Anniversaires et hashage

Le Gourrierec Alan

November 11, 2023

Unité d'enseignement : Algorithmique et programmation impérative

Enseignant : P. Marteau

Établissement : ENSIBS (Vannes)

Contents

Chapter 1

Démonstration fonction de hashage

On pose :

$$H1(x) = \sum_{i=0}^{n} ord(i) * 256^i$$
$$h : x \to (H1(x)[255])$$

Nous souhaitons démontrer que peu importe l'odre des lettres dans un mot, avec cette fonction. Nous savons que pour chaque lettre nous avons la formule suivante :

$$ord(letter) \times 256^n \equiv x \times 256^n[255]$$

Or 256 est un inverse modulaire de 255 $\Rightarrow 256 \equiv 1[255]$

$$\Rightarrow ord(letter) \equiv x \times 1^n[255]$$

Or $0 \leqslant n \leqslant 255$ La solution est donc : $(\sum_{i=0}^{len(mot)} ord(i))[255]$

Chapter 2

Paradox des anniversaire

2.1 Les aniversaires

Le **paradox des anniversaires** déterminé la probabilité, celon un certain nombre de personne (et dans une année non bisextile), la probabilité que deux personne possède la même date d'anniversaire.
Pour exprimer ceci, nous allons déterminer la probabilité que deux personne n'aient pas la même date de naissance et utiliser le propriété suivante après :

$$P(\bar{A}) = \frac{365!}{(365-k)!*365^k}, \forall k \in \mathbb{N} \wedge 1 \leqslant k \leqslant 365$$

Il nous suffit donc d'utiliser la propriété de probabilité suivante :

$$P(A) = 1 - P(\bar{A})$$

Nous obtenons donc ainsi le résultat.

2.2 Généralisation de cette fonction pour le hashage

Cette fonction, déterminant la probabilité que deux personne soient née un même jour. Si nous changeons le nombre de jour d'une année par la taille de nos chaîne (dans l'exercice 3) et que nous remplacons k par le nombre d'itération, nous obtenons les probabilités d'avoir une colision.
La généralisation de cette fonction est donc :

$$P(\bar{C}) = \frac{size!}{(size-i)!*size^i}, \forall (i, size) \in \mathbb{N}^2 \wedge 0 \leqslant i \leqslant size$$

(avec size : la taille de la chaîne, i : le nombre d'itération)