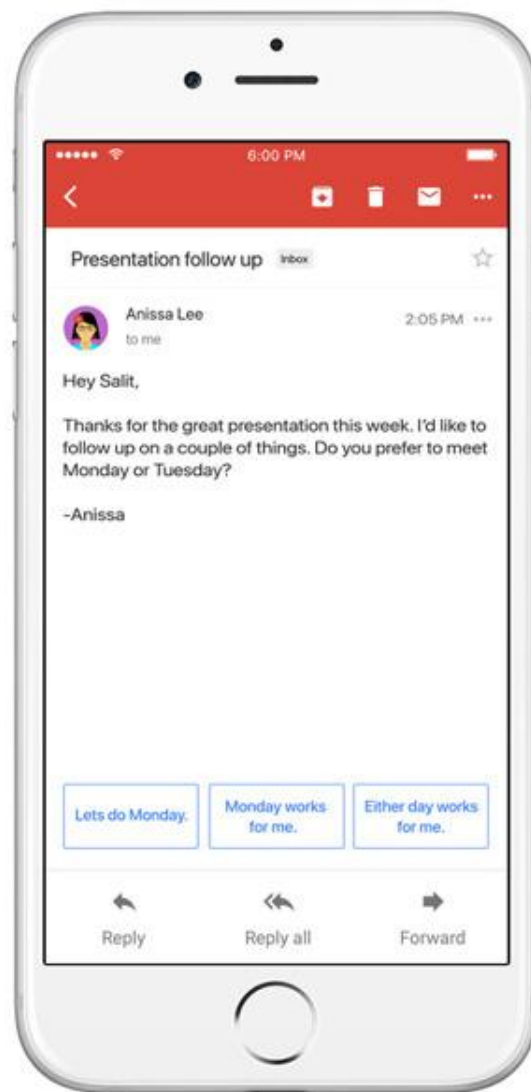


Synthèse sur le Machine Learning introduit au sein de Gmail



Par

Vincenzo DENIS

Etudiant en

M2 Développement Web & Management SI

I- Introduction

Le Machine Learning, ou encore, l'Apprentissage Automatique (Artificiel, Statistiques...) est un fondement contigu aux mathématiques et aux statistiques, se traduisant par de l'intelligence artificielle aux yeux de tous. Lors de la phase de conception d'un système sur l'IA on parlera de capacité à apprendre qu'on attribue aux ordinateurs, en se basant sur des observations et nombres finis à disposition. L'ajout d'un outil de Machine Learning au sein d'une boîte mail a de multiples intérêts, parmi ceux-là, la proposition de réponses automatiques à un mail selon divers facteurs – Des recommandations sur le moment le plus opportun pour se désabonner d'une liste de diffusion – Bloquer les spams à destinations de nos adresses email.

Nous étudierons le Machine Learning implanté dans un outil de messagerie pour comprendre l'intérêt et les enjeux de son usage, représente-t-il un danger pour notre confidentialité ? Un tel algorithme peut-il réellement solutionner le problème de réception de sur-email, ainsi autogérer la gestion de nos emails tout en nous soumettant les bons conseils ?

II- Gmail, outil collaboratif en plein développement

Gmail est lancé en 2004, depuis sa création le service de messagerie a cumulé 1.5 milliard d'utilisateurs actifs de manière mensuelle sur l'année 2019, cela représente actuellement 20% du marché mondial. Une mobilité applicative permettant à 75% de ses utilisateurs d'accéder à leur messagerie de par un support mobile, auquel le prix moyen d'un compte Gmail est estimé à 3588 \$.

Cet outil de messagerie se rapprochant dangereusement de son mentor Outlook, celui-ci engage un nombre considérable d'utilisateur parmi lesquels il est intéressant de relever que 61% d'entre eux sont âgés de 18 à 29 ans. Il a su se faire une place parmi les petites entreprises et Start-Up mais peine encore à satisfaire le grand public, conjointement en concurrence avec l'outil de messagerie issu de la sphère Microsoft.

Google réalise un franc succès au printemps 2018 avec une refonte importante de l'outil, et surtout en y incluant d'innovantes fonctionnalités, en effet la firme américaine implémente un de ses propres outils open source d'apprentissage automatique, nommé TensorFlow. La technologie propre à Google est fondée sur une infrastructure « DistBelief ¹ » et possède une interface Python et Julia. En plus de mettre à disposition de ses utilisateurs un outil de messagerie doté de machine learning, et donc proposé une expérience utilisateur unique, Google reste en terre conquise du fait de traiter avec des implémentations déjà internes à l'entreprise.

Avec TensorFlow, Google frappe fort, ses utilisateurs bénéficient d'une nouvelle protection contre les spams, 100 millions de spams supplémentaires sont maintenant contrés d'après la firme américaine. Cependant Google n'a pas échappé à une légère crise recensée au cœur de ses utilisateurs, certains d'entre eux se plaignaient sur le forum dédié *Gmail Help Forum* ² de recevoir des spams provenant de leurs propres adresses emails... Paramètre surprenant, chacun de ces plaignants avait un point

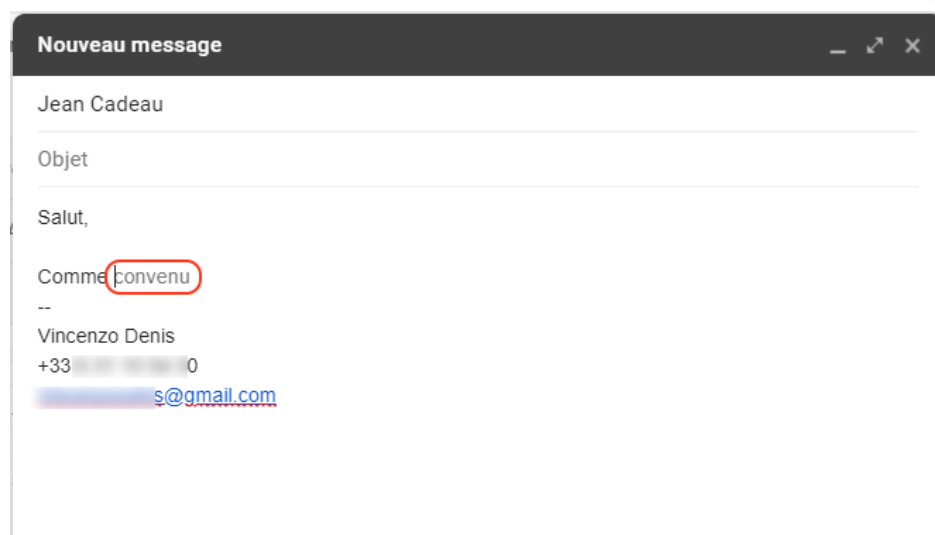
¹ Le code qu'est DistBelief a été transformé en une bibliothèque plus rapide et plus solide qui est devenue TensorFlow.

² <https://support.google.com/mail/community/>

commun, ils utilisaient l'identification à deux facteurs. On apprendra par la suite que tout cela était donc dû à une campagne de spam (biens réels) affectant un ensemble d'utilisateurs, plus précisément le problème que la machine Learning n'a pas réussi à parer venait en fait d'un en-tête d'email qui avait été falsifiée pour donner l'impression à un utilisateur qu'il recevait un email de sa propre adresse.

D'autre part l'algorithme de TensorFlow possède une particularité qui n'est pas des moindres, en effet la signification de spam peut être variée en fonction de chacun des profils d'utilisateurs, par exemple, la réception systématique d'email attestant d'une simple notification ou action sur une application tiers peut être considéré comme tel. Lorsque nous commandons une course en VTC dans 100% des cas nous recevons un email récapitulatif à la fin de la course, celui-ci a pour but d'attester, comme justificatif de la course que vous venez de réaliser. Dans le cas d'une personne qui prend de manière régulière un VTC, se verra automatiquement incendiée d'innombrables emails récapitulatifs, l'intelligence artificielle fondée derrière TensorFlow considérerait potentiellement cela comme un spam. La machine Learning a su se séparer de se différencier par le biais de facteurs déterminants, en apprenant des actions effectuées par les utilisateurs, si le mail était déplacé vers la corbeille à chaque reprise cela était donc un spam, au contraire, si celui-ci était déplacé dans une boîte tierce, imprimé, ou encore, transféré à un destinataire nous n'étions donc pas en face d'un spam. Toutefois comme je le précisais précédemment, l'exemple des justificatifs n'est pas propre à chacun des utilisateurs, là-encore TensorFlow doit apprendre à différencier, et gérer chacun des cas de figures.

Une fois la différence apprise et gérée l'outil de machine learning propose automatiquement différentes actions à l'ouverture de l'email comme, « **Déplacer dans nom de boîte au lettre** » ; « **Déplacer dans la corbeille** » ; « **Transférer à nom utilisateur** ». Un réel gain de temps quand on fait parti des personnes qui traitent plusieurs centaines de mails par jour... La même méthodologie est donc appliquée au contenu de l'email, non plus pour déterminer la potentialité d'un spam, quoique cela sert tout de même à quantifier et enrichir l'apprentissage de l'algorithme. Mais pour simplifier et optimiser les temps de réponses à un email, et non pas de manière générale, justement avec un attrait personnalisé pour chacun des destinataires de nos emails. Le principe demeure exactement le même, simplement à défaut de présenter des boutons d'actions à l'utilisateur, c'est à la rédaction de l'email que l'intelligence fera effet, illustrons mes propos par le biais d'une capture d'écran. (Cf. Image ci-dessous)



Comme nous pouvons le constater sur la capture ci-dessus à la deuxième ligne lorsque je commence à écrire « Comme », là où est positionné mon curseur va se voir être proposé le mot « convenu » de couleur grisée, libre à moi de simplement déplacer mon curseur à la fin du mot pour l'ajouter rapidement au corps de mon email. L'exemple ici représente la méthodologie appliquée, en plus des mots, l'outil propose parfois des composés de phrase lorsque cela a du sens.

III- Le Machine Learning

Le sujet abordé ici ne relate pas d'une récente évolution de notre espèce, ni d'un nouveau « gadget » mis au goût du jour, non, l'idée d'une machine dotée de pensée occupe les esprits depuis bien des millénaires. Simplement celle-ci se matérialise de plus en plus depuis 1936 grâce à Alan Turing et se prénomme au départ : Machine Universelle ; Cela a continué jusqu'en 1950 dans le domaine de l'apprentissage automatique, cette même année-là il développe Le test de Turing.³

C'est 9 ans plus tard que le terme « *machine learning* » sera utilisé pour la première fois par un informaticien, Arthur Samuel. Tout cela est parti d'une partie de Dames, il développa en 1952 un programme qui jouait au jeu de Dames pour IBM qui avait comme particularité de s'améliorer en jouant. Ce qui découlera d'une victoire pour la machine contre le quatrième meilleur joueur des États-Unis. Depuis cet événement qui n'est pas des moindres, les étapes n'ont cessées d'être franchies, la suivante étant la création d'une machine « Deep Blue » par IBM qui gagna le match face champion du monde d'échecs en 1997 – En 2012, un réseau dit neuronal développé par Google est capable de reconnaître des visages dans des vidéos youtube – 2014, Eugene Goostman une IA russe créée en 2001 réussira le test de Turing - En 2015, une énième étape est acquise, l'ordinateur « AlphaGo » de Google gagna au « jeu de Go » contre un des meilleurs joueurs – 2016, un système d'IA basé sur l'apprentissage automatique parvient à lire sur lèvres – Puis maintenant Gmail est dotée d'un outil d'apprentissage automatique.

Les grands principes du machine learning sont basés sur de l'algorithmie, à cela y est appairé un système piloté par un ordinateur qui permet de traduire et adapter les analyses effectuées ainsi que les comportements en réponse. Notamment grâce à de l'analyse empirique⁴ de donnée fondée sur une base de données ou encore, sur des capteurs. Tout cela engendre une multitude de calcul qui amène ensuite à un problème de complexité, plus communément appelé explosion combinatoire, ce problème se résout par l'ajustement de modèle qui simplifie la complexité de l'équation.

La machine learning dispose de plusieurs méthodes d'apprentissages, six précisément, voici donc une liste exhaustive des méthodes d'appréhension appliquées à l'intérieur des algorithmes :

- **Apprentissage supervisé** : Dans ce cas de figure les classes sont prédéterminées et les exemples connus, la machine apprendra donc selon un modèle de classification. Un ingénieur doit étiqueter des exemples pour que le processus puisse se dérouler en deux phases :
 - **Première** : Il détermine un modèle, hors ligne, avec les données étiquetées cette étape est l'apprentissage.

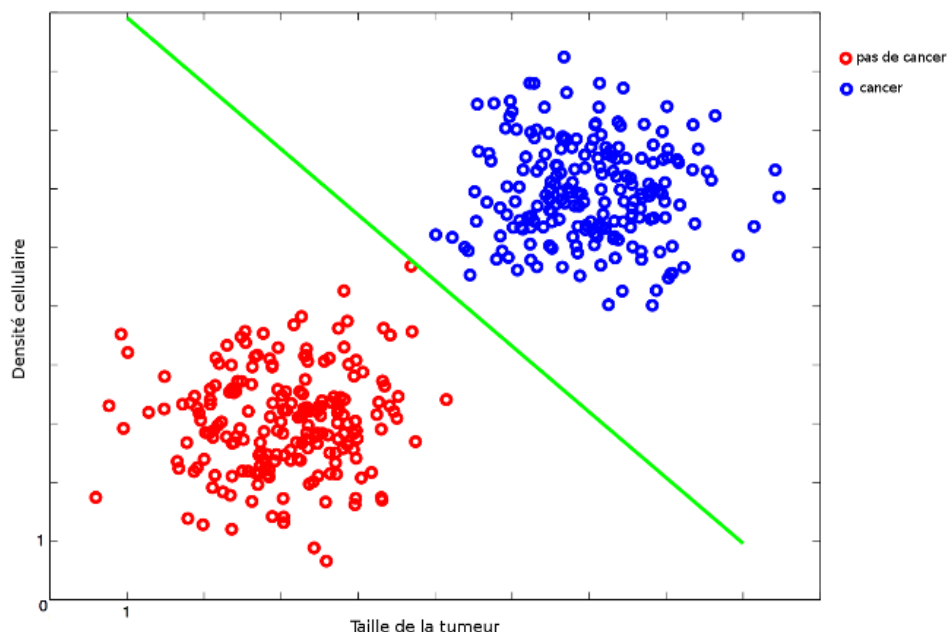
³C'est une proposition de test d'Intelligence Artificielle fondée sur la faculté d'une machine à imiter la conversation humaine.

⁴ Sources de la connaissance acquise au moyen des sens, de par l'observation et l'expérimentation.

- **Seconde** : Celle-ci est dite phase de test, en ligne, et consiste à tester les capacités du programme en devinant l'étiquette d'une nouvelle donnée.
- **Apprentissage non supervisé** : Cette méthode intervient lorsque le système possède que des exemples et non pas d'étiquette. Ainsi les classes et leur nature n'ont pas été définies, nul besoin de faire appel à un expert pour cette méthode. C'est l'algorithme lui-même qui découvre les données, et la structure de donnée, une opération connue de nous, informaticiens, le partitionnement de donnée, qui est un vrai apprentissage sans supervision.
 - **Apprentissage semi-supervisé** : La méthode étudiée ici se base sur la probabilité, le principe étant de faire apparaître différents facteurs / exemples, le modèle est informé que des données manquent, afin qu'il puisse utiliser des exemples qui n'auront pas été étiquetés mais qui peuvent le renseigner.
 - **Apprentissage partiellement supervisé** : Dans cet exemple nous avons toujours nos valeurs de références, exemples, données et/ou étiquettes, là-encore la notion de probabilité est forte, cependant l'étiquetage des données est cette fois partiel.
 - **Apprentissage par renforcement** : Cela se passe au développement de l'algorithme, celui-ci va apprendre un comportement sur la base de l'observation, l'action codée sur l'algorithme produit une valeur de retour qui va ensuite orienter l'algorithme dans son apprentissage.
 - **Apprentissage par transfert** : Concernant cette dernière méthode d'apprentissage, le transfert est comme la capacité d'un système à identifier et mettre en œuvre des connaissances ainsi que des compétences assimilées à partir de tâches antérieures, sur de nouvelles tâches ou domaines partageant des similitudes.

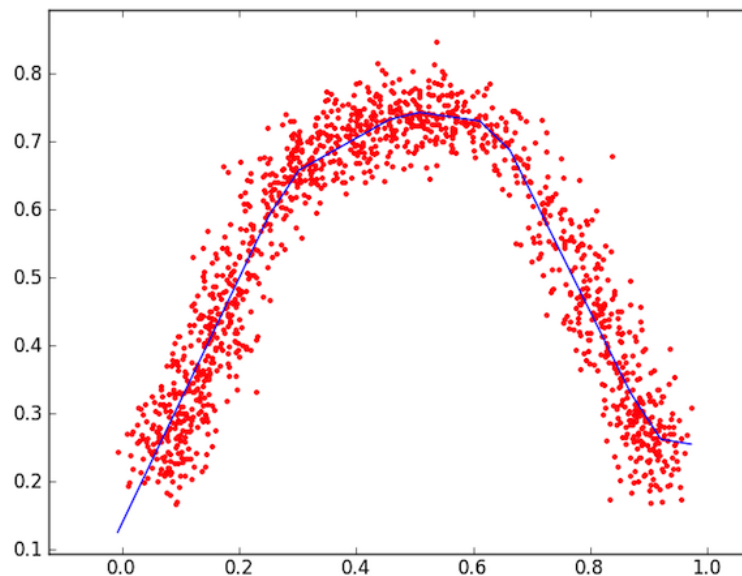
Parmi chacun des éléments étudiés ci-dessus l'apprentissage supervisé reste une des méthodes les plus appliquée dans le domaine, l'entraînement est la clé de la réussite, afin de vous illustrer cette conclusion observons deux graphiques représentant un modèle d'entraînement pour un algorithme :

1^{er} type d'apprentissage représenté graphiquement, la classification :



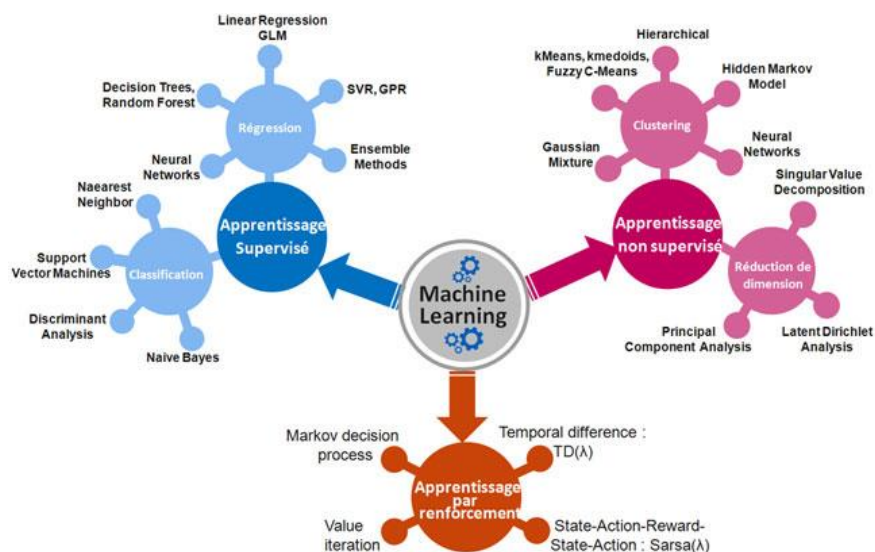
Un exemple médical parfaitement représentatif de ce que peut assimiler un algorithme d'apprentissage, le modèle n'aura plus qu'à juxtaposer le nuage de points rouge représentant les cellules non cancéreuses avec un test médical.

2^{ème} type d'apprentissage supervisé représenté graphiquement, la régression :



Le principe reste identique, la différence se fera de part la méthodologie de disposition des cellules avec le trait continu.

Pour conclure la partie sur la machine learning laissez-moi vous proposer cette représentation schématique des divers modes d'apprentissage affiliés à des exemples d'applications auxquels ils correspondraient le mieux.



IV- Conclusion

Après avoir pris le temps d'étudier les deux composants principaux de ma synthèse, l'outil de messagerie Gmail et le machine learning, je suis à même de pouvoir répondre d'une conclusion concluante sur la thématique abordée : L'introduction du machine learning au sein d'un outil de messagerie. En parallèle de ce sujet j'ai évoqué deux questions principales, « l'introduction d'une AI dans un outil de tous les jours représente-t-il un danger pour notre confidentialité ? » Et « Un tel algorithme peut-il réellement solutionner le problème de réception de sur-email, ainsi autogérer la gestion de nos emails tout en nous soumettant les bons conseils ? ».

Tout d'abords je comprends mieux la méthodologie abordée derrière les nouveautés que Gmail nous proposait lors du mois d'avril 2018, aussi bien sur le plan sécuritaire avec le contre de spam, que sur le plan « user experience » et praticité avec les actions automatiques proposées lors de l'ouverture d'un email. Ainsi nous comprenons mieux la méthode adoptée pour enrichir le contenu de cet algorithme, encore une fois, aussi bien pour la sécurité que pour la proposition d'action, et/ou de mots/bouts de phrase. Il va de soit qu'un apprentissage supervisé ou encore, partiellement supervisé est employé au cœur de cet algorithme. En suivant la logique de l'algorithme il est clair que le danger pour nous utilisateur ne sera pas augmenté plus qu'il l'est déjà, avec ou sans l'aide du machine learning, il faut donc voir cela comme une opportunité de maximiser et optimiser le blocage de spam dans un premier temps pour ensuite étendre les perspectives vers des dimensions plus importantes. L'ajout de ce nouvel assistant est donc une réelle aubaine pour nous utilisateurs, qui passons un temps considérable à rédiger, consulter, déplacer et supprimer des emails, cela n'est que positif et nous permet de réduire notre temps d'actions sur un outil de messagerie afin de le consacrer à d'amples activités professionnelles.