Le projet doit être réalisé en **équipe de deux** étudiants-es.
Remise analyse préliminaire : Lundi 12 mars 2025 à 23h59.
Remise rapport final : Vendredi 2 mai à 23h59.

Mise en contexte

Vous travaillez dans une compagnie de consultants en intelligence artificielle (IA). Un de vos client s'intéresse à l'utilisation de l'apprentissage par renforcement (RL) pour optimiser des procédés industriels. Son contexte d'utilisation demande d'apprendre des politiques sécuritaires, au sens de la définition suivante :

> *Une politique est considérée sécuritaire si elle permet d'éviter les situations associées à la réception de récompenses négatives de grande amplitude relativement à la récompense moyenne (aussi dites catastrophiques).*

Votre client considère apprendre les politiques dans un environnement de simulation, pour ensuite les transférer sur le système réel. Il s'intéresse donc à la *sécurité des politiques apprises* et non à la sécurité pendant l'apprentissage.

Votre client vous demande de réaliser une étude montrant les limitations des stratégies de RL classiques face à ce défi et d'évaluer des approches proposées dans la littérature pour aborder ce problème. Il vous demande également de considérer dans votre étude l'impact du transfert de la politique apprise sur une configuration de l'environnement (système simulé) vers une autre configuration du même environnement (système réel).

Travail à réaliser

Le travail sera effectué en trois étapes : 1) l'analyse préliminaire; 2) les expériences; et 3) le rapport final.

Analyse préliminaire

Dans un premier temps, votre client vous demande de produire une analyse préliminaire pour décrire et justifier les grandes lignes de votre étude à réaliser. Pour ce faire, vous devez fouiller la littérature scientifique et **identifier trois articles** publiés (journaux ou conférences scientifiques), chacun abordant une variante différente de problème correspondant au RL sécuritaire général décrit dans la mise en contexte. Vous devrez ensuite sélectionner une de ces variantes comme sujet de votre étude et **détailler la formulation spécifique du problème**. Finalement, vous devrez **identifier deux méthodes à considérer dans votre étude**. Une des méthodes doit être une stratégie classique générale (non-spécifique à l'aspect sécuritaire) et l'autre méthode doit avoir été proposée pour aborder la variante de problème à l'étude. Vous devez justifier le choix des méthodes sélectionnées. Si vous compter utiliser des librairies existantes qui fournissent une implémentation des méthodes, vous devez indiquer ces librairies.

Votre document doit suivre la structure suivante :

- Revue de la littérature
- Formulation du problème sélectionné
- Présentation des méthodes à étudier
- Bibliographie

Votre document peut contenir **jusqu'à 2 pages** (excluant la bibliographie) et doit être rédigé en LaTeX dans le style suivant : https://github.com/kourgeorge/arxiv-style. Ne pas inclure le résumé *(abstract)* ni les mots-clés *(keywords)*.

Vous devez remettre l'analyse préliminaire en format PDF.

Expériences

Vos expériences doivent être réalisées en Python. Votre projet doit être hébergé sur GitHub. Nous vous communiquerons les noms d'utilisateurs à ajouter au projet en vue de la correction. Assurez-vous de bien utiliser la commande `commit` puisque l'historique des modifications sera utilisé pour valider vos contributions au projet et contrôler le plagiat.

Pénalité possible jusqu'à 50% pour non-contribution.

Rapport final

Suite à une validation de l'analyse préliminaire par le client, vous devez **mettre à jour** votre revue de la littérature, votre formulation du problème, ainsi que la présentation des méthodes considérées. Vous devez notamment **expliquer le fonctionnement des méthodes sélectionnées**, en incluant notamment leur pseudo-codes. Vous pouvez ensuite vous lancer dans la réalisation de l'étude. Vous devez **décrire la méthodologie expérimentale** mise en place pour comparer les méthodes sélectionnées. Notamment, il est important de décrire comment vous comptez étudier l'impact d'un transfert de politique de la simulation vers la réalité. Notez ici que la "réalité" sera simulée aussi dans votre projet. Si vous utilisez des librairies existantes pour votre environnement, vous devez présenter ces librairies. Vous allez finalement réaliser vos expériences et **présenter les résultats** associés, accompagnés d'une **discussion**. Vos résultats doivent inclure des tableaux et/ou figures qui permettent de comprendre la différence entre les politiques sécuritaires et non-sécuritaires apprises. Ils doivent également inclure des tableaux et/ou figure permettant de comprendre comment le transfert simulation-réalité affecte les politiques (sécuritaires ou non).

Votre document doit suivre la structure suivante :

- Revue de la littérature (mise à jour)
- Formulation du problème (mise à jour)
- Présentation des méthodes étudiées (mise à jour)
- Description de la méthodologie expérimentale
- Présentation des résultats
- Discussion
- Bibliographie (mise à jour)

Votre document peut contenir **jusqu'à 6 pages** (excluant la bibliographie) et doit être rédigé en LaTeX dans le style suivant : `https://github.com/kourgeorge/arxiv-style`. Ne pas inclure le résumé *(abstract)* ni les mots-clés *(keywords)*.

Vous devez remettre le rapport final en format PDF. Votre rapport doit contenir l'URL du projet GitHub contenant le code source (Python) documenté pour reproduire vos expériences.