Ambient IT
128 Boulevard Macdonald
75019 Paris

Mail : formation@ambient-it.net
Tél : +33 (0)1 40 34 11 53

AMBIENT-IT

Formation Spécialisation et veille en Deep Learning

2 jours (14 heures)

Description

Dans la lignée de notre cours d'introduction, cette formation vise à parfaire les connaissances jusqu'à arriver aux sujets de pointe qui font aujourd'hui l'innovation du Deep Learning. De l'apprentissage auto supervisé ou Bayésien aux nouvelles possibilités d'entraînement sur des données encryptées, il s'agit ici de donner les solutions existantes, les limites connues et les pistes d'avancement qui demain bouleverseront le quotidien des data-scientists ou ingénieurs travaillant sur ces sujets.

Objectifs

- Mise à niveau de l'état de l'art de la recherche en Deep Learning (self-supervised, Bayesian, continual and security)
- Maîtrise des techniques de Deep Learning les plus récentes

Public visé

Développeurs, Architectes, Big Data Data Analyst / Data Engineer / Data Scientist

Pré-requis

- Connaissance de Python et en mathématique

Pour aller plus loin

- ? Notre certification au Deep Learning ?
- Nous vous proposons en introduction un formation sur l'Intelligence Artificielle
- En complément la technologie
  - TensorFlow de Google
  - Pytorch de Facebook

Programme de notre formation Introduction Spécialisation et veille en Deep Learning

[JOUR 1]

1. Apprentissage non supervisé ou auto-supervisé (Unsupervised & self-supervised learning)

- Présentation des approches, définition du self-supervised learning. Possibilités dans la gestion de datasets déséquilibrés ou imparfaits, comme dans la définition de nouvelles tâches
- Application à l'apprentissage de représentation d'images. Apprentissage automatique de features spécifiques, clustering non supervisé, apprentissage adversarial.
- Application à l'apprentissage de représentations de vidéos. Utilisation d'événements anormaux. Apprentissage non supervisé de mouvements.
- Apprentissage non supervisé de profondeur estimée sur une image.
- Gestion de problèmes de traduction par apprentissage non supervisé.
- Applications au Deep Reinforcement Learning

2. Bayesian Deep Learning

- Approche bayésienne et réseaux de neurones. Nécessité d'une incertitude dans les prédictions d'un réseau. Limites des approches comparées.
- Dropout : ré-interprétation de la méthode de régularisation en inférence Bayésienne. Reformulation.
- Variational AutoEncoder : approfondissement de l'architecture sous son approche Bayésienne. Extensions du VAE.
- Bayes by backprop : Multi-layer perceptron bayésien.
- Réseaux convolutifs bayésiens.

3. Continual Learning

- Présentation de l'apprentissage continu. Cas d'usages et limites. Oubli catastrophique d'un réseau.
- Spécialisation sur le transfert learning. Usages de base et spécialisations.
- Nouvelles métriques d'apprentissage continu.
- Framework Progress & Compress.
- Exemple d'architecture GAN continue : Deep Generative Replay.
- Meta learning : définition et principes. Applications aux réseaux de neurones.
- Lifelong learning : enjeux et review des solutions existantes.

4. Sécurité en Deep Learning

- Définition et analyse des attaques adversariales. Exemples sur l'image et le texte.
- Présentation des principales défenses trouvées et de leurs limites. Etat à date de la sécurité adversariale des réseaux.
- Recherche d'approches robustes d'apprentissage (Algorithme Sever).
- Exemple d'attaques adversariales sémantiques.
- Framework d'analyse de la sécurité d'un réseau de neurones.
- Considérations légales (US) sur le détournement par attaques adversariales d'un réseau de neurones.

[JOUR 2]

5. Optimisation de réseaux de neurones

- Techniques de pruning : considérations et comparaisons. Méthodes d'application
- Pruning sur un multi-layer perceptron.
- Pruning sur un réseau convolutif.
- Approche mobileNet : développement dédié aux périphériques mobiles.
- Exemples d'applications.

6. Deep learning et respect de la donnée privée

- Differential privacy : définition, applications fondamentales et limites
- Etude du framework tensorflow/privacy.
- Cas d'étude d'une application à la classification MNIST.
- Mesures de la capacité d'un réseau de neurones à "involontairement" retenir de la donnée.
- Capacité d'extraction d'informations à partir d'un réseau entraîné (Secret Sharer).
- Apprentissage de modèles récurrents du langage en Differential Privacy.
- Travail sur la donnée encryptée : présentation du framework tf-encrypted.
- Exemples d'utilisation et de travaux récents.

7. Graph Networks : un nouvel outil de modélisation

- Intérêts fondamentaux de pouvoir traiter des données sous forme de Graphe.
- Modélisations et représentations possibles.
- Approches particulières (message passing networks, Set Networks).
- Approche DeepMind GraphBlock, généralisation.
- Applications à différents problèmes : classification, analyse d'un système complexe, transformation.

8. Outils avancés de visualisation Deep Learning

- Lucid : outil de visualisation et d'interprétation Deep Learning. Exemples pratiques.
  - Visualisation de la diversité apprise d'un CNN.
  - Visualisation de régularisations.
  - Analyse de grilles d'activation.
  - Analyse des attributions spatiales et par canal.
  - Atlas d'activations : nouvelles visualisations et interprétations.
- Hierarchical Contextual Decomposition :
  - Détail de l'algorithme implémenté.
  - Application aux réseaux récurrents (détection de sentiment).
  - Application aux réseaux convolutifs (classification).

9. Spécialisations récentes Deep Reinforcement Learning

- Large-Scale Study of Curiosity-Driven Learning : exploitation d'un apprentissage sans récompense.
- Contingency-Aware Exploration in Reinforcement Learning.
- Contingency awareness. Architecture Attentive Dynamics Model. Expérimentations avec A2C et PPO.
- Deep Reinforcement Learning and the Deadly Triad : analyse de la "triade" d'échecs en DRL sur un algorithme Q-Learning classique.
- Deep Counterfactual Regret Minimization - Noam Brown et al.
- Approche de problèmes avec une information particulièrement imparfaite. Présentation du CFR et algorithme particulier.
- An Atari Model Zoo for Analyzing, Visualizing, and Comparing Deep Reinforcement Learning Agents.
- Banc de test d'algorithmes, gestion d'analyse et de visualisation d'approches DRL.

Sociétés concernées

Cette formation s’adresse aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiple permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.