CNN). Elle est utilisé pour extraire des caractéristiques à partir de données d'entrée, souvent des images, en appliquant un ensemble de filtres convolutifs appris à l'entrée.

Dans une couche convolutive, chaque filtre est convolué avec l'entrée pour produire une carte de caractéristiques. Cette opération est faite en glissant le filtre sur l'entrée et en calculant le produit scalaire à chaque position. Généralement, une couche convolutive possède trois hyperparamètres qui doivent être définis : **le nombre de filtres**, **la taille des filtres** et **la Stride**. Le nombre de filtres détermine le nombre de cartes d'entités produites, tandis que la taille des filtres détermine la taille du champ récepteur de chaque carte d'entités. La stride détermine la quantité de décalage du filtre à chaque étape.

Les couches convolutives sont suivies de fonctions d'activation,et de couches de pooling. Ces dernières permettent de réduire les dimensions spatiales des cartes d'entités. Plusieurs

couches convolutives peuvent être empilées pour créer un réseau neuronal convolutif profond.Les couches convolutives sont particulièrement efficaces pour traiter des images et d'autres données de grande dimension avec une structure spatiale, car elles peuvent apprendre automatiquement à détecter les caractéristiques importantes, telles que les bords, les coins et les textures [Kimura et al. 2019, Goodfellow et al. 2016].

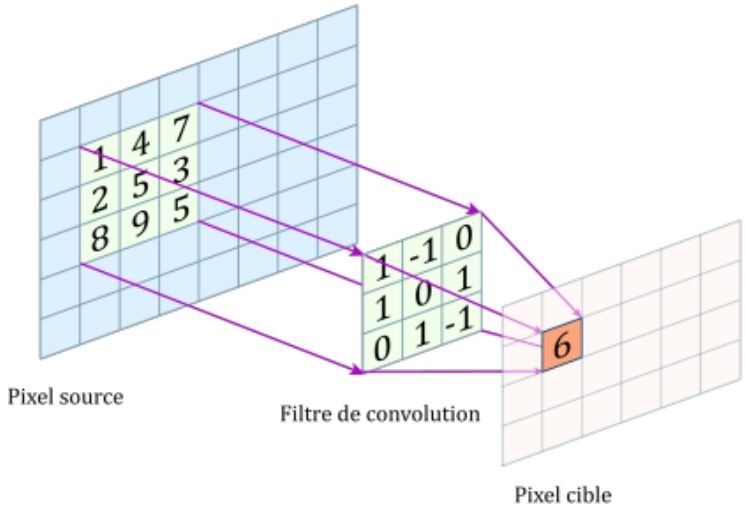

Fig. 1.7 : Exemple du fonctionnement d'une couche convolutive [Kimura et al. 2019].

Couche pooling

Le pooling est une opération quie est utilisée pour sous-échantillonner les cartes de caractéristiques résultantes des couches convolutives en réduisant leurs dimensions spatiales tout en conservant les informations importantes. Parmi les types de pooling, on trouve le pooling maximal et le pooling moyen [Goodfellow et al. 2016].

Dans le pooling maximal, la valeur maximale de chaque région est sélectionnée comme valeur représentative, tandis que dans le pooling moyen, la valeur moyenne est calculée à la place. Il en résulte une carte d'entités plus petite avec une résolution spatiale réduite, qui peut être traitée plus efficacement par les couches suivantes du réseau.

Cependant, le pooling excessive peut entraîner une perte d'informations spatiales importantes. Il est donc important d'équilibrer la quantité de pooling avec les besoins du réseau et la nature de la tâche à accomplir.

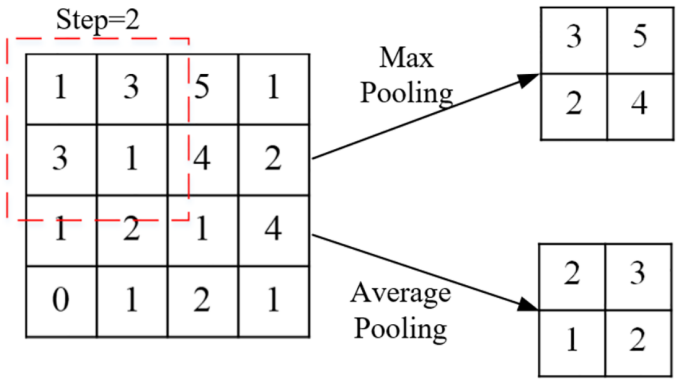

FIG. 1.8 : Exemples de pooling maximal et pooling moyen [HU et al. 2022].

1.6.4 Réseaux résiduels (ResNet)

Les réseaux résiduels ont été conçus par Microsoft afin de résoudre le problème des gradients qui disparaissent dans les réseaux de neurones très profonds, ce qui peut rendre l'entraînement difficile et diminuer significativement les performances du réseau.

Un ResNet est composé d'une ensemble de blocs résiduels, qui sont constitués de plusieurs couches avec des connexions de raccourci qui contournent une ou plusieurs couches. Ces raccourcis permettent aux gradients de circuler plus facilement à travers le réseau et évitent qu'ils ne disparaissent à mesure que le réseau devient plus profond [HE et al. 2016].

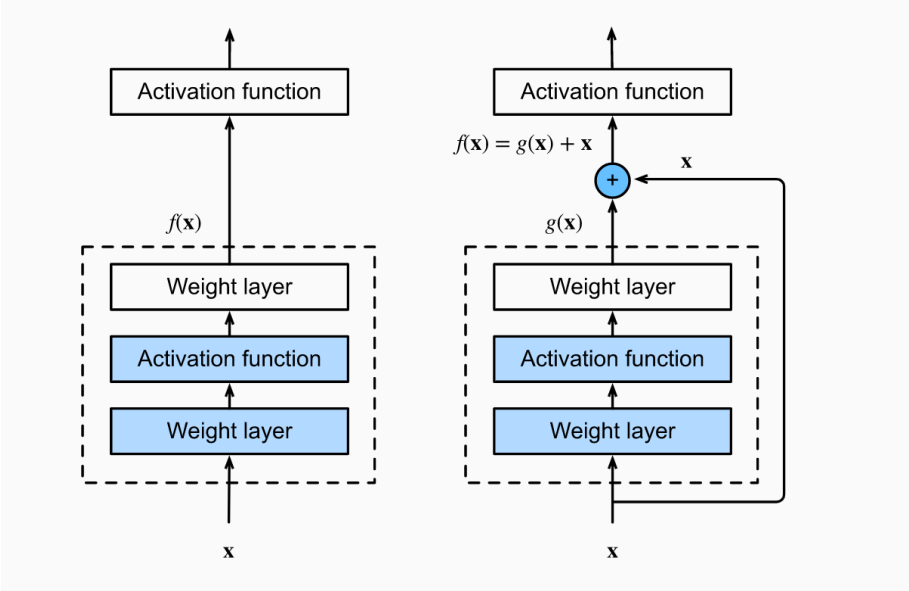

FIG. 1.9 : Un bloc régulier (gauche) et un bloc résiduel (droite) [DONG et al. 2022].

ResNet est très efficace dans les tâches de vision par ordinateur, telles que la classification d'images, la détection d'objets et la segmentation. Il a joué un rôle important dans l'avancement de l'état de l'art en apprentissage profond et en vision par ordinateur, et continue d'être un domaine de recherche actif.

1.6.5 Réseaux de neurones en graphe (GNN)

Les réseaux de neurones en graphe (GNN) sont conçus pour traiter des données structurées sous forme de graphes. Les GNN sont capables d'apprendre et de faire des prédictions sur les données du graphe en propageant les informations à travers les bords et les nœuds du graphe [Zhou et al. 2020].

L'idée de base derrière les GNN est d'utiliser un ensemble de paramètres entraînables pour transformer les caractéristiques de chaque nœud dans le graphe en fonction des caractéristiques de ses nœuds voisins (plongement de graphe). Ce processus est répété de manière itérative sur plusieurs couches du réseau, permettant au GNN d'apprendre des motifs et des relations complexes à partir des données [Zhou et al. 2020].

Parmi les tâches réalisées par ce type de réseaux :

- **Classification des graphes** : Les GNN peuvent être utilisées pour classer des graphes en différentes catégories, tels que dans le cas de l'analyse des réseaux sociaux, la classification de textes et classification des molécules.

- **Prédiction de lien** : Les GNN peuvent prédire le lien manquant entre une paire de nœuds dans un graphe avec une matrice d'adjacence incomplète. Ils sont souvent utilisés pour les réseaux sociaux (tel que la suggestion des amis)

- **Plongement de graphe** : Les GNN permettent de faire la transformation de graphe en vecteurs, en préservant les informations pertinentes sur les nœuds, les arêtes et la structure générale du graphe.

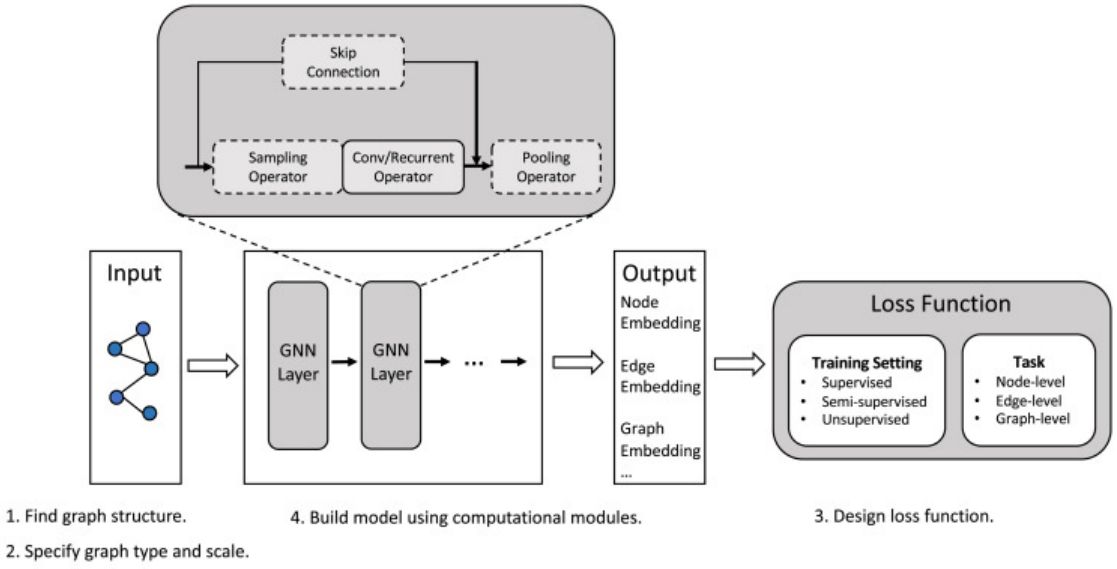

Fig. 1.10 : Le pipeline de conception générale pour un modèle GNN [Zhou et al. 2020].

1.7 Le processus d'apprentissage

L'apprentissage est le processus itératif et continu d'ajustement des paramètres du réseau neuronal afin d'obtenir une meilleure précision du modèle [Goodfellow et al. 2016]. Il peut être complexe car il nécessite souvent une combinaison de techniques telles que le **prétraitement** des données, le choix de l'architecture du réseau de neurones et des hyperparamètres, ainsi que l'algorithme d'optimisation.

Ce processus d'apprentissage commence d'abord par l'initialisation aléatoire des paramètres (poids) du modèle. Ensuite, le modèle est entraîné sur un ensemble de données (**dataset**) en utilisant un algorithme d'optimisation pour ajuster les poids du modèle afin de minimiser la perte.

Lors de l'entraînement, le modèle est alimenté en entrée avec des exemples à partir du dataset d'entrainement et compare sa sortie à la sortie attendue. Ensuite, il calcul la perte en faisant la différence entre la sortie prédite et la sortie attendue. L'algorithme de **rétropropagation** de gradient ajuste les poids du modèle en claculant les gradient de la fonction de perte afin de la minimiser.

Le processus d'apprentissage continue jusqu'à ce que la performance du modèle sur le dataset de validation arrête de s'améliorer ou jusqu'à ce qu'un nombre prédéfini d'itérations d'apprentissage soit atteint. Le modèle final est ensuite utilisé pour effectuer des prédictions sur de nouvelles données.

Ce processus peut être résumé dans les points suivants :

- L'apprentissage consiste à modifier progressivement les paramètres (poids) en passant un lot de données en entrée et en évaluant le taux de perte.
- La définition de la fonction de perte est utilisée pour les modifications de réseaux dans le processus de l'entraînement.
- La modification des poids du réseau est effectuée grâce a l'algorithme de rétropropagation (backpropagation).

1.7.1 Descente de gradient

La descente de gradient est une méthode utilisée dans le processus d'optimisation. Elle est basée sur la différentiabilité d'une fonction et elle est appliquée pour calculer la fonction dérivée du premier ordre pour trouver le minimum de la fonction de perte [Goodfellow et al. 2016]. Sa simplicité d'application est l'un des avantages de cette méthode.

L'algorithme commence par l'initialisation aléatoire des paramètres (poids) du modèle. Ensuite, il calcule le gradient de la fonction de perte par rapport à chaque paramètre. Le gradient indique la direction dans laquelle la fonction de perte augmente le plus, donc l'algorithme met à jour les paramètres dans la direction opposée au gradient pour réduire la valeur de perte. Ce processus est répété itérativement jusqu'à ce que la valeur de perte ne puisse plus être réduite ou jusqu'à ce qu'un critère d'arrêt soit atteint. Le taux

d'apprentissage est un hyperparamètre qui contrôle la taille des mises à jour de paramètres et la vitesse de convergence de l'algorithme [Goodfellow et al. 2016].

Des variantes de la descente de gradient existent, telles que la descente de gradient stochastique, Adam et la descente de gradient avec moment.

1.7.2 Propagation de l'erreur

La propagation d'erreur est utilisée dans le processus d'apprentissage pour calculer le gradient de la fonction de perte par rapport aux paramètres du modèle [Goodfellow et al. 2016].

Dans la propagation d'erreur, l'erreur est propagée en arrière à travers les couches du modèle, en commençant par la couche de sortie et en allant vers l'entrée. Chaque couche calcule la dérivée de sa sortie par rapport à ses entrées, qui est ensuite multipliée par l'erreur propagée de la couche suivante. Ce processus est répété jusqu'à ce que l'erreur soit propagée jusqu'à la couche d'entrée, où le gradient de la fonction de perte par rapport aux paramètres du modèle est obtenu [Goodfellow et al. 2016].

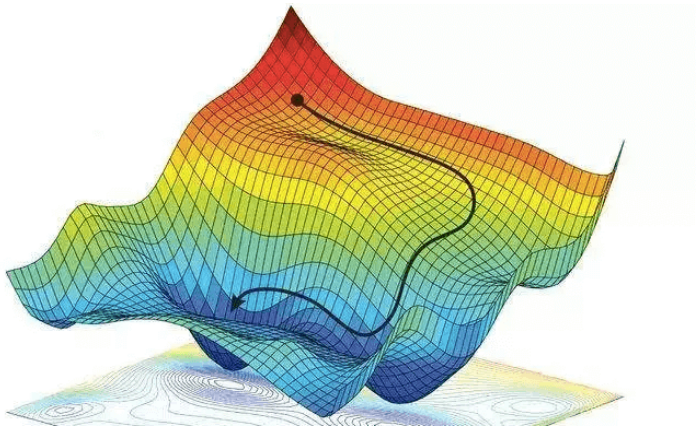

Fig. 1.11 : Fonction de taux d'erreur [Amini et al. 2018].

1.7.3 Hyperparameters

Les hyperparamètres sont les paramètres qui sont définis avant de lancer le processus d'apprentissage et ils contrôlent l'entraînement. Les valeurs des hyperparamètres, contrairement aux paramètres du modèle, ne sont pas apprises lors de l'apprentissage [Goodfellow et al. 2016]. Parmi les hyperparamètres, on peut définir :

- **Taux d'apprentissage** : Il contrôle la vitesse d'apprentissage du modèle à partir des données.
- **Nombre d'époques** : Le nombre d'époques correspond au nombre d'itération sur le dataset d'entraînement.

- **Taille du batch** : Elle représente le nombre d'échantillons des données d'entraînement qui sont utilisés dans un passage avant/arrière (feedforward et backpropagation).

- **Nombre de couches** : C'est un hyperparamètre qui caractérise la profondeur du réseau.

- **Fonction d'activation** : La fonction d'activation est utilisée pour introduire la non-linéarité dans le modèle. C'est un hyperparamètre qui contrôle la sortie du neurone.

- **Initialisation des poids** : Les valeurs initiales des poids peuvent affecter de manière significative les performances du modèle. Elle affecte le processus de trouver le minimum local ou le minimum global.

- **Paramètre de régularisation** : Il est utilisé pour éviter le **surapprentissage**, c'est-à-dire éviter de construire un modèle qui est trop complexe par rapport à la quantité de données d'entraînement. Cela peut entraîner une adaptation excessive du modèle aux données d'entraînement et une mauvaise généralisation aux données inconnues.

- **Optimiseur** : L'optimiseur est l'algorithme utilisé pour mettre à jour les poids pendant l'entraînement.

Cependant, le réglage de ces hyperparamètres peut être une tâche complexe nécessitant souvent des essais et des erreurs.

1.8 Types d'apprentissage

Il existe plusieurs types d'apprentissage, et chacun de ces types a des applications spécifiques en deep learning, et peut être utilisé pour résoudre différents types de problèmes. Dans ce qui suit, nous parlons brièvement sur les quatre types d'apprentissage en deep learning les plus courants : l'apprentissage supervisé, l'apprentissage non supervisé, l'apprentissage semi-supervisé et l'apprentissage par renforcement.

1.8.1 Apprentissage supervisé

Dans l'apprentissage supervisé, l'apprentissage s'effectue sur un ensemble de données étiqueté, où les étiquettes sont connues à l'avance. En d'autres termes, les données d'entrée sont accompagnées d'étiquettes de sortie ou de valeurs cibles correspondantes. Le but de l'apprentissage supervisé est d'apprendre à prédire les étiquettes à partir des données d'entrée, de sorte que lorsqu'on donne au modèle de nouvelles données en entrée, l'algorithme puisse prédire la sortie correspondante. Pendant le processus d'apprentissage, l'algorithme ajuste itérativement ses paramètres pour minimiser la différence entre la sortie prédite et la sortie réelle [Aggarwal 2018, Goodfellow et al. 2016].

Ce type d'apprentissage est applicable dans plusieurs domaines, tels que la reconnaissance d'images et de la parole, le traitement du langage naturel et la modélisation prédictive dans la finance, la santé, le marketing, etc. Parmi les algorithmes d'apprentissage supervisés, nous pouvons citer la régression linéaire et les arbres de décision.

1.8.2 Apprentissage non-supervisé

L'apprentissage non supervisé se fait sur un dataset non étiqueté, sans aucune information sur les étiquettes [Goodfellow et al. 2016]. En d'autres termes, il n'y a pas de valeurs cibles ou d'étiquettes de sortie fournies à l'algorithme. L'algorithme est laissé à lui-même pour trouver les motifs et relations dans les données, sans recevoir d'instructions explicites sur ce qu'il faut rechercher.

L'utilisation de cette approche d'apprentissage peut impliquer le regroupement de points de données similaires, la découverte de structures ou de caractéristiques cachées dans les données (réduction de la dimensionnalité) ou l'identification de valeurs aberrantes ou d'anomalies dans les données.

Nous pouvons appliquer l'apprentissage non supervisé dans divers domaines, tels que la segmentation des marchés, la détection d'anomalies et l'extraction de caractéristiques. Parmi les algorithmes d'apprentissage non supervisés courants, on trouve le clustering k-means, l'analyse en composantes principales (PCA) et les auto-encodeurs.

L'un des principaux défis dans l'apprentissage non supervisé est d'évaluer la qualité des résultats, car il n'y a pas d'objectifs ou d'étiquettes explicites à comparer. Au lieu de cela, les résultats sont souvent évalués en fonction de leur utilité ou de leur interprétabilité pour une tâche ou un domaine particulier.

1.8.3 Apprentissage semi-supervisé

L'apprentissage semi-supervisé est un type d'apprentissage qui combine des éléments d'apprentissage supervisé et non supervisé. Dans l'apprentissage semi-supervisé, un petit ensemble de données étiquetées est fourni, tandis que la grande partie de données est non étiquetées [Goodfellow et al. 2016].

Le but dans l'apprentissage semi-supervisé est d'utiliser les données étiquetées pour guider le processus d'apprentissage sur les données non étiquetées, afin d'améliorer la précision du modèle. Cela peut être particulièrement utile dans les situations où il est difficile ou coûteux d'obtenir des données étiquetées, mais il existe une abondance de données non étiquetées disponibles.

Il existe plusieurs approches, mais une méthode courante consiste à utiliser les données étiquetées pour créer un modèle, puis à utiliser ce modèle pour faire des prédictions sur les données non étiquetées. Les étiquettes prédites sont ensuite utilisées pour améliorer le modèle, et le processus est répété de manière itérative.

L'un des défis de l'apprentissage semi-supervisé est que la qualité des résultats peut

dépendre fortement de la distribution des données non étiquetées. Si les données non étiquetées ne sont pas représentatives du domaine cible, le modèle peut mal fonctionner même avec une grande quantité de données non étiquetées.

1.8.4 Apprentissage par renforcement

L'apprentissage par renforcement se concentre sur la prise de décision. Il s'agit d'une méthode d'apprentissage dans laquelle un agent apprend à prendre des décisions en interagissant avec un environnement. L'agent doit choisir une action à partir d'un état donné, et l'environnement renvoie un signal de récompense ou de pénalité en fonction de l'action choisie. L'objectif de l'agent est de maximiser la récompense totale sur une période donnée [Wiering et al. 2012]. Dans le chapitre suivant, nous présenterons l'apprentissage par renforcement et nous en parlerons avec plus de détails.

1.9 Catégories de données

La division du jeu de données est une étape cruciale avant de commencer l'entraînement du modèle de manière. Elle permet d'éviter les problèmes de surapprentissage. Il est courant de diviser un jeu de données en trois parties distinctes : l'ensemble d'entraînement, l'ensemble de validation et l'ensemble de test [Goodfellow et al. 2016].

- **Ensemble d'entraînement** : Il s'agit de la partie de données utilisée pour entraîner le modèle. Il est important que ce dataset soit représentatif de l'ensemble des données et qu'il contienne une variété de cas d'utilisation différents.
- **Ensemble de validation** : Il s'agit d'un sous-ensemble de l'ensemble de données utilisé pour évaluer les performances du modèle pendant l'entraînement. L'ensemble de validation est utilisé pour régler les hyperparamètres du modèle et pour éviter le surapprentissage. Il est important qu'il soit représentatif et distinct du dataset d'entraînement.
- **Ensemble de test** : Il s'agit d'un ensemble de données utilisé pour évaluer les performances du modèle après son entraînement. L'ensemble de test est utilisé pour obtenir une estimation impartiale de la performance du modèle sur de nouvelles données inédites, donc il est nécessaire que ce dataset soit représentatif de l'ensemble des données et distinct des deux autres datasets cités précédemment.

La distinctivité des datasets assure que le modèle se généralise bien aux nouvelles données invisibles. En règle générale, l'ensemble de données est divisé en ces trois ensembles dans un rapport de 60-20-20 ou 70-15-15 respectivement.

1.10 Défis de l'apprentissage profond

L'apprentissage profond a fait des progrès remarquables ces dernières années et a obtenu des résultats excellents dans divers domaines tels que la vision par ordinateur,

le traitement du langage naturel et la reconnaissance de la parole. Cependant, il reste encore plusieurs défis à relever afin d'améliorer encore l'efficacité et l'efficience des modèles d'apprentissage profond. Certains défis majeurs incluent :

- **Rareté des données** : les modèles d'apprentissage profond nécessitent une grande quantité de données pour être entraînés efficacement. Cependant, dans de nombreux domaines, tels que l'imagerie médicale et la conduite autonome, les données sont rares et coûteuses à collecter.
- **Surapprentissage (overfitting)** : les modèles d'apprentissage profond peuvent facilement sur-adapter les données d'apprentissage, en particulier lorsque le modèle comporte un grand nombre de paramètres. Le surapprentissage peut entraîner de mauvaises performances de généralisation sur de nouvelles données.
- **Interprétabilité** : les modèles d'apprentissage profond sont souvent appelés "boîtes noires" car il peut être difficile de comprendre comment ils arrivent à leurs prédictions. Ce manque d'interprétabilité peut compliquer le débogage et l'amélioration des modèles de l'apprentissage profond
- **Limitations matérielles** : les modèles d'apprentissage profond sont coûteux en termes de calcul et nécessitent un matériel spécialisé tel que des unités de traitement graphique (GPU) ou des unités de traitement de tenseur (TPU). Le coût de ce matériel peut constituer un obstacle pour les petits groupes de chercheurs ou les entreprises.
- **Attaques contradictoires** : les modèles d'apprentissage profond peuvent être vulnérables aux attaques contradictoires, où un attaquant manipule délibérément les données d'entrée pour amener le modèle à faire des prédictions incorrectes.

1.11 Conclusion

En conclusion, l'apprentissage profond est devenu un domaine de recherche actif de l'apprentissage automatique qui a révolutionné la façon dont nous abordons de nombreux problèmes difficiles, tels que la vision par ordinateur, le traitement du langage naturel et la robotique. Avec l'avènement d'un matériel puissant, d'ensembles de données à grande échelle et d'algorithmes sophistiqués, les modèles d'apprentissage profond ont connu un avancement remarquable dans plusieurs domaines tels que la reconnaissance d'images, la reconnaissance vocale, la traduction linguistique et la conduite autonome.

Malgré son énorme succès, l'apprentissage en profondeur fait encore face à plusieurs défis, tels que le besoin d'algorithmes d'entraînement plus efficaces et fiables, une meilleure interprétabilité, etc. L'utilisation et l'entraînement de modèles d'apprentissage profond exigent des ordinateurs assez puissants et ne peuvent pas être utilisés sur les appareils moins puissants comme les ordinateur embarqués ou les smartphones, ce qui signifie qu'on a besoin de trouver des moyens pour optimisation ces modèles afin de les utiliser ultérieurement par les machines moins puissantes. Ces méthodes d'optimisation font l'objet du dernier chapitre.

Dans ce qui suit, nous présenterons l'apprentissage profond et ses algorithmes. La raison pour laquelle on a réservé un chapitre complet pour l'apprentissage profond est que ce type d'apprentissage peut aider beaucoup dans l'optimisation des réseaux de neurones profonds, comme nous le verrons plus tard.

Chapitre 2

Intelligence Artificielle Générative (GenAI)

2.1 Introduction

Avec les avancées fulgurantes du deep learning, de nouvelles méthodes d'intelligence artificielle ont émergé, souvent désignées sous le terme de modèles génératifs. Ces technologies de pointe, telles que les auto-encodeurs variationnels, les réseaux adversariaux génératifs (GANs), les modèles de diffusion, les transformers et les modèles de langage de grande taille (LLM) sont capables de produire des données d'une qualité impressionnante, ressemblant de manière frappante aux données réelles. Les données générées par ces modèles sont souvent indiscernables des données authentiques, ce qui pose de nouveaux défis en matière d'identification et d'authenticité.Les modèles génératifs permettent la génération de textes, d'images, de séries temporelles et de données tabulaires avec une grande précision.

La puissance de ces modèles repose sur des ressources de calcul considérables, notamment l'utilisation de GPU, et sur l'accès à des ensembles de données massifs. Par exemple, des modèles tels que ChatGPT-4 ont été entraînés sur l'intégralité du contenu disponible sur Internet.

Dans ce chapitre, nous allons examiner en détail les différentes architectures de ces modèles génératifs, ainsi que les techniques et pratiques associées à leur fonctionnement et à leur mise en œuvre. Nous aborderons les principes de base, les innovations récentes, et les applications potentielles de ces technologies révolutionnaires.

2.2 Les Auto-Encodeurs Variationnels (VAE)

2.2.1 Introduction

Les auto-encodeurs variationnels (VAE) sont des modèles génératifs puissants, reconnus pour leur capacité à apprendre une représentation compacte et structurée des données.

Cette approche a révolutionné le domaine de l'apprentissage non supervisé et des modèles génératifs. Les VAE appartiennent à la classe des modèles génératifs probabilistes, combinant les principes des autoencodeurs et des modèles de variational Bayes pour générer des données nouvelles et similaires à celles d'un jeu de données d'entraînement. Depuis leur introduction par Kingma et Welling en 2013 [Kingma et al. 2012] , les VAE ont connu un grand succès dans diverses applications, allant de la génération d'images à la synthèse de texte.

2.2.2 Fonctionnement

Les VAE sont composés de trois éléments principaux : l'encodeur, le décodeur et l'espace latent. Chacune de ces composantes joue un rôle crucial dans le fonctionnement global du modèle.

L'Encodeur :L'encodeur est responsable de la transformation des données d'entrée $\mathbf{x}$ en une distribution dans l'espace latent. Plus précisément, il mappe les données d'entrée à une distribution gaussienne paramétrée par une moyenne μ et une variance σ^2. Cette distribution est souvent représentée comme :

$$q(\mathbf{z} \mid \mathbf{x}) = \mathcal{N}(\mathbf{z} \mid \mu(\mathbf{x}), \sigma^2(\mathbf{x})) \tag{2.1}$$

où $\mathbf{z}$ est la variable latente que l'encodeur cherche à estimer.

Le Décodeur : Le décodeur prend un échantillon $\mathbf{z}$ de la distribution gaussienne dans l'espace latent et génère une reconstruction $\hat{\mathbf{x}}$ des données d'entrée. Il modélise la distribution des données d'entrée conditionnellement à $\mathbf{z}$ comme suit :

$$p(\mathbf{x} \mid \mathbf{z}) \tag{2.2}$$

Typiquement, le décodeur est un réseau neuronal qui produit les paramètres de cette distribution, souvent supposée gaussienne ou Bernoulli selon la nature des données.

L'Espace latent :est la représentation comprimée et structurée des données d'entrée. Il est généralement conçu comme un espace continu, où chaque point de l'espace latent correspond à une instance possible de données générées. L'idée est que cet espace latent capture les caractéristiques essentielles des données d'entrée de manière à permettre la génération de nouvelles instances en échantillonnant de cet espace.

L'objectif principal d'un VAE est d'optimiser une fonction de coût qui combine deux termes principaux : la divergence de Kullback-Leibler (KL) et la vraisemblance de reconstruction.

Divergence de Kullback-Leibler (KL) : Ce terme mesure la différence entre la distribution latente approximée $q(z|x)$ et la distribution prior $p(z)$. La divergence KL est donnée par :

$$D_{KL}(q(z|x) \parallel p(z))$$

où $q(z|x)$ est la distribution gaussienne paramétrée par l'encodeur, et $p(z)$ est généralement choisie comme une distribution normale standard.

Vraisemblance de Reconstruction

Ce terme mesure la capacité du modèle à reconstruire les données d'entrée x à partir de la variable latente z. Il est donné par la vraisemblance de x conditionnée par z :

$$\log p(x|z)$$

Fonction de Perte VAE

La fonction de coût totale d'un VAE, également appelée fonction de perte VAE, combine ces deux termes. Elle peut être formulée comme suit :

$$\mathcal{L}(\theta, \phi; x) = -\mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x|z)] + D_{KL}(q_\phi(z|x) \parallel p(z))$$

où θ et ϕ sont les paramètres du décodeur et de l'encodeur respectivement. Le premier terme, $-\mathbb{E}_{q_\phi(z|x)}[\log p_\theta(x|z)]$, représente l'erreur de reconstruction, et le second terme, $D_{KL}(q_\phi(z|x) \parallel p(z))$, régularise la distribution latente pour qu'elle soit proche de la distribution prior.

En optimisant cette fonction de perte, les VAE parviennent à apprendre des représentations latentes qui permettent une reconstruction fidèle des données d'entrée tout en assurant une régularité statistique dans l'espace latent.

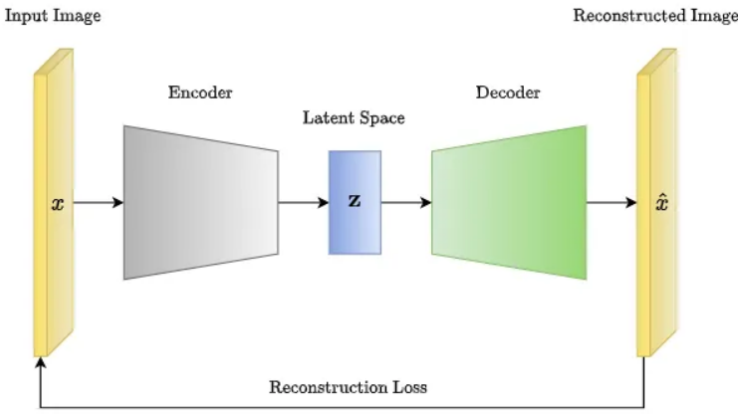

Fig. 2.1 : Le fonctionnement d'un neurone artificiel [Kingma et al. 2012].

2.2.3 Applications des Auto-Encodeurs Variationnels (VAE)

Les auto-encodeurs variationnels (VAE) ont démontré leur efficacité dans divers domaines grâce à leur capacité à apprendre des représentations latentes significatives. Voici quelques-unes des principales applications des VAE :

Génération d'Images

Les VAE sont largement utilisés pour générer des images réalistes. En apprenant une représentation latente des images d'entraînement, les VAE peuvent échantillonner de cet

espace latent pour créer de nouvelles images qui partagent des caractéristiques similaires avec les données d'origine. Cela a des applications potentielles dans la création de contenu, la conception assistée par ordinateur et la synthèse d'images médicales.

Synthèse de Texte

Les VAE peuvent être appliqués à la génération de texte en apprenant les structures latentes des séquences de texte. Ils permettent de produire des phrases cohérentes et des paragraphes qui imitent le style et le contenu des textes d'entraînement. Cette technique est utile dans des domaines tels que la génération automatique de rapports, l'écriture créative assistée et la traduction automatique.

Compression de Données

Les VAE sont efficaces pour la compression de données, en particulier pour des données de grande dimension comme les images et les vidéos. En apprenant une représentation latente compacte, les VAE peuvent réduire la dimensionnalité des données tout en préservant leurs caractéristiques essentielles. Cela permet une transmission et un stockage plus efficaces des données compressées.

Détection d'Anomalies

Dans les systèmes de détection d'anomalies, les VAE peuvent être utilisés pour identifier des données aberrantes qui diffèrent significativement des données d'entraînement. En apprenant une distribution latente des données normales, le VAE peut détecter des échantillons qui ne correspondent pas à cette distribution, ce qui est particulièrement utile dans la surveillance de systèmes industriels, la cybersécurité et la détection de fraudes.

Imputation de Données Manquantes

Les VAE peuvent également être employés pour l'imputation de données manquantes. En apprenant la structure latente des données complètes, les VAE peuvent estimer les valeurs manquantes de manière cohérente avec les données observées. Cette application est cruciale dans des domaines tels que l'analyse de données médicales, les études socio-économiques et les bases de données incomplètes.

En résumé, les VAE sont des outils polyvalents dans le domaine de l'apprentissage machine, avec des applications variées allant de la génération de contenu à la compression de données et à la détection d'anomalies. Leur capacité à apprendre des représentations latentes significatives permet de traiter efficacement une large gamme de problèmes complexes.

2.3 Réseaux Antagonistes Génératifs (GANs)

2.3.1 Introduction aux Réseaux Antagonistes Génératifs (GANs)

Les réseaux antagonistes génératifs, ou Generative Adversarial Networks (GANs) en anglais, sont une classe de modèles génératifs introduite par Ian Goodfellow et ses collègues en 2014 [Goodfellow et al. 2014]. Les GANs se composent de deux réseaux de neurones concurrents : un générateur et un discriminateur. Le générateur cherche à produire des échantillons réalistes à partir d'un bruit aléatoire, tandis que le discriminateur tente de distinguer les échantillons réels des échantillons générés. Cette compétition incite les deux réseaux à s'améliorer simultanément, aboutissant à la génération de données de haute qualité.

2.3.2 Fonctionnement des Réseaux Antagonistes Génératifs (GANs)

Les GANs sont des modèles très performants et sont adaptés à plusieurs architectures variées. Cependant, ils se composent principalement de deux réseaux de neurones principaux :

Générateur

Le réseau générateur prend un vecteur de bruit z tiré d'une distribution uniforme ou normale et produit une donnée synthétique $G(z)$. Mathématiquement, le générateur peut être représenté comme une fonction $G : Z \to X$, où Z est l'espace du bruit et X est l'espace des données. L'objectif du générateur est de "tromper" le discriminateur en générant des données indiscernables des données réelles.

$$G(z; \theta_g) : z \sim p_z(z) \to x = G(z)$$

où θ_g représente les paramètres du générateur, $p_z(z)$ est la distribution du bruit (généralement uniforme ou normale), et x est la donnée synthétique générée.

Le générateur apprend à partir des erreurs du discriminateur, en améliorant constamment la qualité des données générées. En d'autres termes, il essaie de maximiser la probabilité que le discriminateur classifie ses sorties comme étant des données réelles.

Discriminateur

Le réseau discriminateur reçoit soit une donnée réelle x soit une donnée générée $G(z)$. Il sort une probabilité $D(x)$ ou $D(G(z))$ indiquant si l'entrée est réelle ou générée. Mathématiquement, le discriminateur peut être représenté comme une fonction $D : X \to [0, 1]$, où $D(x)$ représente la probabilité que x soit une donnée réelle.

$$D(x; \theta_d) : x \to [0, 1]$$

où θ_d représente les paramètres du discriminateur. Le discriminateur est entraîné pour maximiser la probabilité d'assigner la bonne étiquette aux échantillons réels et générés. Il essaie de minimiser la probabilité d'être trompé par les fausses données produites par le générateur.

Le discriminateur est, en essence, un classificateur binaire qui essaie de distinguer entre les données authentiques et celles générées.

Fonction de Perte

Les fonctions de perte pour le générateur et le discriminateur sont définies comme suit :

$$\mathcal{L}_D = -\mathbb{E}_{x\sim p_{data}}[\log D(x)] - \mathbb{E}_{z\sim p_z}[\log(1 - D(G(z)))]$$

$$\mathcal{L}_G = -\mathbb{E}_{z\sim p_z}[\log D(G(z))]$$

Où :

$\mathcal{L}_D$: fonction de perte du discriminateur
$\mathcal{L}_G$: fonction de perte du générateur
x : donnée réelle tirée de la distribution p_{data}
z : vecteur de bruit tiré de la distribution p_z
$D(x)$: probabilité estimée par le discriminateur que x soit une donnée réelle
$G(z)$: donnée synthétique générée à partir du bruit z

L'objectif du générateur est de minimiser $\mathcal{L}_G$, tandis que le discriminateur cherche à minimiser $\mathcal{L}_D$. Plus formellement, l'objectif est de résoudre le problème de minimax suivant :

$$\min_G \max_D \mathbb{E}_{x\sim p_{data}}[\log D(x)] + \mathbb{E}_{z\sim p_z}[\log(1 - D(G(z)))]$$

Entraînement des GANs

L'entraînement des réseaux antagonistes génératifs (GANs) implique une série d'étapes répétitives où le générateur et le discriminateur sont mis à jour tour à tour pour améliorer leurs performances respectives. Le processus se déroule comme suit :

L'entraînement des GANs se fait par les étapes suivantes :

1. Tirer un échantillon de bruit z de la distribution p_z.
2. Générer une donnée synthétique $G(z)$ à partir du générateur.
3. Tirer un échantillon de données réelles x de la distribution de données p_{data}.
4. Mettre à jour les poids du discriminateur D en minimisant la fonction de perte $\mathcal{L}_D$.

5. Tirer un nouvel échantillon de bruit z.

6. Mettre à jour les poids du générateur G en minimisant la fonction de perte $\mathcal{L}_G$.

7. Répéter les étapes ci-dessus pour un nombre prédéfini d'itérations.

En suivant ces étapes, les GANs sont entraînés pour générer des données synthétiques réalistes qui peuvent être utilisées dans diverses applications, telles que la génération d'images, la super-résolution d'images et la synthèse de texte.

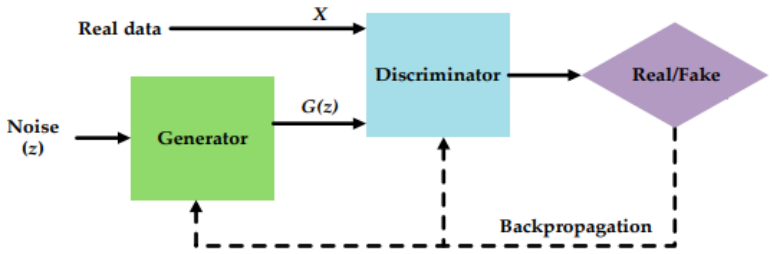

FIG. 2.2 : Un modèle de réseau générateur adversaire (GAN) [Jie FENG et al. 2020].

2.3.3 Applications des GANs

Les GANs ont une variété d'applications dans différents domaines :

Génération d'Images

Les GANs sont largement utilisés pour générer des images réalistes. Ils ont été appliqués avec succès dans la création d'images de haute qualité, la génération de visages humains, et même la création artistique. Par exemple, les GAN peuvent générer des images de personnes qui n'existent pas en apprenant les caractéristiques des visages humains à partir de vastes bases de données d'images.

Super-Résolution d'Images

Les GANs sont également utilisés pour la super-résolution d'images, c'est-à-dire augmenter la résolution d'une image basse résolution. Le modèle SRGAN (Super-Resolution GAN) est un exemple où les GANs sont utilisés pour produire des images de haute résolution à partir d'images de basse résolution, améliorant ainsi les détails visuels et la clarté.

Synthèse de Texte et Traduction Automatique

Dans le traitement du langage naturel (NLP), les GANs sont appliqués à la génération de texte et à la traduction automatique. Les modèles basés sur les GAN peuvent générer des phrases cohérentes et contextuellement appropriées, imitant le style et le contenu des

textes d'entraînement. Cela est particulièrement utile pour les applications comme les chatbots, la création de contenu textuel, et les systèmes de traduction.

StyleGAN : This Person Does Not Exist

StyleGAN, ou Style-Based Generator Architecture for Generative Adversarial Networks, est un modèle génératif avancé développé par les chercheurs de NVIDIA[Karras et al. 2019]. Il représente une avancée significative dans la génération d'images de haute qualité et photoréalistes, y compris les visages de personnes qui n'existent pas. StyleGAN a diverses applications, y compris dans l'industrie du divertissement, la réalité virtuelle et la recherche académique.

This Person Does Not Exist : Un exemple frappant de l'application de StyleGAN est le site web "This Person Does Not Exist" [Wang 2019] . Ce site utilise un modèle StyleGAN pour générer de manière aléatoire des visages de personnes qui n'existent pas à chaque rechargement de la page.

Fig. 2.3 : Quelques images générées par le modèle StyleGAN sur le site 'This Person Does Not Exist'[Wang 2019].

En résumé, les GANs sont des outils puissants et polyvalents dans le domaine de l'apprentissage machine, avec des applications qui vont de la génération d'images à la traduction automatique. Leur capacité à apprendre et à générer des données réalistes ouvre de nombreuses perspectives dans divers domaines.

2.4 Diffusion models

2.4.1 Introduction

Les modèles de diffusion, également connus sous le nom de diffusion models, représentent une avancée significative dans le domaine des modèles génératifs au sein de l'apprentissage automatique. Émergents de manière proéminente ces dernières années, ces modèles ont attiré l'attention pour leur remarquable capacité à générer des données synthétiques de haute qualité, les positionnant comme une alternative prometteuse aux

techniques plus établies telles que les Réseaux Antagonistes Génératifs (GANs) et les Autoencodeurs Variationnels (VAEs) [Ho et al. 2020].

La fondation conceptuelle des modèles de diffusion s'inspire des processus de diffusion physique, où les particules migrent des régions de haute concentration vers des zones de moindre concentration. Ces modèles sont également basés sur les chaînes de Markov comme illustré dans la figure (2.4), un concept clé en probabilité qui décrit une série de transitions d'état où chaque état dépend uniquement de l'état précédent. Dans le contexte des données, ce principe est exploité pour affiner progressivement les données bruitées en représentations réalistes [Yang Song 2022].

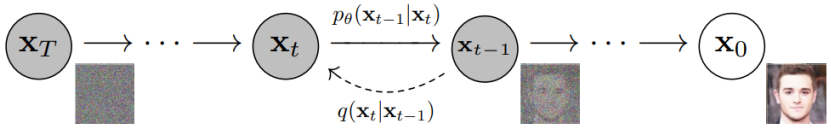

Fig. 2.4 : Chaîne de Markov du processus de diffusion [Ho et al. 2020].

2.4.2 Fonctionnement des Modèles de Diffusion

Les modèles de diffusion utilisent un processus en deux étapes cruciales : le bruitage (noising, également appelé Forward Process) et le débruitage (denoising, ou Reverse Process). Ces étapes sont essentielles pour transformer des données réelles en une distribution de bruit et inversement. Le Forward Process consiste à ajouter progressivement du bruit aux données réelles, les transformant ainsi en une séquence de données de plus en plus bruitées. Ensuite, le Reverse Process inverse ce processus en éliminant le bruit étape par étape, recréant des données réalistes à partir du bruit.

Pour effectuer le débruitage, un réseau de neurones est utilisé. Ce réseau de neurones est entraîné à détecter et à éliminer le bruit à chaque étape du Reverse Process. Il apprend à prédire l'état précédent des données à partir de l'état actuel bruité, permettant ainsi de reconstruire progressivement les données originales. Cette méthode en deux phases, combinée à l'utilisation d'un réseau de neurones pour le débruitage, permet de modéliser et de générer des données synthétiques de haute qualité de manière efficace et contrôlée.

Les modèles de diffusion utilisent un processus en deux étapes : le bruitage (noising, également appelé *Forward Process*) et le débruitage (denoising, ou *Reverse Process*). Ces étapes sont essentielles pour transformer des données réelles en une distribution de bruit et inversement.

Forward Process (Bruitage)

L'étape de bruitage ajoute progressivement du bruit gaussien aux données réelles. Ce processus est modélisé comme une chaîne de Markov où chaque état x_t dépend uniquement de l'état précédent x_{t-1}.

La transition conditionnelle pour le bruitage est donnée par :

$$q(x_t|x_{t-1}) = \mathcal{N}(x_t; \sqrt{1-\beta_t}x_{t-1}, \beta_t\mathbf{I})$$

où :

x_t : état des données à l'étape t
β_t : taux de bruitage (un hyperparamètre ou une fonction du temps)
$\mathcal{N}$: distribution normale gaussienne
$\mathbf{I}$: matrice identité

La séquence complète des T étapes de bruitage est décrite par :

$$q(x_{1:T}|x_0) = \prod_{t=1}^{T} q(x_t|x_{t-1})$$

Explication du Forward Process :

- À chaque étape t, une petite quantité de bruit gaussien est ajoutée à x_{t-1}, produisant x_t.
- La moyenne de la distribution est $\sqrt{1-\beta_t}x_{t-1}$, indiquant que la contribution des données d'origine diminue progressivement.
- La variance est β_t, contrôlant la quantité de bruit ajouté.

Reverse Process (Débruitage)

L'étape de débruitage consiste à inverser le processus de bruitage pour transformer le bruit gaussien en données réalistes. Cela se fait en utilisant un modèle génératif pour approximer la distribution inverse.

La transition conditionnelle pour le débruitage est donnée par :

$$p_\theta(x_{t-1}|x_t) = \mathcal{N}(x_{t-1}; \mu_\theta(x_t, t), \Sigma_\theta(x_t, t))$$

où :

p_θ : distribution paramétrée par les poids du modèle θ
μ_θ : moyenne apprise par le modèle
Σ_θ : covariance apprise par le modèle

Explication du Reverse Process :

- Le modèle est entraîné pour prédire x_{t-1} à partir de x_t.
- La moyenne $\mu_\theta(x_t, t)$ est une fonction paramétrée par θ, dépendant de x_t et du temps t.
- La covariance $\Sigma_\theta(x_t, t)$ représente l'incertitude du modèle.

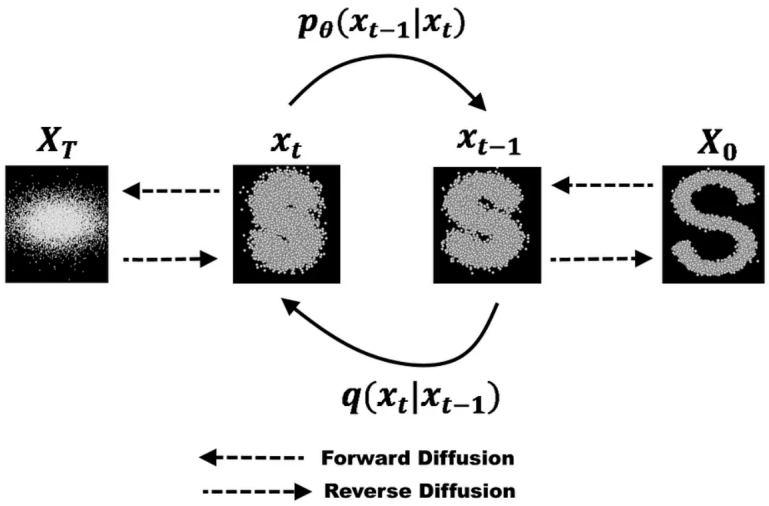

FIG. 2.5 : Illustration des Processus de Diffusion : Forward Process et Reverse Process.

Objectif d'Entraînement : L'objectif est de minimiser la divergence de Kullback-Leibler (KL) entre la distribution réelle q et la distribution générée par le modèle p_θ :

$$\mathcal{L} = \mathbb{E}_q \left[\sum_{t=1}^{T} D_{KL}(q(x_{t-1}|x_t, x_0) \| p_\theta(x_{t-1}|x_t)) \right]$$

Conclusion

Les étapes de bruitage et de débruitage dans les modèles de diffusion permettent de transformer des données réelles en bruit gaussien et inversement. La formulation mathématique de ces étapes repose sur des distributions normales et des chaînes de Markov, et l'entraînement du modèle vise à minimiser la divergence entre les distributions réelles et générées. Ces processus sont cruciaux pour les applications de génération de données synthétiques de haute qualité dans divers domaines de l'apprentissage automatique.

2.5 Large Language Models

Les grands modèles de langage, également connus sous le nom de Large Language Models (LLM) en anglais, ont révolutionné le domaine de l'intelligence artificielle en réalisant des avancées significatives dans la génération et la compréhension du langage naturel. Leur capacité à analyser, traiter et produire du texte de manière contextuelle et cohérente a ouvert de nouvelles perspectives dans divers secteurs, notamment la traduction automatique, la création de contenu et l'assistance virtuelle [Naveed et al. 2023]. Parmi les méthodes et techniques employées dans ces modèles de langage, les réseaux neuronaux de type transformeur occupent une place prépondérante. Ce type de réseau neuronal sera présenté en détail dans les pages suivantes.

2.5.1 Réseaux de Neurones de Transformation (Transformers)

Les réseaux de neurones de transformation, ou Transformers, sont une architecture de réseau de neurones introduite par Google. Ils sont principalement utilisés pour le traitement du langage naturel (NLP), la traduction de texte et la génération de texte. Les Transformers se distinguent des réseaux récurrents (RNN) par leur capacité à traiter les dépendances séquentielles sans utiliser de couches récurrentes. Au lieu de cela, ils exploitent une technique appelée *self-attention*, permettant au modèle de se concentrer sur les parties importantes de l'entrée [Vaswani et al. 2017].

2.5.2 Fonctionnement des Transformers

Self-Attention

Dans un réseau de neurones à auto-attention, chaque mot ou token en entrée est représenté par un vecteur. Ces vecteurs sont utilisés pour calculer les scores d'attention entre les différentes parties de l'entrée. La formule de l'attention pour une tête est donnée par :

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{2.3}$$

où Q (queries), K (keys), et V (values) sont des matrices dérivées des représentations d'entrée, et d_k est la dimension des clés. Ces scores d'attention pondèrent les vecteurs en entrée, mettant plus d'importance sur les parties les plus pertinentes [Vaswani et al. 2017].

Architecture des Transformers

L'architecture des Transformers est composée de deux blocs principaux : l'encodeur et le décodeur.

Bloc d'Encodage Un bloc d'encodage transforme une séquence d'entrée $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ en une séquence de représentations contextuelles $\mathbf{h} = (h_1, h_2, \ldots, h_n)$. Chaque couche d'encodage comprend deux sous-couches principales :

- **Mécanisme d'Attention Multi-Têtes** : L'attention multi-têtes permet au modèle de se concentrer sur différentes parties de la séquence d'entrée pour chaque mot de sortie.
- **Feed-Forward Network** : Une couche de réseau de neurones feed-forward est appliquée à chaque position de manière indépendante :

$$\text{FFN}(x) = \max(0, xW_1 + b_1)W_2 + b_2 \tag{2.4}$$

où W_1, W_2, b_1, et b_2 sont des paramètres appris.

Bloc de Décodage Un bloc de décodage génère la séquence de sortie $\mathbf{y} = (y_1, y_2, \ldots, y_m)$, en utilisant les représentations contextuelles de l'encodage et les sorties précédentes. Le bloc de décodage inclut également des sous-couches d'attention multi-têtes, ainsi que des mécanismes pour l'attention croisée entre les représentations de l'entrée et de la sortie.

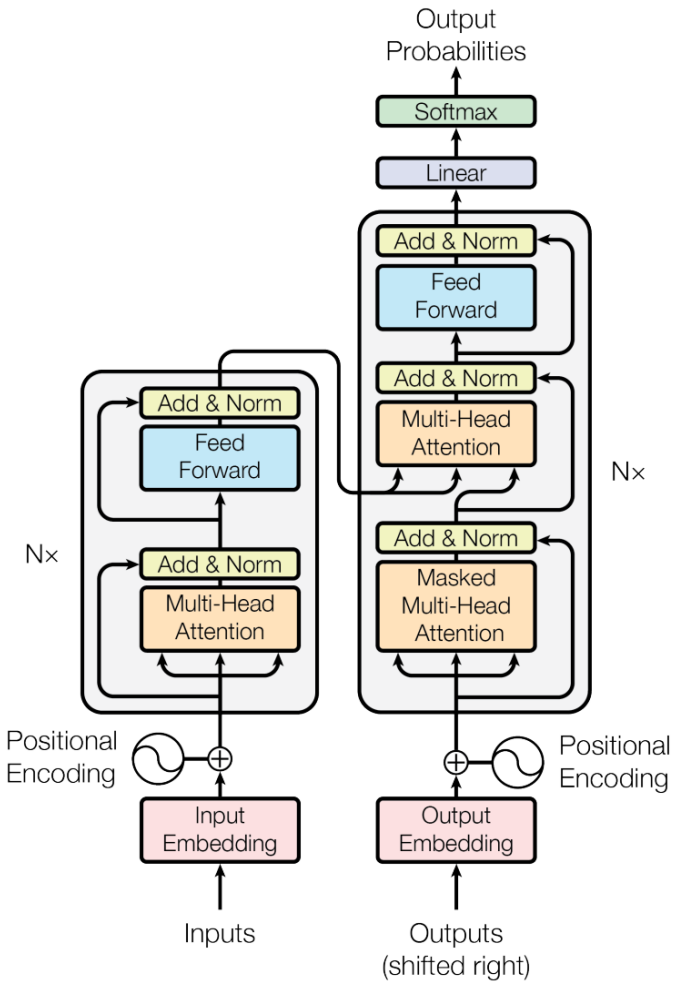

Fig. 2.6 : Architecture d'un reseau de neurones de transformation (Transformer) [Vaswani et al. 2017].

2.5.3 Applications des Transformers

Traduction Automatique

Les Transformers ont contribué de manière significative aux avancées récentes dans la traduction automatique. Leur capacité à gérer les dépendances à longue portée et à traiter les séquences en parallèle leur permet de surpasser les modèles récurrents traditionnels.

Génération de Texte

Les modèles GPT (Generative Pre-trained Transformer) de OpenAI, comme GPT-3, utilisent des architectures de Transformers massives avec des milliards de paramètres. Ces modèles sont capables de générer du texte de manière cohérente et contextuellement pertinente. Par exemple, GPT-3, avec ses 175 milliards de paramètres, peut produire des textes qui imitent le style et le contenu des textes d'entraînement [Brown et al. 2020].

2.5.4 Conclusion

Les Transformers ont révolutionné le domaine du traitement du langage naturel grâce à leur architecture innovante basée sur le mécanisme de *self-attention*. Leur capacité à gérer les dépendances séquentielles sans recourir à des couches récurrentes en fait des outils puissants pour des applications variées telles que la traduction automatique et la génération de texte. Les modèles avancés comme GPT-3 de OpenAI démontrent le potentiel énorme des Transformers lorsqu'ils sont mis à l'échelle avec des milliards de paramètres.

2.5.5 Réseaux de neurones de transformation (Transformer)

Les réseaux de neurones de transformation (Transformers) sont une architecture de réseau de neurones conçue par Google. Il sont utilises principalement pour le traitement du langage naturel, la traduction du texte et la génération de texte.

De ce fait, les Transformers ressemblent aux réseaux récurrents (RNN) mais la principale différence entre eux est que les Transformers n'utilisent pas de couches récurrentes pour modéliser les dépendances séquentielles. Au lieu de cela, ils utilisent une technique appelée "self-attention", qui permet au modèle de s'auto-atténuer sur les parties importantes de l'entrée [Vaswani et al. 2017].

Dans un réseau de neurones à auto-attention, chaque mot ou token en entrée est représenté par un vecteur, et ces vecteurs sont utilisés pour calculer les scores d'attention entre les différentes parties de l'entrée. Ces scores sont ensuite utilisés pour pondérer les vecteurs en entrée, en mettant plus d'importance sur les parties les plus pertinentes [Vaswani et al. 2017].

Les Transformers ont contribué significativement aux avancées récentes dans le domaine du traitement du langage naturel, en particulier dans la traduction automatique et de la génération de texte. Les modèles les plus avancés, telles que GPT-3 de OpenAI ou Bard de Google, utilisent des architectures de Transformers massives avec des milliards de paramètres.

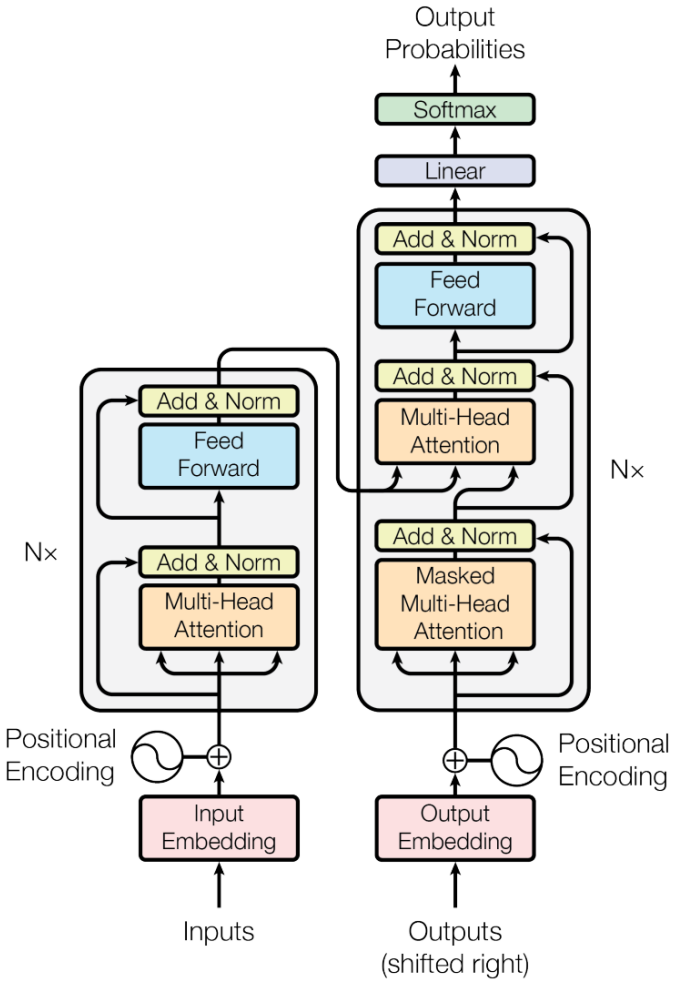

FIG. 2.7 : Architecture d'un reseau de neurones de transformation (Transformer) [VASWANI et al. 2017].

partie II

Contribution

Chapitre 3

Organisme d'accueil

3.1 Introduction

Dans ce chapitre, nous présenterons l'organisme qui nous a accueillis pour la réalisation de notre projet de fin d'études. Nous commencerons par une brève introduction de l'entreprise, en mettant en évidence son domaine d'activité et son positionnement sur le marché. Ensuite, nous détaillerons les différents services proposés par l'organisme, ainsi que son organigramme organisationnel. Cette présentation nous permettra de mieux comprendre l'environnement dans lequel notre projet s'est déroulé et les contraintes spécifiques auxquelles nous avons été confrontés.

3.2 Présentation de l'organisme d'accueil

STIE, ou Schneider Toshiba Inverter Europe SAS, est un département relié à Schneider Electric. Ce département offre une gamme complète d'équipements électroniques industriels. Il propose des inverseurs polyvalents, des variateurs de vitesse industriels, des composants de contrôle, et des produits de distribution électrique. STIE dispose également de laboratoires équipés de divers matériels, tels que des moteurs électriques et leurs dérivés, pour répondre aux besoins de ses clients à travers le monde. STIE est principalement basé à Pacy-sur-Eure et à Rueil-Malmaison.

Schneider Electric est un leader mondial de la technologie industrielle avec une expertise de référence dans l'électrification, l'automatisation, et la digitalisation des industries intelligentes, des infrastructures résilientes, des centres de données durables, des bâtiments intelligents, et des maisons intuitives. L'entreprise mène la transformation numérique de la gestion de l'énergie et des automatismes dans les secteurs résidentiel, des bâtiments, des centres de données, des infrastructures et des industries. Présente dans plus de 115 pays, Schneider Electric est le leader incontesté de la gestion électrique, couvrant la moyenne tension, la basse tension, l'énergie sécurisée, et les systèmes d'automatismes. La société fournit des solutions d'efficacité intégrées qui associent gestion de l'énergie, automatismes, et logiciels. L'écosystème qu'elle a construit lui permet de collaborer sur sa plateforme ouverte avec une large communauté de partenaires, d'intégrateurs, et de dé-

veloppeurs pour offrir à ses clients à la fois contrôle et efficacité opérationnelle en temps réel. La répartition géographique de son chiffre d'affaires est la suivante :

- France : 5,8%
- Europe de l'Ouest : 18,5%
- États-Unis : 27,9%
- Amérique du Nord : 4,2%
- Chine : 15,1%
- Asie-Pacifique : 15,2%
- Autres : 13,3%

3.3 Services

Schneider Electric propose une gamme étendue de produits et services innovants, notamment :

- **Produits d'automatisation et de contrôle** : Solutions complètes pour l'automatisation des processus et la gestion des systèmes de contrôle industriel.
- **Produits et systèmes basse tension** : Équipements pour la distribution électrique et la protection des installations basse tension.
- **Énergie solaire et stockage** : Solutions pour la production d'énergie solaire et le stockage d'énergie.
- **Distribution moyenne tension et automatisation du réseau** : Systèmes pour la distribution d'énergie moyenne tension et l'automatisation des réseaux électriques.
- **Énergie critique, refroidissement et racks** : Solutions pour la gestion de l'énergie critique, le refroidissement des infrastructures et les racks de serveur.

3.4 Organigramme de l'entreprise

3.5 Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil qui nous a permis de réaliser notre projet de fin d'études. Nous avons fourni une description détaillée de l'entreprise, de ses activités principales et de son positionnement sur le marché. Nous avons également mis en évidence les différents services proposés par l'organisme, ainsi que son organigramme organisationnel.

Cette présentation nous a permis de mieux comprendre l'environnement dans lequel notre projet s'est déroulé et les contraintes spécifiques auxquelles nous avons été confrontés. Les

Chapitre 4

Conception

4.1 Introduction

Le domaine de l'apprentissage profond a connu une grande croissance de la profondeur des architectures de réseaux de neurones. Cependant, cette croissante pose des défis importants en termes d'exigences de calcul et mémoire et de consommation d'énergie. Ainsi, la nécessité de concevoir des techniques efficaces de compression et d'optimisation des modèles est devenue primordiale. Dans ce chapitre, nous présenterons une méthode automatique pour l'elagage des réseaux neuronaux très profonds qui exploite l'apprentissage par renforcement et le plongement des couches du réseau.

4.2 Vue globale de la solution

Chapitre 5

Réalisation et tests

5.1 Introduction

Après avoir exposé en détail notre méthode automatique d'élagage dans le chapitre précèdent, nous discuterons maintenant sur les technologies et outils qui ont été choisis pour matérialiser cette approche et garantir son déploiement efficace. De ce fait, il est essentiel d'examiner en détail les langages de programmation, les bibliothèques et les frameworks qui ont été sélectionnés pour concrétiser notre approche. Nous offrons également un aperçu des stratégies de test que nous avons employées pour évaluer la performance de notre solution. Ces tests ont été établis pour mesurer les performances des modèles VGG-19 et ResNet-34 et la précision de chacun.

5.2 Modèles et jeu de données utilisés

Notre méthode d'élagage a été conçue pour élaguer les réseaux de neurones comportant seulement deux types de couches : les couches de convolution et les couches entièrement connectées. C'est pourquoi nous avons choisi d'utiliser des modèles tels que VGG-19 et ResNet-34. Dans cette section, nous parlerons de l'architecture et de l'organisation de ces deux modèles ainsi que le jeu de données CIFAR-10 qui est utilisé pour les entraîner.

5.2.1 CIFAR-10

CIFAR-10 [1] est un jeu de données qui est souvent utilisé dans le domaine de la vision par ordinateur. Il se compose d'un total de 60 000 images en couleur de 32x32 pixels chacune, réparties en 10 classes différentes, avec 6 000 images par classe [Krizhevsky et al. 2009]. Ces 10 classes d'images comprennent : des avions, des automobiles, des oiseaux, des chats, des cerfs, des chiens, des grenouilles, des chevaux, des bateaux et des camions (5.1).

[1] acronyme qui représente le "Canadian Institute for Advanced Research" (Institut canadien de recherches avancées)

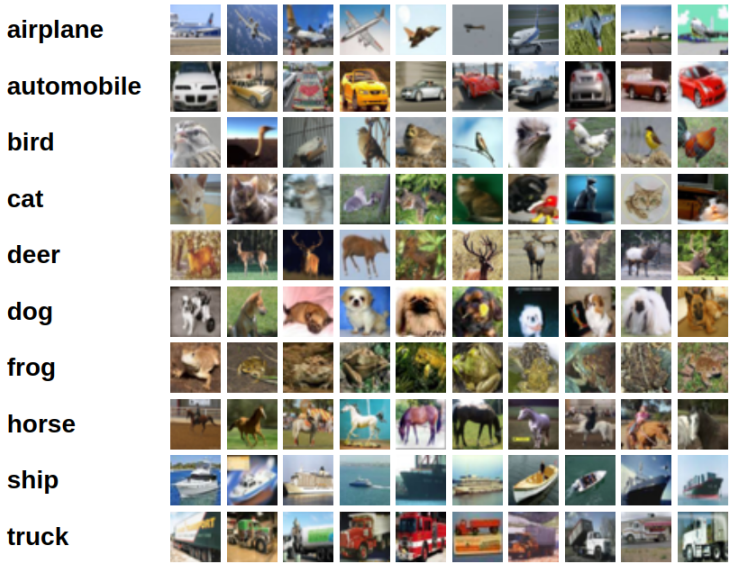

FIG. 5.1 : Les classes du jeu de données CIFAR-10.

Le dataset est divisé en deux ensemble : un ensemble d'entraînement et un ensemble de test. L'ensemble d'entraînement est composé de 50 000 images, tandis que l'ensemble de test est composé de 10 000 images. Dans ce dataset, les images sont de résolution relativement basse et présentent une variabilité dans les poses, l'éclairage, les arrière-plans et les détails, ce qui rend le dataset proche des défis du monde réel. Il est souvent utilisé pour l'entraînement, l'évaluation et la comparaison des performances des algorithmes de classification d'images et des réseaux de neurones convolutionnels (CNN), et il permet de reconnaître leur capacité à généraliser à partir d'un ensemble d'apprentissage limité [KRIZHEVSKY et al. 2009].

5.2.2 VGG-19

VGG-19 [2] est un réseau de neurones convolutif (CNN) très profond qui possède plus de 19,6 milliards de FLOPs et est utilisé fréquemment dans le domaine de la vision par ordinateur. Il est composé de 19 couches, comprenant 16 couches de convolution et 3 couches entièrement connectées, et les images en entrée sont généralement de taille 224x224 pixels. Le réseau commence par des couches de convolutions successives, qui sont suivies de couches de pooling (de type max pooling). Ces dernières permettent de réduire la dimension spatiale de la sortie en ne conservant que les informations les plus importantes [SIMONYAN et al. 2014].

Chaque couche de convolution est composée de plusieurs filtres (ou noyaux) 3x3 et un padding (stride) de 1 pour préserver les dimensions. Les filtres possèdent 64, 128, 256, 512 et 512 canaux respectivement. Le nombre de canaux augmente à mesure que l'on progresse dans le réseau. tandis que dans les couches de pooling, on a des fenêtres de 2x2 et un décalage de 2 pour réduire la résolution spatiale [SIMONYAN et al. 2014].

Une fois que les données sont réduites en termes de dimensions spatiales, elles sont

[2] acronyme de "Visual Geometry Group" (famille des modèles développés par l'Université d'Oxford)

passées à travers plusieurs couches entièrement connectées afin d'effectuer la classification, en associant les caractéristiques apprises aux classes d'objets. La dernière couche de sortie possède le même nombre de neurones que de classes dans le jeu de données. Elle utilise une fonction d'activation softmax pour obtenir des probabilités normalisées pour chaque classe. Dans les couches de convolution, les fonctions d'activation utilisées sont des fonctions ReLU (Rectified Linear Unit) [Simonyan et al. 2014].

ConvNet Confguration					
A	A-LRN	B	C	D	E
11 weight layers	11 weight layers	13 weight layers	16 weight layers	16 weight layers	19 weight layers
input(224 x 224 RGB image)					
conv 3-64	conv 3-64 **LRN**	conv 3-64 **conv 3-64**	conv 3-64 conv 3-64	conv 3-64 conv 3-64	conv 3-64 conv 3-64
maxpool					
conv 3-128	conv 3-128	conv 3-128 **conv 3-128**	conv 3-128 conv 3-128	conv 3-128 conv 3-128	conv 3-128 conv 3-128
maxpool					
conv 3-256 conv 3-256	conv 3-256 conv 3-256	conv 3-256 conv 3-256	conv 3-256 conv 3-256 **conv 1-256**	conv 3-256 conv 3-256 **conv 3-256**	conv 3-256 conv 3-256 conv 3-256 **conv 3-256**
maxpool					
conv 3-512 conv 3-512	conv 3-512 conv 3-512	conv 3-512 conv 3-512	conv 3-512 conv 3-512 **conv 1-512**	conv 3-512 conv 3-512 **conv 3-512**	conv 3-512 conv 3-512 conv 3-512 **conv 3-512**
maxpool					
conv 3-512 conv 3-512	conv 3-512 conv 3-512	conv 3-512 conv 3-512	conv 3-512 conv 3-512 **conv 1-512**	conv 3-512 conv 3-512 **conv 3-512**	conv 3-512 conv 3-512 conv 3-512 **conv 3-512**
maxpool					
FC-4096					
FC-4096					
FC-1000					
soft-max					

Tab. 5.1 : Les configurations des réseaux VGG (illustrées dans des colonnes selon leurs profondeurs). La colonne E représente la configuration du modèle VGG-19 utilisé [Simonyan et al. 2014].

5.2.3 ResNet-34

ResNet-34 est un réseau de neurones résiduel profond, composé de 34 couches et possédant plus de 3,6 milliards de FLOPs. Ce type de réseau est caractérisé par l'utilisation de blocs résiduels, en introduisant des connexions résiduelles, également appelées connexions "skip", qui sautent une ou plusieurs couches. Cette caractéristique permet d'exploiter les avantages de la profondeur tout en évitant les problèmes de dégradation de performance qui surviennent lorsque les réseaux deviennent plus profonds [He et al. 2016].

Le bloc résiduel de base dans ResNet-34 comprend deux couches de convolution 3x3 accompagnées de fonctions d'activation ReLU, et intègre une connexion résiduelle qui agit comme un raccourci autour des couches de convolution, en ajoutant la sortie de la première couche de convolution à la sortie de la deuxième couche.

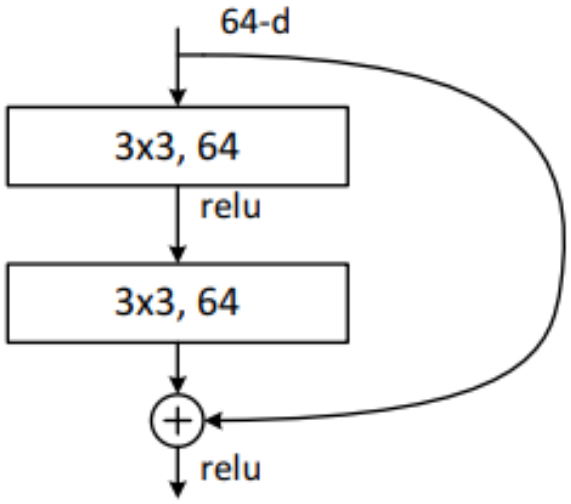

Fig. 5.2 : Un bloc résiduel de base comme sur la figure 5.3 pour ResNet-34 [He et al. 2016].

La fin du réseau ResNet-34 comprend une couche de classification entièrement connectée avec autant de neurones que de classes dans le jeu de données. Une fonction d'activation softmax est généralement utilisée pour obtenir les probabilités de classe normalisées.

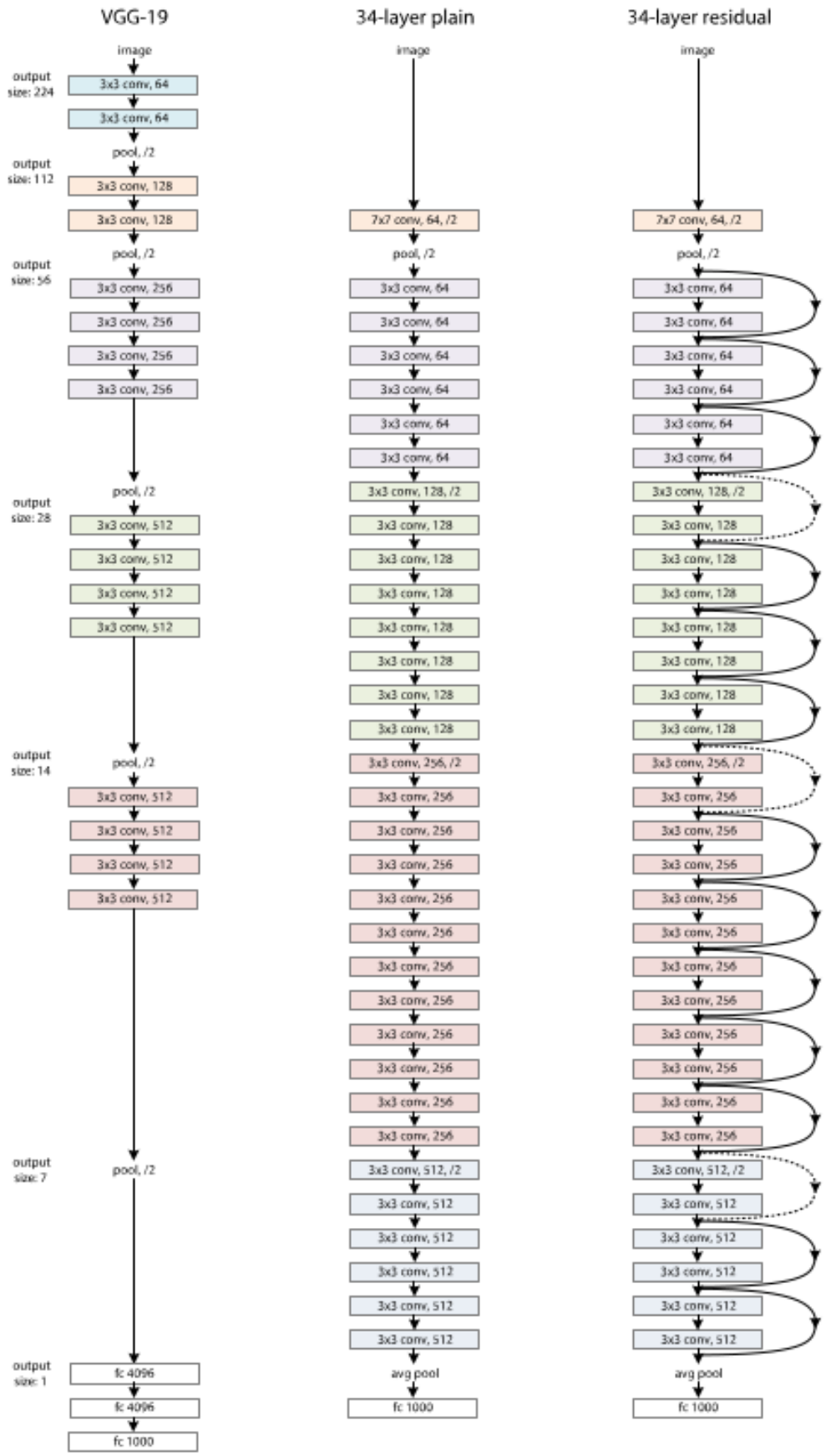

FIG. 5.3 : Les architectures des modèles utilisés. A gauche : le modèle VGG-19. Au milieu : un réseau simple de 34 couches. À droite : le modèle ResNet-34 [HE et al. 2016].

5.3 Technologies utilisées

5.3.1 Python

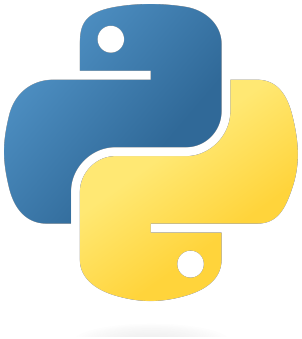

Fig. 5.4 : Python.

Python joue un rôle important dans le domaine de l'intelligence artificielle (IA) grâce à sa polyvalence, sa simplicité et sa richesse en bibliothèques spécialisées. En tant que langage de programmation, Python est devenu le premier choix pour de nombreux chercheurs, ingénieurs et développeurs travaillant dans le domaine de l'IA. D'une part, Python est connu pour sa syntaxe claire et lisible, ce qui permet aux nouveaux arrivants dans le domaine de l'IA de se familiariser rapidement avec les concepts de base. D'autre part, Python offre plusieurs bibliothèques et frameworks spécialisés dans l'IA, tels que TensorFlow, Keras, PyTorch et Scikit-learn. Ces bibliothèques sont souvent utilisées pour le développement de réseaux de neurones, d'algorithmes d'apprentissage automatique et d'autres techniques d'IA. Finalement, Python est un langage polyvalent qui permet aux développeurs de créer et tester différentes approches rapidement.

5.4 Bibliothèque utilisées

Python offre une riche collection de bibliothèques spécialisées dans plusieurs domaines, en particulier l'IA. Ces bibliothèques offrent des outils et des frameworks puissants pour développer des modèles d'apprentissage automatique, des réseaux de neurones, et bien plus encore. Dans cette section, nous allons explorer les bibliothèques que nous avons utilisé pour implémenter et tester notre méthode.

5.4.1 NumPy

Fig. 5.5 : NumPy.

NumPy [3] est une bibliothèque open source qui offre de nombreuses fonctionnalités pour le calcul numérique en Python. Elle offre un support puissant pour la manipulation de tableaux multidimensionnels, ainsi que pour l'exécution de calculs mathématiques complexes sur ces tableaux. Ces tableaux multidimensionnels permettent de stocker et de manipuler efficacement des données numériques sous forme de matrices et de vecteurs. Elle fournit également des fonctions mathématiques de base, des opérations d'algèbre linéaire, des opérations sur les tableaux, des fonctions statistiques et bien plus encore. Elle est largement utilisé en IA pour le traitement et la manipulation de données, la préparation de jeux de données, ainsi que pour la mise en œuvre d'algorithmes d'apprentissage automatique et de réseaux de neurones. La performance élevée de NumPy en calcul numérique en fait un bon choix pour les tâches intensives en termes de calcul.

5.4.2 Matplotlib

Fig. 5.6 : Matplotlib.

Matplotlib est une bibliothèque de visualisation en Python qui aide à créer des graphiques et des visualisations de données de manière interactive et statique. Cette bibliothèque offre un large éventail d'outils pour générer des graphiques de haute qualité à partir de données numériques. Son objectif est de permettre aux utilisateurs de représenter visuellement des données complexes de manière claire et compréhensible. Pour cela, elle propose une grande variété de types de graphiques, tels que les graphiques linéaires, les graphiques en barres, les graphiques à secteurs, les graphiques de dispersion, les graphiques 3D, etc. Elle permet également de personnaliser presque tous les aspects des

[3] acronyme de "Numerical Python"

graphiques, y compris les étiquettes, les couleurs, les styles de ligne, les titres, les axes et les légendes. L'utilisation de Matplotlib est essentielle dans l'analyse de données, la science des données et la recherche en général. En intelligence artificielle et en apprentissage automatique, Matplotlib est souvent employé pour visualiser les performances des modèles, les distributions de données, les tendances, les caractéristiques importantes, les matrices de confusion, les courbes d'apprentissage, etc.

5.4.3 Pytorch

Fig. 5.7 : Pytorch.

PyTorch est une bibliothèque open-source d'apprentissage automatique et d'intelligence artificielle en Python, développée principalement par Facebook's AI Research lab (FAIR). Elle repose sur un concept fondamental appelé "tenseur", qui est une structure de données multidimensionnelle similaire aux tableaux NumPy et elle est conçue pour faciliter le développement et la mise en œuvre de modèles de réseaux de neurones profonds. PyTorch est surtout distinguée par sa prise en charge des calculs automatiques de gradients, ce qui signifie qu'il est possible de définir des opérations mathématiques sur les tenseurs et que PyTorch peut automatiquement calculer les gradients de ces opérations qui sont nécessaires pour ajuster les poids dans les réseaux de neurones et ainsi minimiser une fonction de perte. Elle est utilisé pour la conception des modèles de réseaux de neurones profonds, y compris les réseaux de neurones convolutionnels (CNN), les réseaux de neurones récurrents (RNN), les transformeurs, etc.

5.4.4 Torchvision

Fig. 5.8 : Torchvision.

Torchvision est une bibliothèque qui fait partie de PyTorch. Elle est spécifiquement conçue pour faciliter le chargement et la transformation de jeux de données d'images couramment utilisés dans le domaine de l'apprentissage automatique et de la vision par ordinateur. Elle offre des outils pour prétraiter les données d'image, créer des ensembles de données, appliquer des transformations aux images et charger des ensembles de données préexistants. Elle propose des classes pour charger facilement des ensembles de données standard tels que MNIST, CIFAR-10, ImageNet, etc. Elle permet également d'appliquer diverses transformations aux images, telles que le redimensionnement, le recadrage, la normalisation, les rotations, les miroirs, etc. qui sont utiles pour augmenter la variabilité des données.

5.4.5 NNI

Fig. 5.9 : NNI (Neural Network Intelligence).

NNI (Neural Network Intelligence) est une bibliothèque open-source développée par Microsoft Research. Elle fournit un ensemble d'outils et de bibliothèques pour faciliter l'exploration et l'optimisation des espaces d'hyperparamètres, ainsi que pour la recherche automatique d'architectures de modèles. Elle permet aux utilisateurs de définir un espace de recherche pour les hyperparamètres, tels que les taux d'apprentissage, les tailles de lot, les architectures de couches, etc. NNI exécute ensuite des expériences en utilisant différentes configurations d'hyperparamètres et rapporte les résultats, y compris les performances du modèle. Elle est très utile dans le domaine de l'apprentissage automatique, car elle simplifie et automatise le processus d'ajustement des hyperparamètres et d'exploration des architectures, ce qui peut considérablement accélérer le développement de modèles performants.

5.5 Outils utilisés

5.5.1 Google Colab

Fig. 5.10 : Google Colab.

Google Colab (abrégé de Colaboratory) est une plateforme de notebooks interactifs basée sur le cloud, développée par Google. Elle permet aux utilisateurs d'écrire, d'exécuter et de partager du code Python de manière collaborative, sans nécessiter de configuration ou d'installation. Elle propose des notebooks interactifs qui permettent d'insérer des cellules de code exécutable et des cellules de texte et chaque notebook Colab s'exécute dans un environnement virtuel où les utilisateurs peuvent accéder à la puissance de calcul des processeurs graphiques (GPU) et des unités de traitement tensoriel (TPU) pour accélérer l'entraînement de modèles d'apprentissage automatique. Elle propose également de nombreuses bibliothèques préinstallées, mais les utilisateurs peuvent également installer et utiliser des bibliothèques tierces via des commandes simples.

5.5.2 Google Drive

Fig. 5.11 : Google Drive.

Google Drive est un service de stockage en ligne développé par Google pour stocker, synchroniser et partager des fichiers et des dossiers sur le cloud. Il offre une variété de fonctionnalités telles que le stockage en ligne, la synchronisation multi-appareils, le partage de fichiers, la collaboration en temps réel, etc. De plus, il peut être utilisé avec Google Colab.

5.6 Tests et résultats

Cette dernière section présente une analyse des résultats obtenus après avoir tester notre méthode d'élagage. Nous effectuons nos expérimentations sur CIFAR-10 avec deux réseaux profonds classiques : VGG-19 et ResNet-34. Les résultats obtenus sont examinés et comparés avec les résultats des autres méthodes d'élagage, permettant ainsi de dégager des conclusions quant à la performance et l'efficacité de notre méthode. Cette section donc vise à présenter de manière claire et précise les découvertes issues de ces tests.

Le processus d'exécution des tests est décrit comme suit :

1. Entraînement du modèle jusqu'à la convergence
2. Élagage du modèle avec les pourcentages d'élagage fournis par l'agent DDPG
3. Réglage fin du modèle
4. Mesure de la précision, la taille, le nombre de paramètres, etc. du modèle élagué
5. Comparaison du modèle élagué avec le modèle original

On élague les canaux dont les poids ont la plus petite valeur absolue. Le pourcentage d'élagage maximum a_{max} est fixé pour les couches de convolution à 0,8 et pour la couche entièrement connectée à 0,98. Cette limite supérieure a_{max} est utilisée uniquement pour accélérer la recherche. Nous pouvons simplement prendre $a_{max} = 1$ et nous aurons des résultats similaires. Le réseau d'acteurs μ comporte deux couches cachées, chacune comportant 300 neurones et la couche de sortie finale est une couche sigmoïde pour délimiter les actions dans la plage (0, 1). Le réseau critique Q comportait également deux couches cachées, chacune comptant 300 unités. Nous entraînons le réseau avec 64 comme batch size. L'agent DDPG explore d'abord 100 épisodes avec un bruit constant $\sigma = 0.5$, puis exploite 300 épisodes avec un bruit σ qui décroît de manière exponentielle.

Pour évaluer la performance de notre méthode, nous l'avons comparée avec les deux méthodes d'élagage citées dans la première partie du rapport : ABCPruner [Lin et al. 2020] et CCPrune [Chen et al. 2021]. Ces deux méthodes sont des méthodes automatique qui utilisent le même type d'élagage (élagage des canaux). ABCPruner est une méthode basée sur l'algorithme de colonie d'abeilles artificielles (ABC). Dans cette méthode, la recherche du réseau élagué optimal est formulée comme un problème d'optimisation et l'algorithme ABC est utilisé pour le résoudre de manière automatique afin de réduire les interférences humaines. CCPrune (Collaborative Channel Pruning) est une autre méthode qui utilise aussi l'élagage des canaux. Cette méthode introduit d'abord la régularisation sur les poids des couches de convolution et les facteurs d'échelle de la couche BN (Batch Normalization) respectivement, puis elle combine les poids de la couche de convolution et le facteur d'échelle de la couche BN pour évaluer l'importance du canal.

5.6.1 VGG-19

Le tableau suivant représente les résultats après l'application de notre méthode sur VGG-19 avec une comparaison aux deux autres méthodes d'élagage : ABCPruner et CCPrune.

Méthode	Précision (%)	FLOPs (%)	Paramètres (%)	Taille (MB)
Modèle original	93.71	-	-	548
ABCPruner	93.08	73.68	88.68	62.6
CCPrune	**93.78**	48.92	86.82	77.2
Notre méthode	90.6	91.6	90.2	**52.7**

Tab. 5.2 : Résultats d'élagage de VGG-19 sur CIFAR-10. La deuxième colonne indique la précision du modèle. Les troisième et quatrième colonnes indiquent le taux d'élagage des FLOPs et le taux d'élagage des paramètres. La dernière colonne indique la taille du modèle.

Les résultats dans le tableau 5.2 montrent que les techniques ABCPruner et CCPrune atteignent toujours une précision très proche du réseau original qui est aussi meilleure que celle de notre méthode. Cependant, notre méthode dépasse ces techniques quand nous parlons de la taille du modèle. Nous remarquons qu'avec notre méthode, nous pouvons d'avoir une grande réduction dans la taille du modèle (la taille est 10 fois moins que le modèle original) et dans le nombre de FLOPs et paramètres à cause des pourcentages d'élagage élevés. Cette réduction du nombre de FLOPs signifie que notre méthode effectue moins de calculs que les deux autres méthodes. Nous pouvons donc avoir le meilleur temps d'inférence avec notre méthode. Nous pouvons aussi remarquer que l'utilisation de l'élagage structuré engendre une petite dégradation de la précision des modèles élagués par rapport au modèle original. Cette dégradation est causée par la suppression de canaux entiers, ce qui peut causer une suppression de certains paramètres importants qui peuvent se trouver dans l'un des canaux éliminées.

La figure 5.12 montre les statistiques des canaux restants dans les couche de convolution dans le modèle VGG-19. Sur cette figure, Nous pouvons clairement comprendre la structure du réseau après l'élagage.

Dans VGG-19, 90% des poids sont dans les couches entièrement connectées. Dans notre méthode, nous avons utilisé l'élagage de canaux entiers en couches de convolution et cela a un effet secondaire intéressant en réduisant également la mémoire. Comme observé dans Molchanov et al. 2016, plus la couche est profonde, plus elle sera élaguée. Cela signifie que la dernière couche de convolution sera beaucoup élaguée et que de nombreux neurones de la couche entièrement connectée qui la suit seront également supprimés.

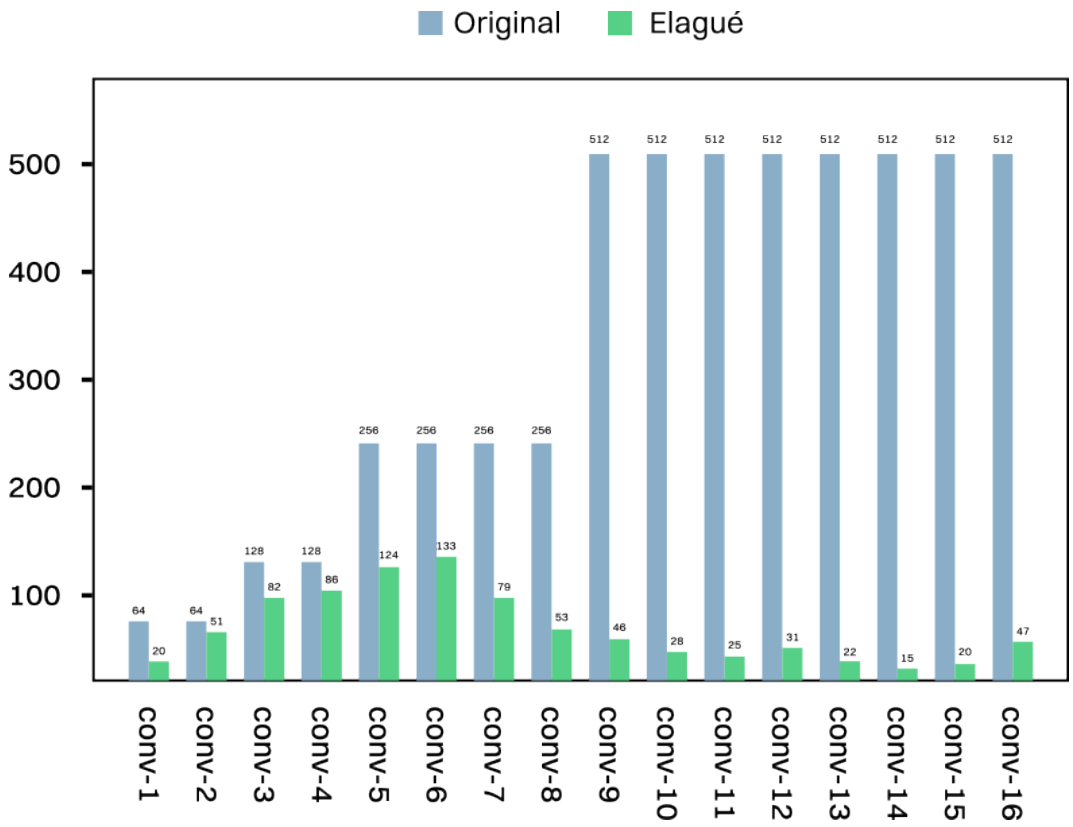

Fig. 5.12 : Statistiques des canaux restants dans les couches de convolution de VGG-19.

5.6.2 ResNet-34

Le tableau suivant représente les résultats après l'application de notre méthode sur ResNet-34 et une comparaison avec les deux autres méthodes d'élagage utilisées : ABC-Pruner et CCPrune.

Méthode	Précision (%)	FLOPs (%)	Paramètres (%)	Taille (MB)
Modèle original	91.45	-	-	81.4
ABCPruner	89.69	58.97	51.76	39.2
CCPrune	**90.76**	57.55	34.78	53.0
Notre méthode	86.21	58.09	67.63	**26.5**

Tab. 5.3 : Résultats d'élagage de ResNet-34 sur CIFAR-10. La deuxième colonne indique la précision du modèle. Les troisième et quatrième colonnes indiquent le taux d'élagage des FLOPs et le taux d'élagage des paramètres. La dernière colonne indique la taille du modèle.

Les résultats dans le tableau 5.3 sont les même que ceux du modèle VGG-19. Ils montrent toujours que la précision dans les techniques ABCPruner et CCPrune dépasse la précision dans notre méthode. Cependant, notre méthode dépasse ces deux techniques dans la compression de la taille du modèle et dans le nombre de FLOPs, ce qui nous donnera un meilleur temps d'inférence. Nous remarquons aussi que la taille du modèle élagué avec notre méthode est presque 3 fois moins que le modèle original, ainsi que le nombre de FLOPs et paramètres (les résultats sont résumés dans la figure 5.13). Nous

avons aussi vu que l'élagage structuré réduit légèrement la précision des modèles élagués par rapport au modèle original et la cause de cette réduction est la même cause mentionnée dans l'interprétation de l'élagage structuré pour le modèle VGG-19.

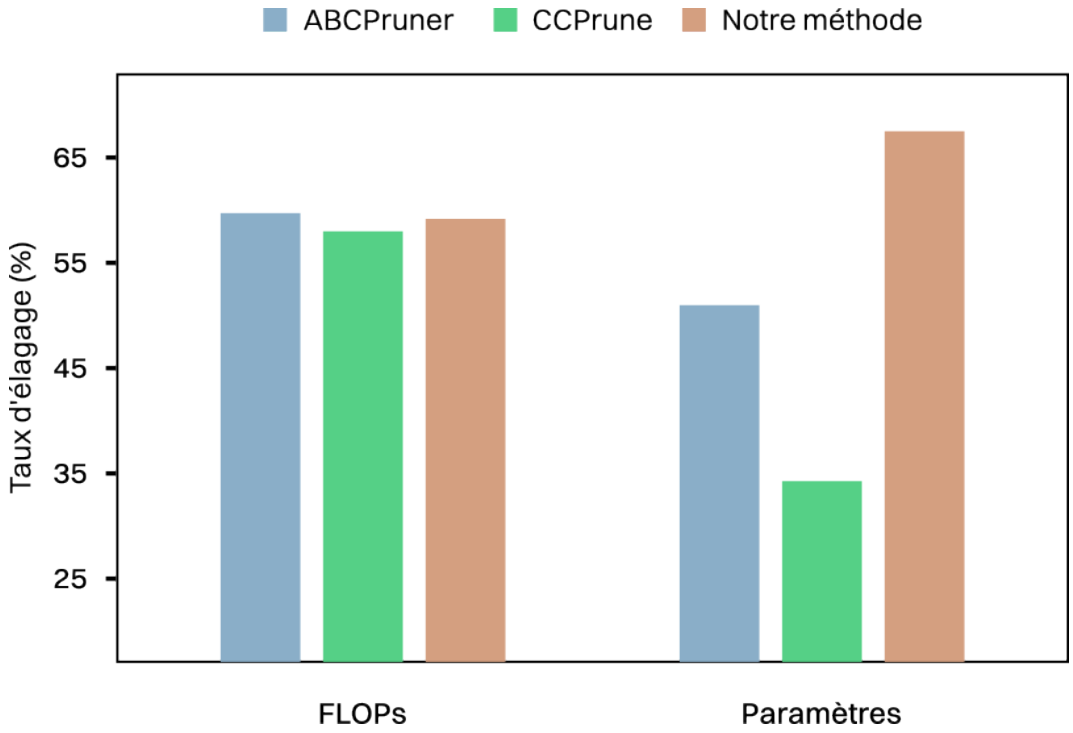

Fig. 5.13 : Comparaison entre les taux d'élagage des FLOPs et des paramètres des trois méthodes d'élagage pour le réseau ResNet-34.

5.7 Conclusion

En conclusion de ce chapitre dédié aux tests et résultats, l'analyse des résultats d'expérimentations menées sur les modèles VGG-19 et ResNet-34 prouvent l'efficacité de notre méthode d'élagage automatique. Nous avons trouvé que notre méthode permet de réduire significativement la taille des modèles et le nombre de FLOPs, en surpassant les deux méthodes utilisées pour la comparaison (ABCPruner et CCPrune). Ces réductions nous permettent d'avoir de très petits modèles qui sont également très performants et faciles à déployer sur des appareils limités en termes de ressources de calcul et de stockage. Cependant, il est important de souligner que le processus d'élagage n'est pas sans compromis. Les avantages en termes de taille sont parfois accompagnés d'une petite dégradation de la précision qui nécessite de faire un réglage fin après l'élagage afin de restaurer partiellement les performances du modèle initial. De plus, le taux d'élagage optimal peut varier en fonction du même jeu de données et des spécificités de la tâche.

On a également présentée au début du chapitre les modèles utilises pour tester la méthode (VGG-19 et ResNet-34) et le jeu de données utilisé (CIFAR-10) pour l'entraînement de ces modèles, ainsi que les différents technologies et outils utilisés pour la conception de notre méthode. Nous avons utilisé le langage de programmation Python avec plusieurs

bibliothèques telles que NumPy, Matplotlib, Pytorch, etc. Ces bibliothèques offrent des outils puissants pour développer et entraîner les différents types de réseaux de neurones.

Enfin, ce chapitre constitue une étape essentielle de ce rapport en fournissant des résultats d'implémentation des concepts et des théories énoncés dans le chapitre précédent. Les résultats obtenus offrent des orientations pratiques pour les applications et les améliorations futures de cette méthode pour élaguer des réseaux de neurones profonds. En considérant ces résultats, la rapport se tourne vers la section finale, où les conclusions et perspectives globales sont tirées.

Conclusion et perspectives

Avec l'augmentation de la profondeur des architecture des réseaux de neurones, le nombre de calculs et la taille des réseaux augmentent également, ce qui rend leurs déploiement sur des appareils dotés d'un matériel limité très difficile et compliqué. L'élagage a émergé comme une approche pour réduire la complexité de ces réseaux profonds. Cependant, cette approche prend beaucoup de temps et nécessite des experts humains afin de bien élaguer un réseau. En raison de ses défauts, des méthodes automatiques utilisant l'apprentissage par renforcement sont apparues. Ces méthodes fournissent des résultats exceptionnels et ont la capacité à s'adapter à une grande variété d'environnements en utilisant des configurations appropriées. Cependant, les algorithmes d'apprentissage par renforcement ne peuvent pas prendre en entrée un réseau profond complet car il est très complexe. Il est donc nécessaire d'utiliser des structures moins complexes comme entrée telles que le plongement de graphe, de chouche, de noeuds, etc. Le plongement est un vecteur unidimentionnel qui garde seulement les informations importantes dans le réseau. En transformant ces données en un vecteur unidimensionnel, cet outil de plongement facilite grandement la capacité de l'agent d'apprentissage par renforcement à appréhender et à interagir avec son environnement.

Dans ce rapport, nous avons découvert les différentes techniques d'élagage des réseaux de neurones, ainsi que les types de plongements et les différents aspects des algorithmes d'apprentissage par renforcement. Nous avons commencé le rapport par une introduction au domaine d'apprentissage profond où nous avons vu quelques définitions et concepts de base, tels que les poids, les connexions, les types de réseaux de neurones, les différents types d'apprentissage (supervisé, non-supervisé, semi-supervisé et par renforcement), etc. Ensuite, nous avons présenté quelques concepts et algorithmes de l'apprentissage par renforcement, tels que les processus de décision de Markov, l'apprentissage Q profond, etc. Nous avons également parlée sur les graphes et les différentes techniques de plongement, ainsi que l'hypothèse du ticket de loterie et les types d'élagage des réseaux de neurones.

On a parlé de tout cela juste pour acquérir suffisamment de connaissances pour pouvoir élaborer une nouvelle approche d'élagage des réseaux de neurones profonds, en utilisant les techniques de plongement de couches et un algorithme d'apprentissage par renforcement complexe pour nous fournir les pourcentage d'élagage du modèle, pour arriver enfin à un modèle de taille considérablement réduite et avec une réduction minimale de la précision. Nous avons commencé par la présentation des modèles testés et le jeux de données utilisée pour les entraîner. Puis, nous avons présenté une vue global de la solution et ensuite les détails de chaque étape de la solution, qui commence par la construction du plongement et finit par le réglage fin. Enfin, nous avons vu les différents résultats d'application de notre méthode sur les modèles et nous les avons comparés avec les résultats de quelques

méthodes performantes.

L'avantage le plus important de notre méthode est qu'elle permet de réduire considérablement la taille des modèles et le nombre de calculs, ce qui est idéal pour déployer ces modèles sur des appareils dotés d'un matériel limité. Toutefois, cet avantage est parfois accompagné d'une petite dégradation de la précision, ce qui nécessite de faire un réglage fin après l'élagage afin de restaurer partiellement la précision du modèle initial.

Même si notre méthode donne de très bons résultats, des améliorations sont encore possibles. Nous pouvons apporter ces améliorations à différentes parties de notre processus d'élagage. Par exemple, nous pouvons essayer de généraliser notre méthode à d'autres types d'architectures de réseau autres que les réseaux convolutifs et résiduels. Nous pouvons également modifier l'algorithme d'élagage de l'élagage des canaux vers un autre type d'élagage qui peut contribuer à augmenter la précision de nos modèles. Nous pouvons également essayer de faire d'autres types de plongement, tels que le plongement de l'ensemble du réseau, et utiliser d'autres algorithmes d'apprentissage par renforcement, tels que PPO ou A3C, ou même essayer un algorithme d'optimisation. Nous pouvons aussi essayer de faire l'élagage au début ou pendant l'entraînement afin d'éviter l'étape de réglage fin qui peut prendre du temps pour le ré-entraînement.

Perspectives

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin posuere euismod neque, non semper nibh viverra sed. Praesent ut varius magna. Fusce ipsum ante, semper nec interdum at, semper et lacus. Nulla ultrices magna a fringilla finibus. Etiam sollicitudin blandit ante. Vivamus blandit rhoncus tincidunt. Morbi sit amet congue purus. Praesent interdum gravida congue. Donec fermentum dui fermentum maximus rutrum. :

- Le développement d'une application mobile pour l'animateur de zone :

  Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin posuere euismod neque, non semper nibh viverra sed. Praesent ut varius magna. Fusce ipsum ante, semper nec interdum at, semper et lacus. Nulla ultrices magna a fringilla finibus. Etiam sollicitudin blandit ante. Vivamus blandit rhoncus tincidunt. Morbi sit amet congue purus. Praesent interdum gravida congue. Donec fermentum dui fermentum maximus rutrum.

- L'amélioration de l'algorithme d'optimisation :

  Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin posuere euismod neque, non semper nibh viverra sed. Praesent ut varius magna. Fusce ipsum ante, semper nec interdum at, semper et lacus. Nulla ultrices magna a fringilla finibus. Etiam sollicitudin blandit ante. Vivamus blandit rhoncus tincidunt. Morbi sit amet congue purus. Praesent interdum gravida congue. Donec fermentum dui fermentum maximus rutrum.

Appréciation personnelle

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin posuere euismod neque, non semper nibh viverra sed. Praesent ut varius magna. Fusce ipsum ante, semper nec interdum at, semper et lacus. Nulla ultrices magna a fringilla finibus. Etiam sollicitudin blandit ante. Vivamus blandit rhoncus tincidunt. Morbi sit amet congue purus. Praesent interdum gravida congue. Donec fermentum dui fermentum maximus rutrum.

Bibliographie

Aggarwal, Charu C. (2018). *Neural networks and deep learning : A textbook*. Springer.

Alharbi, Nouf Fahad et Nabil M. Hewahi (2021). "Exploring deep neural network capability for intrusion detection using different mobile phones platforms". In : *International Journal of Computing and Digital Systems* 10.1, p. 1391-1406.

Amini, Alexander et al. (2018). "Spatial uncertainty sampling for end-to-end control". In : *arXiv preprint arXiv :1805.04829*.

Bishop, Christopher M. (2016). *Pattern recognition and machine learning*. Springer New York.

Brown, Tom B et al. (2020). "Language models are few-shot learners". In : *arXiv preprint arXiv :2005.14165*.

Chen, Yanming et al. (2021). "CCPrune : Collaborative channel pruning for learning compact convolutional networks". In : *Neurocomputing* 451, p. 35-45.

Dong, Peijie et al. (juin 2022). "Prior-guided one-shot neural architecture search". In : *arXiv.org*.

Fawaz, Hassan Ismail et al. (2019). "A survey on long short-term memory networks for time series prediction". In : *Physica A : Statistical Mechanics and its Applications* 534, p. 122-315.

Feng, Jie et al. (2020). "Generative Adversarial Networks based on collaborative learning and attention mechanism for hyperspectral image classification". In : *Remote Sensing* 12.7, p. 1149.

Feng, Junxi et al. (2019). "Reconstruction of Porous Media from extremely limited information using conditional generative adversarial networks". In : *Physical Review E* 100.3.

Goodfellow, Ian, Yoshua Bengio et Aaron Courville (2016). *Deep Learning*. MIT Press.

Goodfellow, Ian et al. (2014). "Generative adversarial nets". In : *Advances in neural information processing systems*, p. 2672-2680.

He, Kaiming et al. (juin 2016). "Deep Residual Learning for Image Recognition". In : *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

Ho, Jonathan, Ajay Jain et Pieter Abbeel (2020). "Denoising Diffusion Probabilistic Models". In : *arXiv preprint arXiv :2006.11239*.

Hochreiter, Sepp et Jürgen Schmidhuber (1997). "Long short-term memory". In : *Neural computation* 9.8, p. 1735-1780.

Hu, Rong et al. (2022). "A multi-attack intrusion detection model based on mosaic coded convolutional neural network and centralized encoding". In : *PLOS ONE* 17.5.

KARRAS, Tero, Samuli LAINE et Timo AILA (2019). "A style-based generator architecture for generative adversarial networks". In : *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, p. 4401-4410.

KIMURA, Nobuaki et al. (2019). "Convolutional neural network coupled with a transfer-learning approach for time-series flood predictions". In : *Water* 12.1, p. 96.

KINGMA, Diederik P. et Max WELLING (2012). "Auto-Encoding Variational Bayes". In.

KRIZHEVSKY, Alex et Geoffrey HINTON (2009). *Learning multiple layers of features from tiny images*. Rapp. tech. 0. Toronto, Ontario : University of Toronto.

KUMARASWAMY, Balachandra (2021). "Neural Networks for Data Classification". In : *Artificial Intelligence in Data Mining*, p. 109-131.

LIN, Mingbao et al. (2020). "Channel pruning via automatic structure search". In : *arXiv preprint arXiv :2001.08565*.

MCCULLOCH, Warren S. et Walter PITTS (1943). "A logical calculus of the ideas immanent in nervous activity". In : *The Bulletin of Mathematical Biophysics* 5.4, p. 115-133.

MOLCHANOV, Pavlo et al. (2016). "Pruning convolutional neural networks for resource efficient inference". In : *arXiv preprint arXiv :1611.06440*.

MUNIASAMY, Anandhavalli et al. (2020). "Deep Learning for Predictive Analytics in Healthcare". In : *The International Conference on Advanced Machine Learning Technologies and Applications (AMLTA2019)*. Sous la dir. d'Aboul Ella HASSANIEN et al. Cham : Springer International Publishing, p. 32-42.

NAVEED, Humza et al. (2023). "A Comprehensive Overview of Large Language Models". In : *arXiv preprint arXiv :2307.06435*.

ROSENBLATT, F. (1958). "The Perceptron : A probabilistic model for information storage and organization in the brain." In : *Psychological Review* 65.6, p. 386-408.

SIMONYAN, Karen et Andrew ZISSERMAN (2014). "Very deep convolutional networks for large-scale image recognition". In : *arXiv preprint arXiv :1409.1556*.

VASWANI, Ashish et al. (2017). "Attention is All you Need". In : *Advances in Neural Information Processing Systems*. Sous la dir. d'I. GUYON et al. T. 30. Curran Associates, Inc.

WIERING, Marco et Martijn van OTTERLO, éd. (2012). *Reinforcement Learning : State-of-the-Art*. Springer.

YANG SONG, Stefano Ermon (2022). "Diffusion Models : A Comprehensive Survey of Methods and Applications". In : *arXiv preprint arXiv :2209.00796*.

ZHOU, Jie et al. (2020). "Graph neural networks : A review of methods and applications". In : *AI Open* 1, p. 57-81.

Webographie

WANG, Phillip (2019). *This Person Does Not Exist*. https://thispersondoesnotexist.com. Accessed : 2024-08-03.