Université de Paris

Mathématiques discrètes
Projet : Extracteurs d'aléa

Consignes Le but du projet est de présenter une application dans laquelle les mathématiques discrètes jouent un rôle fondamental.

Le rendu final du projet consistera en un article destiné au grand public au format pdf de 800-1000 mots plus une annexe numérique, qui pourra contenir par exemple une démonstration interactive, une vidéo explicative et/ou des graphiques générés par du code écrit par vous-même ; cette annexe sera rendue sous la forme d'un lien vers un dépôt en ligne. La forme exacte et la technologie utilisée pour l'annexe peut varier et est donc laissé au libre choix des étudiants. L'article et son annexe seront jugés non seulement sur le contenu mais aussi sur la clarté de la présentation, la qualité de rédaction, et la créativité.

Contenu Le sujet détaille quelques points à développer mais ceux-ci sont seulement proposés comme point de départ de votre travail. Vous êtes encouragés à développer d'autres pistes en lien avec les mathématiques discrètes. De même, la bibliographie conseillée est un point de départ. Vous pouvez vous appuyer sur d'autres sources sur lesquelles vous porterez un œil critique et que vous prendrez soin de citer correctement.

Charte de bonne conduite Lisez attentivement la charte de bonne conduite. Portez une attention particulière à citer toutes vos sources, y compris les exemples et les images que vous utiliserez. L'utilisation d'outils d'IA tels que ChatGPT est formellement interdite. L'équipe pédagogique sera très attentive à tous ces aspects lors de la correction.

Calendrier Consultez la page Moodle du cours pour les dates des principales étapes du projet.

Bref descriptif du sujet

Les algorithmes ont souvent besoin pour fonctionner de pouvoir utiliser de l'aléa. On peut citer par exemple les jeux vidéos, les méthodes de chiffrement et de protection de données, la génération de mots de passe, mais aussi les nombreux algorithmes classiques dont l'efficacité peut être améliorée par l'usage d'aléa.
Pour générer cet aléa, les systèmes informatiques utilisent généralement une source externe qui stocke des informations contenant une bonne part d'aléa : mouvements de la souris, temps précis d'appui sur les touches, variations infimes de températures des composants, sont autant de processus contenant une part d'aléa, que le système va stocker.
Un extracteur d'aléa est un processus qui, à partir d'une certaine source qui *contient* de l'aléa, mais qui peut être biaisée car partiellement déterministe, construit une séquence aléatoire uniformément distribuée. C'est le processus par lequel l'ordinateur extrait du « vrai » aléa à partir d'une source imprédictible. Le projet vise à présenter la notion d'extracteurs d'aléa, d'en discuter certaines des constructions principales et d'en aborder les aspects mathématiques.

Bibliographie conseillée

- `https://en.wikipedia.org/wiki/Randomness_extractor`
- `http://www.eecs.harvard.edu/~michaelm/coinflipext.pdf`

Pistes de développement

1. Présenter les extracteurs d'aléa et en détailler quelques applications choisies
2. Présenter l'extracteur de Von Neumann et quantifier ses propriétés (temps moyen nécessaire pour extraire un bit uniforme)
3. Écrire un programme qui extrait, à partir d'une entrée aléatoire mais biaisée, une chaîne aléatoire uniforme
4. Présenter une construction optimisée d'extracteur lorsque le biais est connu