# - Notes de cours -

# Présentation du module

Objectifs du cours. Ce cours fait suite au cours d'algorithmique de L2. Son but est de poursuivre l'étude de la conception et de l'analyse d'algorithmes. Les problèmes algorithmiques que nous étudierons viendront de différents domaines : traitement informatique, recherche oprérationnelle, logique, graphes, algèbre, combinatoire...

Intervenants. S. Bessy (responsable du module), M. Bougeret, A. Perret Du Cray, L. Isenmann (mail:prenom.nom@umontpellier.fr)

Contenu. Quatre chapitres principaux:

- Algorithmes exhaustifs et backtrack,
- Analyse en moyenne et algorithmes probabilistes,
- Hachage et
- Algorithmes d'approximation.

**Planning (a priori...)** Les cours (10 séances d'1h30) ont lieu le mercredi à 13h15, les tds et tps (10 séances de 3h) le mardi à 8h00 ou le jeudi matin à 9h45 (selon votre groupe). L'emploi du temps exact est à consulter sur l'ENT.

Sem.	Date	Contenu
37	Me 14/09	CM1 : Chapitre 1 : Complexité et Probabilités : aléatoire en algorith-
		mique
38	Me 21/09	CM2 : Chapitre 2 : Recherche exhaustive et backtrack
		TD1 : Complexité, aléatoire en algorithmique
39	Me 28/09	CM3: Fin du Chapitre 2
		TP1: Algorithmes probabilistes
40	Me $05/10$	CM4: Chapitre 3: Analyse amortie, en moyenne et algorithmes pro-
		babilistes
		TD2: Recherche exhaustive
41	Me $12/10$	CM5 : Fin du Chapitre 3
		TP2: Recherche exhaustive
42	Me $19/10$	CM6: Chapitre 4: Hachage
		TD3 : Analyse amortie, en moyenne et algos probabilistes
43	Me $26/10$	CM7 : Fin du Chapitre 4
		TD4 : Fin des Algos probabilistes et début des exos sur le Hachage
44	Me 02/11	VACANCES D'AUTOMNE
45	Me 09/11	CM8: !!! Controle continu, type exam!!! (Contenu: Chap. 1,2 et 3)
		TD5 : Fin des exercices sur le Hachage
46	Me 16/11	CM9: Chapitre 5: Algorithmes d'approximation
		TP3: Hachage
47	Me 23/11	CM10 : Fin du Chapitre 5
		TD6: Algorithmes d'approximation
14	Me $30/11$	TP4: Algorithmes d'approximation

Modalité de contrôle de connaissance. L'évaluation comportera un contrôle continu et un examen. Le contrôle continu est composé d'une partie type exam (sur le créneau de cours du 9 novembre a

priori) et d'une bonification sur l'avancée en tp (au plus 2pts). Le contrôle continu compte pour 30% dans la note finale avec la 'règle du max', c'est-à-dire que la note finale sera max $\{exam; 0.7 \times exam + 0.3 \times cc\}$ . Une deuxième session d'examen est prévue, pas de contrôle continu.

Pour les exams et le contrôle continu, les seuls documents autorisés sont ces notes de cours.

Prérequis. D'un point de vue algorithmique, sont attendues des connaissances sur les instructions classiques en pseudo-code, la récursivité, les heuristiques classiques de complexité (glouton, diviser pour régner, programmation dynamique), le calcul de la complexité d'un algorithme et la connaissance des structures de données usuelles (tableaux, piles, files, liste chaînées, structures arborescentes). En programmation, les tp se feront en Python. Il faut maîtriser a minima le langage.

Ressource. Les ressources pédagogiques seront disponibles sur le moodle de l'Université (HAI503I). Les ouvrages suivant contiennent l'essentiel du cours (et même plus...) :

- T.H. Cormen, C.E. Leiserson, R. Rivest and C. Stein. Introduction to Algorithms, 3rd Edition, MIT Press, 2009 (une version française existe).
- S. Dasgupta, C. Papadimitriou and U. Vazirani. Algorithms, McGraw-Hill Higher Education, 2006 (version électronique gratuite).
- J. Erickson. Algorithms, University of Illinois at Urbana-Champaign, 2019, ainsi que le chapitre supplémentaire sur les probabilités (version électronique gratuite).
- J. Kleinberg, E. Tardos. Algorithm design, Pearson education, 2005.
- V.V. Vazirani. Approximation algorithms, Springer, 2001.

#### Rappels de complexité, probabilité 1

#### 1.1 Rappels de complexité

• Une notation de Landau : Soient  $f,g:\mathbb{N}\longrightarrow\mathbb{R}^+$ . On dit que f=O(g) si il existe une constante c > 0 et un rang  $n_0 \in \mathbb{N}$  tels que :  $\forall n \geq n_0$  on ait  $f(n) \leq c.g(n)$ 

**Lemme 1** (O et limites) Pour  $f: \mathbb{N} \longrightarrow \mathbb{R}$  et  $g: \mathbb{N} \longrightarrow \mathbb{R}^{+*}$ , si il existe une constante  $c \geq 0$  telle que  $\frac{f(n)}{g(n)} \underset{n \to +\infty}{\longrightarrow} c$  alors on a f = O(g). Et si  $\frac{f(n)}{g(n)} \underset{n \to +\infty}{\longrightarrow} +\infty$  alors on a  $f \neq O(g)$ .

Lemme 2 (Limites comparées) -  $Pour \ \alpha, \beta > 0 \ on \ a :$   $\frac{(\log n)^{\alpha}}{n^{\beta}} \underset{n \to +\infty}{\longrightarrow} 0 \qquad \frac{n^{\alpha}}{(2^{n})^{\beta}} \underset{n \to +\infty}{\longrightarrow} 0 \qquad \frac{(2^{n})^{\alpha}}{n!} \underset{n \to +\infty}{\longrightarrow} 0$ -  $Soit \ u(n) \ est \ une \ fonction \ telle \ que \ u(n) \underset{n \to +\infty}{\longrightarrow} \infty \ (typiquement, \ u(n) = n \ ou \ u(n) = \log n \ ou \ u(n) = 2^{n}).$ 

 $Si\ a.X^p\ et\ b.X^q\ avec\ a>0\ et\ b>0\ sont\ respectivement\ les\ termes\ de\ plus\ haut\ degr\'e\ de\ deux\ polynomes\ P$ et Q alors  $\lim_{n\to\infty} P(u(n))/Q(u(n))$  vaut : 0 si q>p, a/b si q=p et  $+\infty$  si p>q.

Lemme 3 (Règles de calcul pour le log) Pour  $a, b \in \mathbb{R}^{+*}$  et  $c \in \mathbb{R}$ , on a:

log 0 est non défini  $\log 1 = 0$ 

 $\log(\frac{a}{b}) = \log a - \log b$  $\log(a \times b) = \log a + \log b$  $\log(a^c) = c \times \log a$ 

Lemme 4 (Règles de calcul pour l'exp)  $Pour\ a,b\in\mathbb{R}^{+*},\ on\ a:$   $2^{a+b}=2^a\times 2^b$   $2^{a\times b}=(2^a)^b$ 

 $2^{\log a} = a$  $\log 2^a = a$ 

Lemme 5 (Sommes arithmétique et géométrique) Pour  $a, b \in \mathbb{N}$  avec  $a \leq b$  et  $x \in \mathbb{R} \setminus \{1\}$ , on a:

$$\sum_{i=a}^{b} i = (b-a+1) \cdot \frac{b+a}{2} \qquad et \qquad \sum_{i=a}^{b} x^{i} = \frac{x^{b+1} - x^{a}}{x-1}$$

```
Théorème 1 ('Master Theorem') Si il existe trois entiers a \ge 0, b > 1 et d \ge 0 tels que pour tout n > 0 on ait t(n) \le a.t(\lceil n/b \rceil) + O(n^d) alors:

- t(n) = O(n^d) si b^d > a (c'est-à-dire si d > \log a/\log b),

- t(n) = O(n^d \log n) si b^d = a (c'est-à-dire si d = \log a/\log b), ou

- t(n) = O(n^{\frac{\log a}{\log b}}) si b^d < a (c'est-à-dire si d < \log a/\log b).
```

### 1.2 Rappel de probabilités discrètes

- L'ensemble des résultats possibles d'une expérience probabiliste est appelé son **univers**, souvent noté Ω. Un **évènement primitif** (ou **élémentaire**) est un élément de l'univers, c'est-à-dire, un résultat possible. Plus généralement, un **évènement** est un sous-ensemble de l'univers, donc un ensemble de résultats possibles.
- Étant donné un univers  $\Omega$ , une **probabilités** sur  $\Omega$  est une valeur pour chaque élément primitif x, notée  $\Pr[x]$ , telle que  $\sum_{x \in \Omega} \Pr[x] = 1$ . La **probabilité d'un évènement** est la somme des probabilités de ses éléments.
- Si tous les évènements primitifs d'un univers ont la même probabilité (c'est-à-dire que pour tout  $x \in \Omega$  on a  $\Pr[x] = 1/\Omega$ ), on parle de **probabilité uniforme** sur  $\Omega$ . Dans ce cas, un évènement A a pour probabilité  $|A|/|\Omega|$  ('nombres de cas favorables/nombre de cas possibles').
- Une variable aléatoire est une fonction  $X:\Omega \to V$  avec  $V \subseteq \mathbb{R}$ . "X=v" est l'évènement  $\{\omega \in \Omega: X(\omega)=v\}$  et  $\Pr[X=v]=\sum_{\omega:X(\omega)=v}\Pr[\omega]$  " $X \le v$ " est l'évènement  $\{\omega \in \Omega: X(\omega) \le v\}$  et  $\Pr[X \le v]=\sum_{\omega:X(\omega) \le v}\Pr[\omega]$
- Soit  $X: \Omega \to V$  une variable aléatoire. L'espérance de X est :  $\mathbb{E}[X] = \sum_{v \in V} v \times \Pr[X = v]$ .
- La probabilité de E sachant F est  $\Pr[E \mid F] = \frac{\Pr[E \cap F]}{\Pr[F]}$ . L'espérance de X sachant F est  $\mathbb{E}[X \mid F] = \sum_{v \in V} t \times \Pr[X = v \mid F]$ .
- Deux évènements sont **indépendants** si  $\Pr[E \wedge F] = \Pr[E].\Pr[F]$ . Deux variables aléatoires sont indépendantes si  $\Pr[X = u \wedge Y = v] = \Pr[X = u].\Pr[Y = v]$  pour tous u, v.

```
Théorème 2 (Propriétés) Soient E et F deux évènements et X,Y:\Omega\to V deux variables aléatoires. On a les propriétés suivantes :  -Pr[\neg E] = 1 - Pr[E]   -Pr[E\vee F] \leq Pr[E] + Pr[F]  Inégalité de Boole ou 'Union bound'  -\sum_{v\in V} Pr[X=v] = 1   -\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]  Linéarité de l'espérance
```

Si, de plus,  $\Omega = \bigsqcup_i F_i$ , partition de  $\Omega$  en  $(F_i)_i$ , on a aussi :

de plus,  $\Omega = \bigsqcup_{i} F_{i}$ , partition de  $\Omega$  en  $(F_{i})_{i}$ , on a auss

-  $Pr[E] = \sum_{i} Pr[E \mid F_i] . Pr[F_i]$ -  $\mathbb{E}[X] = \sum_{i} \mathbb{E}[X \mid F_i] . Pr[F_i]$ 

Formule des probabilités totales Formule de l'espérance totale

# 1.3 Bits et entiers aléatoires ou pseudo-aléatoires

• Les générateurs **pseudo-aléatoires** implantés dans les machines sont considérés d'un point de vue théorique et pratique comme des générateurs acceptables de bits, d'entiers et de réels aléatoires.

### 1.4 Lois de probabilités usuelles

- La loi **Uniforme** sur l'ensemble  $V = \{1, ..., n\}$  est donné par  $\Pr[X = v] = 1/|V| = 1/n$  pour tout  $v \in V$ . Elle se simule par le tirage d'un entier entre 1 et |V|.
- La loi **Bernoulli**(p) sur l'ensemble  $V = \{0,1\}$  est donnée par  $\Pr[X=1] = p$  et  $\Pr[X=0] = 1 p$ . Elle se simule par letirage d'un bit aléatoire biaisé.

Notes de Cours L3 Info

- La loi **Binomiale**(p, n) sur l'ensemble  $V = \{0, ..., n\}$  est donnée par  $\Pr[X = k] = \binom{n}{k} p^k (1 p)^k$  pour k = 0, ..., n. Elle se simule comme la somme de n variables de Bernoulli de paramètre p.
- La loi **Géométrique**(p) sur l'ensemble  $V = \mathbb{N}$  est donnée par  $\Pr[X = n] = p(1-p)^{n-1}$  pour  $n \in \mathbb{N}$ . Elle se simule comme la loi de la première apparition du '1' dans une suite de variables de Bernoulli de paramètre p.

### 1.5 Borne des queues de distribution

```
Lemme 6 (Inégalité de Markov) Soit X: \Omega \to V une variable aléatoire positive (V \subseteq \mathbb{R}^+).
Pour tout t > 0, on a: Pr[X \ge t] \le \frac{1}{t}.\mathbb{E}[X]
```

### 2 Recherche exhaustive et backtrack

#### 2.1 Recherche exhaustive

• Un littéral est une variable logique ou sa négation. Une clause est une disjonction de de littéraux. Et une formule SAT est une conjonction de clauses.

```
Ex: \varphi(x_1, x_2, x_3) = (\neg x_1 \lor x_2) \land (x_1 \lor x_2 \lor \neg x_3) \land \neg x_2
```

- Le problème SAT prend en entrée une formule SAT  $\varphi$  et décide si il existe ou non une affection des variables à vrai ou faux qui satifasse  $\varphi$ .
- Chaque clause C de  $\varphi$  est codé par un tableau où chaque case contient l'indice de la variable correspondante, précédée d'un signe moins si la variable est négative dans C. Une affectation A est codée par un tableau tel que A[i] = 1 (resp. -1) si  $x_i$  est affecté à vrai (resp. faux).
- Les algorithmes TestAff et AffSuivante respectivement testent une affectation et passe à l'affectation suivante.

```
Algorithme : TestAff(\varphi, A)

pour C dans \varphi faire

OK \leftarrow \text{faux};
pour \ell dans C faire
\text{si } \ell \times A_{[|\ell|-1]} > 0 \text{ alors}
\text{O}K \leftarrow \text{VRAI};
si OK = \text{faux alors retourner faux};
retourner VRAI;
```

```
 \begin{array}{|c|c|c|c|} \textbf{Algorithme}: \texttt{AffSuivante}(A) \\ i \leftarrow 0; \\ \textbf{tant que} \ i < n \ et \ A_{[i]} = 1 \ \textbf{faire} \\ & A_{[i]} \leftarrow -1; \\ & i \leftarrow i+1; \\ & \textbf{si} \ i = n \ \textbf{alors} \\ & \bot \ \textbf{retourner} \ \ll \text{Fin} \ \gg \\ & A_{[i]} \leftarrow 1; \\ & \textbf{retourner} \ A; \end{array}
```

• L'algorithme Recherche Exhaustive SAT cherche une affectation positive pour une formule SAT.

Théorème 3 (Resolution SAT exhaustive) L'algorithme RECHERCHEEXHAUSTIVESAT trouve une affectation satisfaisante s'il en existe une, et renvoie « Insatisfiable » sinon, en temps  $O(|\varphi|2^n)$ .

- Le principe de la recherche exhaustive est de parcourir toutes les solutions possibles et pour chacune de tester si elle répond au problème.
  - La complexité des algos correspondants est O (Nombre Solutions  $\times$  (Coût Test + Coût Passage Suivant))
- Le problème du **Voyageur de commerce** a pour entrée un graphe G = (S, A) avec une longueur  $\ell(u, v)$  pour chaque arête, et pour sortie une numérotation  $u_0, \ldots, u_{n-1}$  des sommets qui minimise la longueur totale  $\sum_{i=0}^{n-1} \ell(u_i, u_{i+1}) + \ell(u_{n-1}, u_0)$ .

La résolution du Voyageur de commerce par recherche exhaustive demande de générer toutes les permutations des entiers 0 à n-1. Pour cela, on part de la permutation  $\pi=0,1,2,\ldots,n-1$  et on applique l'algorithme suivant.

```
Algorithme: PERMSUIVANTE(\pi)

si \pi_{[0]} > \cdots > \pi_{[n-1]} alors retourner 'Fin';

Trouver j maximal tel que \pi_{[j]} < \pi_{[j+1]};

Trouver \ell > j maximal tel que \pi_{[j]} < \pi_{[\ell]};

Échanger \pi_{[j]} et \pi_{[\ell]};

pour 0 < k < \frac{n-j}{2} faire

Léchanger \pi_{[j+k]} et \pi_{[n-k]}; Retournement de \pi_{j+1,n} retourner \pi;
```

• L'algorithme suivant résout alors le problème du voyageur de commerce sur le graphe G = (S, A) muni d'une fonction de longeur  $\ell$  sur ses arêtes.

```
Algorithme: VoyageurDeCommerce(S, A, \ell)
\pi \leftarrow \text{tableau de taille } n, \text{ initialisé à } [0, 1, \dots, n-1];
L_{\min} \leftarrow +\infty;
\pi_{\min} \leftarrow \pi;
tant que PermSuivante ne retourne pas 'Fin' faire
\begin{bmatrix} L \leftarrow \sum_{i=0}^{n-1} \ell(S[\pi_{[i]}], S[\pi_{[i+1 \bmod n]}]); \\ \text{si } L < L_{\min} \text{ alors} \\ \lfloor (L_{\min}, \pi_{\min}) \leftarrow (L, \pi); \\ \pi \leftarrow \text{PermSuivante}(\pi); \end{bmatrix}
retourner \pi_{\min};
```

Théorème 4 (Résolution exhaustive de VoyageurDeCommerce) L'algorithme VoyageurDeCommerce résout le problème du voyageur de commerce en temps  $O(n \times n!)$ .

#### 2.2 Backtrack ou 'retour sur trace'

• La résolution de SAT par backtrack se fait en affectant récursivement chaque variable en testant à chaque étape la solution partielle obtenue. On utilise les algorithmes suivants, où  $\varphi$  est une formule SAT à n variables et b est une valeur booléenne (Vrai ou Faux).

Théorème 5 (Resolution SAT par backtrack) L'algorithme SATBACKTRACK trouve une affectation satisfaisante s'il en existe une, et renvoie « Insatisfiable » sinon, en temps  $O(|\varphi|2^n)$  (mais est beaucoup plus efficace en pratique que l'algorithme RECHERCHEEXHAUSTIVESAT).

```
Algorithme: ÉLIMINATION(\varphi, n, b)

\psi \leftarrow \text{formule vide};

\mathbf{pour} \ C \ dans \ \varphi \ \mathbf{faire}

C' \leftarrow \text{clause vide};

sat \leftarrow \text{FAUX};

\mathbf{pour} \ \ell \ dans \ C \ \mathbf{faire}

\mathbf{si} \ |\ell| = n \ et \ \ell \times b > 0 \ \mathbf{alors}
+ sat \leftarrow \text{VRAI}
\mathbf{sinon}
\mathbf{sinon}
\mathbf{si} \ |\ell| \neq n \ \mathbf{alors}
+ \mathbf{Ajouter} \ \ell \ \grave{a} \ C';

\mathbf{si} \ \text{NoN}(sat) \ \mathbf{alors}
+ \mathbf{Ajouter} \ C' \ \grave{a} \ \psi;

\mathbf{retourner} \ \psi;
```

```
Algorithme: SatBacktrack(\varphi, n)

si \varphi est vide alors

\lfloor retourner A = [1, \dots, 1];

si \varphi possède une clause vide alors

\lfloor retourner "Insatisfiable";

pour b \in \{1, -1\} faire

\downarrow \psi \leftarrow \text{\'ELIMINATION}(\varphi, n, b);
A \leftarrow \text{SatBacktrack}(\psi, n - 1);
si \psi n'est pas insatisfiable alors

\lfloor retourner A + [b];

retourner "Insatisfiable";
```

- Le principe des algorithmes de Backtrack est de constuire récursivement des solutions partielles et de tester celles-ci à chaque étape (ce qui permet d'éliminer des branches de l'exploration). Cela correspond à parcourir l'arbre des solutions en profondeur en évitant de parcourir certaines branches.
- Le problème de **Sudoku généralisé** est le suivant. Entrée : Une grille G de dimensions  $n^2 \times n^2$ , remplie d'entiers de 0 (= vide) à  $n^2$ Sortie : La même grille G sans 0, tel que  $G_{[i,j]} \neq G_{[k,\ell]}$  dès que : i = k (ligne), ou  $j = \ell$  (colonne), ou |i/n| = |k/n| et  $|j/n| = |\ell/n|$  (zone), ou alors 'aucune solution'.
- La grille du Sudoku s'encode de façon linéaire. La grille G de dimensions  $n^2 \times n^2$  est représentée par un tableau T de taille  $n^4$ . La case  $G_{[i,j]}$  correspond à la case  $T_{[in^2+j]}$  (stockage ligne par ligne). Inversement, la case  $T_{[u]}$  correspond à la case  $G_{[u \text{ div } n^2, u \text{ mod } n^2]}$  où  $u \text{ div } n^2 = \lfloor u/n^2 \rfloor$ .
- La résolution par backtrack du Sodoku généralisé se fait par les deux algorithmes suivants où pour le premier u est un numéro de case et x une valeur à tester dans la case u.

```
Algorithme: Valide (G, n, u, x)

(i, j) \leftarrow (u \operatorname{div} n^2, u \operatorname{mod} n^2);
pour k = 0 à n^2 - 1 faire
\begin{bmatrix} \mathbf{si} & (k \neq i \text{ et } G_{[kn^2 + j]} = x) \text{ alors} \\ & \mathbf{retourner Faux}; \end{bmatrix}
si (k \neq j \text{ et } G_{[in^2 + k]} = x) \text{ alors} \\ & \mathbf{retourner Faux}; \end{bmatrix}
\begin{bmatrix} \mathbf{ci} & (x, z_j) \leftarrow (n \lfloor i/n \rfloor, n \lfloor j/n \rfloor); \\ \mathbf{pour} & k = 0 \text{ à } n - 1 \text{ faire} \end{bmatrix}
\begin{bmatrix} \mathbf{pour} & \ell = 0 \text{ à } n - 1 \text{ faire} \\ & \mathbf{si} & ((z_i + k)n^2 + (z_j + \ell) \neq u \text{ et } G_{[(z_i + k)n^2 + (z_j + \ell)]} = x) \text{ alors} \\ & \mathbf{retourner Faux}; \end{bmatrix}
retourner Vrai;
```

# 3 Analyse amortie, analyse d'algorithmes probabilistes

# 3.1 Analyse amortie

• On revient sur le compteur binaire, qui prend un tableau T de taille k en entier représentant l'entier N encodé en binaire et retourne le tableau correspondant à l'entier N+1.

```
\begin{aligned} & \textbf{Algorithme}: \text{Incrément}(T) \\ & i \leftarrow 0; \\ & \textbf{tant que} \ i < k \ et \ T[i] = 1 \ \textbf{faire} \\ & \quad T[i] \leftarrow 0; \\ & \quad i \leftarrow i+1; \\ & \quad \textbf{si} \ i = k \ \textbf{alors} \ \textbf{retourner} \ \text{'Fin'}; \\ & \textbf{si} \ i < k \ \textbf{alors} \\ & \quad T[i] \leftarrow 1; \\ & \quad \textbf{retourner} \ T; \end{aligned}
```

Théorème 6 (Compteur binaire armorti) INCRÉMENT est correct, a une complexité en O(k) et une complexité amortie en O(1) lorsqu'on l'appelle  $2^k$  fois depuis l'appel initial sur  $T = [0, 0, \dots, 0]$ .

- Si on appelle un algorithme sur N instances résultant en un nombre  $c_i$  d'opérations élémentaires sur la ième instance, le **coût amorti** (ou **complexité amortie**) sur la séquence d'instances est  $\frac{1}{N} \sum_{i=1}^{N} c_i$ . Classiquement, il y a trois méthode pour caluler ou borner cela.
- La méthode de l'agrégat consiste à calculer explicitement  $\sum_{i=1}^{N} c_i$  et à retourner  $\frac{1}{N} \sum_{i=1}^{N} c_i$ .
- La **méthode comptable** consiste à considérer un 'compte' qui ne doit jamais être en négatif et surlequel, à l'étape i, on verse la somme  $a_i$  et on prélève la somme  $c_i$ . Plus précisément, on détermine des entiers  $a_i$  positifs ou négatifs, vérifiant pour tout  $i=0,\ldots,N-1$  l'inégalité  $\sum_{0\leq j\leq i}c_j\leq \sum_{0\leq j\leq i}a_j$ . Le coût amorti est alors borné par  $\frac{1}{N}\sum_{0\leq i\leq N-1}a_i$ .
- La **méthode du potentiel** consiste à associer à l'instance produite après le *i*ème appel un potentiel  $\Phi_i$  et à estimer le coût  $a_i = c_i + (\Phi_i \Phi_{i-1})$  après chaque appel. Le coût amorti est alors borné par  $\frac{1}{N} \sum_{0 \le i \le N-1} a_i$
- Une liste dynamique est donné par un tableau T de taille N et ayant une taille utile n. Les algorithmes d'ajout et de suppression d'un élément dans une telle liste sont données ci-dessous.

```
Algorithme: AJOUT(T, N, n, x)

si n < N alors

T[n] \leftarrow x;

retourner (T,N,n+1)

U \leftarrow \text{tableau de taille } 2N;

pour i = 0 à N - 1 faire

U[i] \leftarrow T[i];

U[N] \leftarrow x;

retourner (U, 2N, n + 1)
```

Théorème 7 (Tableaux dynamiques) Ajout et Suppression sont corrects, de complexité O(n) dans le pire des cas, mais avec un coût amorti en O(1) pour n'importe quelle séquence d'opérations en partant d'une liste vide.

# 3.2 Analyse d'algorithmes probabilistes

• Le problème de **sélection** (ou du kième rang) consiste à trouver le kième plus petit élément d'un tableau T donné, de taille n. L'algorithme suivant permet de répondre au problème.

Théorème 8 (Espérance de complexité pour QUICKSELECT) Soit  $C_n$  le nombre de comparaisons effectuées par QUICKSELECT(T,k) où T est de taille n. Alors  $\mathbb{E}[C_n] \leq 4n$ , quelque soit k.

- Un multigraphe est un graphe dans lequel chaque paire de sommets est relié par aucune, une ou plusieurs arêtes.
- Une **coupe** dans un multigraphe G = (V, A) est une partition  $(V_1, V_2)$  de l'ensemble de ses sommets en deux ensembles non vides.

La **taille** de la coupe  $(V_1, V_2)$  est le nombre d'arêtes entre  $V_1$  et  $V_2$ , c'est-à-dire  $|\{u_1u_2 \in A : u_1 \in V_1, u_2 \in V_2\}|$ 

Le **problème de la coupe minimale** prend en entrée un multigraphe G et retourne une coupe de taille minimale.

- Soit G = (V, A) un multigraphe et uv une arête de G. Le multigraphe G/uv, obtenu par contraction de l'arête uv, a pour sommets  $V \setminus v$  et pour ensemble d'arêtes  $(A \setminus \{xv : xv \in A\}) \cup \{xu : xv \in A, x \neq u\}$
- l'algorithme suivant prend en entrée un multigraphe G et retourne une coupe de G.

```
Algorithme : CoupeMin(G)

tant que G possède au moins 3 sommets faire

Choisir une arête uv de G, aléatoirement et uniformément;

Contracter l'arête uv dans G;

retourner la coupe définie par les deux sommets restants
```

Théorème 9 (Analyse de CoupeMin) En admettant que l'opération de contraction d'arête puisse s'effectuer en temps O(n), où n est le nombre de sommets de G, alors CoupeMin retourne une coupe de G en temps  $O(n^2)$ .

De plus, cette coupe est une coupe minimale de G avec probabilité  $\geq \frac{2}{n(n-1)}$ .

Lemme 7 (Lemme de répétition) Si on répète N fois COUPEMIN et qu'on garde la plus petite coupe renvoyée, cette coupe est minimale avec probabilité  $\geq 1 - e^{-2N/n(n-1)}$ 

Théorème 10 (COUPEMIN répété) Si on répète  $N=2n^2$  fois l'algorithme COUPEMIN et que l'on retourne la coupe trouvée de plus petite taille, alors, en temps  $O(n^4)$  une coupe minimale est retournée avec probabilité  $\geq 98\%$ .

- Les algorithmes probabilistes se divisent classiquement en deux grandes familles :
  - Les algorithmes de type Las Vegas dont le résultat ne dépend pas des choix aléatoires, mais

Notes de Cours L3 Info

la complexité si (ex : QUICKSELECT).

- Les algorithmes de type **Monte Carlo** dont le résultat dépend des choix aléatoires, mais pas la complexité (ex : COUPEMIN).
- L'algorithme suivant prend en entrée un tableau T et retourne ce tableau, trié.

```
 \begin{aligned} \mathbf{Algorithme:} & \operatorname{TriRapide}(T) \\ \mathbf{si} & \ taille(T) = 1 \ \mathbf{alors\ retourner}\ T; \\ p \leftarrow T_{[i]} & \ avec\ i \ \text{choisi al\'eatoirement entre 0 et } n-1; \\ n_p \leftarrow & \ nombre\ d'indices\ i \ \text{tels que}\ T_{[i]} = p; \\ T_0 \leftarrow & \ \text{tableau des \'el\'ements de}\ T \ \text{qui sont}\ < p; \\ T_1 \leftarrow & \ \text{tableau des \'el\'ements de}\ T \ \text{qui sont}\ > p; \\ T_0 \leftarrow & \ \text{TriRapide}(T_0); \\ T_1 \leftarrow & \ \text{TriRapide}(T_0); \\ T_1 \leftarrow & \ \text{TriRapide}(T_1); \\ \mathbf{retourner}\ & \ a \ concat\'enation\ T_0,\ n_p\ \text{fois}\ p,\ \text{et}\ T_1 \end{aligned}
```

Théorème 11 (Trirapide) Trirapide retourne bien le tableau initial, trié. L'espérance du nombre de comparaisons effectuées par Trirapide est  $O(n \log n)$ 

# 4 Tables de hachage

#### 4.1 Introduction

- Une table de hachage est donnée par :
  - Un ensemble de **clefs** : un **univers** U des clefs possibles :  $U = \{0, ..., N-1\}$  et un ensemble  $K \subset U$ , de taille n, de **clefs utilisées**.
  - Une table T de taille m, dont chaque cas contient aucune, une ou plusieurs valeurs.
  - Une fonction de hachage  $h: U \to \{0, \dots, m-1\}$ , qui permet d'insérer le couple (k, v) dans la case T[h(k)].
- Un ensemble  $\mathcal{H}$  de fonctions de  $U = \{0, ..., N-1\}$  dans  $\{0, ..., m-1\}$  est **universel** si pour tout  $k_1 \neq k_2 \in U$ , lorsqu'on tire uniformément h dans  $\mathcal{H}$  on a  $\Pr[h(k_1) = h(k_2)] \leq 1/m$ .

## 4.2 Résolution des collisions

• Il y a **collision** entre les clefs  $k_1$  et  $k_2$  si  $h(k_1) = h(k_2)$ .

Lemme 8 (Collisions dans une grande table)  $Si m = n^2$ , et h est tirée uniformément dans un ensemble universel  $\mathcal{H}$ , alors la probabilité qu'il existe deux clefs  $k_1 \neq k_2$  telles que  $h(k_1) = h(k_2)$  est  $\leq \frac{1}{2}$ .

• Dans la **résolution par chaînage**, chaque case i de T contient une liste chaînée. On désigne cette liste par T[i] et pour une clef  $k \in K$ , la longueur de la liste T[h(k)] est noté  $\ell(k)$ .

```
Algorithme: Recherche(k, h, T)
Calculer h(k);
Parcourir la liste T[h(k)];
si on trouve k alors retourner (k, v);
sinon retourner NULL;
```

```
Algorithme: INSERTION(k, v, h, T)
Calculer h(k);
Parcourir la liste T[h(k)];
si on trouve k alors Changer la valeur de k en v;
sinon Ajouter (k, v) à la fin de la liste T[h(k)];
```

• Les algorithmes RECHERCHE et INSERTION permettent de rechercher et d'insérer une clef dans la table,

tous deux de complexité O(L), où  $L=\max\{\ell(k)\ :\ k\in K\}.$ 

Théorème 12 (Résolution par chaînage) Soit T une table de hachage de taille m, avec h tirée uniformément dans un ensemble  $\mathcal H$  universel. Si T contient n éléments et que les collisions sont résolues par chaînage, l'espérance de la complexité de RECHERCHE et de INSERTION est en  $O(\alpha)$ , où  $\alpha = n/m$  est le taux de remplissage de la table.

• Dans l'adressage ouvert, on se donne m fonctions de hachage  $h_1, h_2, \ldots, h_m$ , telles que pour tout  $k \in U$   $(h_1(k), h_2(k), \ldots, h_m(k))$  est une permutation de  $(0, 1, \ldots, m-1)$ .

```
Algorithme: Recherche(k, h_1, \dots, h_m, T)

pour i = 1 à m faire

Calculer h_i(k);

si T[h_i(k)] contient k alors retourner (k, v);

si T[h_i(k)] est vide alors retourner NULL;
```

Théorème 13 (Adressage ouvert) Sous l'hypothèse que pour tout k,  $(h_1(k), \ldots, h_m(k))$  est une permutation aléatoire et si le facteur de remplissage  $\alpha = n/m$  est < 1, alors l'espérance du nombre de cases visitées pour une RECHERCHE infructueuse ou une INSERTION est  $\leq \frac{1}{1-\alpha}$ .

### 4.3 Une famille universelle de fonctions de hachage

- Conditions sur les familles universelles de fonctions de hachage. On va demader qu'une famille universelle H de fonctions de hachage vérifie les conditions suivantes :
  - la **taille de**  $\mathcal{H}$  est polynomiale en N et est  $\geq {N \choose 2}$
  - la représentation d'une fonction h de  $\mathcal{H}$  se fait en  $O(\log N)$  bits
  - le **tirage aléatoire** d'une fonction de  $\mathcal{H}$  se fait en temps  $O(\log N)$ .
- Le hachage multiplicatif est la famille universelle  $\mathcal{H}_p^{N,m}$  définie pour p premier avec p > N et formée des fonctions suivantes pour 0 < a < p et  $0 \le b < p$ :

$$h_{a,b}: \left| \begin{array}{ccc} \{0,\dots,N-1\} & \to & \{0,\dots,m-1\} \\ k & \to & ((ak+b) \bmod p) \bmod m \end{array} \right.$$

Lemme 9 (Système linéaire modulo p) Soit  $k_1 \neq k_2$  et  $u \neq v$  dans  $\mathbb{Z}/p\mathbb{Z}$ , alors il existe un unique couple  $a, b \in \mathbb{Z}/p\mathbb{Z}$  tel que  $u = ak_1 + b$  et  $v = ak_2 + b$ .

Théorème 14 (Hachage universel multiplicatif) Pour tout  $k_1 \neq k_2$ , on a  $Pr[h_{a,b}(k_1) = h_{a,b}(k_2)] \leq 1/m$ . Autrement dit, la famille  $\mathcal{H}_p^{N,m}$  est universelle (pour tout N, m et  $p \geq N$  avec p premier).

# 5 Algorithmes d'approximation

# 5.1 Premiers exemples

• Étant donné un graphe G = (V, E), une **couverture par sommets** de G est un sous-ensemble de sommets de G qui touche toutes les arêtes de G. Autrement dit, X est une couverture par sommets de G si pour

toute arête  $uv \in E(G)$ , on a  $u \in X$  ou  $v \in X$ .

```
Algorithme : CouvApprox(G = (V, E))

C \leftarrow \emptyset;

tant que G contient encore au moins une arête faire

| Choisir une arête uv de G;

C \leftarrow C \cup \{u, v\};

| Supprimer u et v (et leurs arêtes incidentes) de G;

retourner C;
```

Théorème 15 (Approximation de la couverture minimum par sommet) L'algorithme COUVAP-PROX retourne une couverture C du graphe G donné en paramètre en temps  $O(n^2)$  (où n est le nombre de sommets de G). De plus, si OPT désigne la taille d'une couverture de taille minimale de G, alors C vérifie  $|C| \leq 2$ .OPT.

• Le problème de la SOMME PARTIELLE prend en entrée un ensemble E d'entiers strictement positifs et un entier cible t et cherche un sous-ensemble  $S \subset E$  dont la somme est  $\leq t$  et tel que la somme des éléments de S soit la plus grande possible.

Pour un sous-ensemble  $S \subset E$ , on note  $\Sigma S$  la somme  $\sum_{x \in S} x$ .

```
Algorithme: SommePartApprox(E,t)
Trier E par ordre décroissant;
S \leftarrow \emptyset;
pour i = 0 à |E| - 1 faire

| si E[i] \le t alors
| Ajouter E[i] à S;
| t \leftarrow t - E[i];
retourner S;
```

Théorème 16 (Analyse de SommePartApprox) L'appel SommePartApprox(E,t) retourne en temps  $O(n \log n)$ , une solution S vérifiant  $\Sigma S \geq \frac{1}{2}$  OPT, où OPT est la valeur d'une solution optimale au problème Somme Partielle pour (E,t).

#### 5.2 Les algorithmes d'approximation

- On se donne un ensemble I des instances (entrées) et pour chaque  $x \in I$ , l'ensemble S des solutions acceptables (sorties possibles). De plus, il existe une fonction de coût  $c: S \to \mathbb{R}$  qui définit la valeur d'une solution.
- Un problème est un **problème de maximisation** si il faut trouver  $s \in S$  telle que c(s) soit maximum, c'est-à-dire, telle que :  $\forall s' \in S, c(s') \leq c(s)$ . Symériquement, un problème est un **problème de minimisation** si il faut trouver  $s \in S$  telle que c(s)

Symériquement, un problème est un **problème de minimisation** si il faut trouver  $s \in S$  telle que c(s) soit minimum, c'est-à-dire, telle que :  $\forall s' \in S, c(s') \geq c(s)$ .

- On note OPT la valeur d'une solution optimale, et on dit que OPT est la **valeur optimale** du problème. Si on traite un problème de maximisation, on a OPT =  $\max_{s \in S} c(s)$ , et si on traite un problème de minimisation, on a OPT =  $\min_{s \in S} c(s)$ .
- Un algorithme d' $\alpha$ -approximation est un algorithme qui pour tout entrée x renvoie une solution  $s \in S$  telle que
  - $\alpha \cdot \text{OPT} \le c(s) \le \text{OPT}$  pour un problème de maximisation, avec  $0 < \alpha < 1$
  - OPT  $\leq c(s) \leq \alpha$  · OPT pour un problème de minimisation, avec  $\alpha > 1$

Le réel  $\alpha$  est appelé facteur d'approximation de l'algorithme.

# 5.3 Exemples plus avancés

• Le problème d'Équilibrage prend en entrée un tableau D d'entiers positifs, de taille n, correspondant aux  $dur\acute{e}es$  des tâches à répartir et un entier m correspondant aux nombres de processeurs disponibles. En sortie, on cherche un tableau A d'affectation de chaque tâche à un processeur (tâche i affectée au processeur j:A[i]=j). L'objectif est de minimiser le temps total correspondant à l'affectation, calculé comme :  $t(A)=\max_{1\leq j\leq m}\left(\sum_{i:A[i]=j}D[i]\right)$ .

```
\begin{aligned} \textbf{Algorithme:} & \text{\'EQUILIBRAGEGLOUTON}(D, m) \\ T &\leftarrow \text{tableau de taille } m, \text{ intialis\'e \`a 0 (temps total par processeur)}; \\ \textbf{pour } i = 1 & \text{\~a } n \text{ faire} \\ & \text{\ifootnote{$j$}} \leftarrow \text{indice du minimum de } T; \\ & A_{[i]} \leftarrow j; \\ & T_{[j]} \leftarrow T_{[j]} + D_{[i]}; \\ \textbf{retourner } A; \end{aligned}
```

Théorème 17 (Analyse de Équilibrage Glouton) L'algorithme Équilibrage Glouton est une 2-approximation pour le problème Équilibrage et a une complexité O(nm) (ou  $O(n \log m)$  avec un tas).

Théorème 18 (Analyse de ÉQUILIBRAGEGLOUTON) Si le tableau D est connu à l'avance et est trié avant d'appeler ÉQUILIBRAGEGLOUTON, alors cet algorithme est une  $\frac{3}{2}$ -approximation pour le problème ÉQUILIBRAGE et a une complexité  $O(n(m + \log n))$  (ou  $O(n \log n)$  avec un tas).

• Le problème d'MaxSat prend en entrée un ensemble  $C_1, \ldots C_m$  de m clauses disjonctives sur n variables booléennes. On cherche une affectation des variables qui maximise le nombre de clauses satisfaites.

Théorème 19 (Analyse de MAXSATRAND) L'algorithme MAXSATRAND, qui affecte chaque variable aléatoirement à vrai ou faux avec probabilité  $\frac{1}{2}$ , a une complexité de O(n) et l'espérance du nombre de clauses qu'il satisfait est  $\geq \frac{1}{2}$  OPT, où OPT est le OPT est le nombre maximum de clauses qui peuvent être satisfaites par une affectation.

- Le problème du VOYAGEURDECOMMERCE sur un graphe prend en entrée un graphe G = (S, A) avec une longueur  $\ell(u, v)$  pour chaque arête vérifiant l'inégalité triangulaire :  $\ell(u, w) \leq \ell(u, v) + \ell(v, w)$  pour tous u, v, w si les arêtes correspondantes existent. On cherche une tournée, c'est-à-dire une numérotation  $u_0, \ldots, u_{n-1}$  des sommets telle que pour tout  $i = 0, \ldots, n-2$  l'arête  $u_i u_{i+1}$  existe dans G, ainsi que l'arête  $u_{n-1}u_0$ , et qui minimise la longueur totale  $\sum_{k=0}^{n-1} \ell(u_i, u_{i+1}) + \ell(u_{n-1}, u_0)$ .
- Pour un graphe G = (V, E), un **chemin** de G est une suite  $v_1, v_2, \ldots, v_k$  de sommets de G telle que  $v_i v_{i+1}$  est une arête de G pour tout  $i = 1, \ldots, k-1$ . Un **cycle** de G est une suite  $v_1, v_2, \ldots, v_k$  de sommets de G telle que  $v_i v_{i+1}$  est une arête de G pour tout  $i = 1, \ldots, k-1$  et que  $v_k v_1$  soit aussi une arête de G.
- Un graphe G est **connexe** si pour tous sommets u et v de G, il existe un chemin de u à v. Un **arbre** est un graphe connexe sans cycle. Et un **arbre couvrant** de G est un sous-graphe de G, contenant tous ses sommets et qui est un arbre.

```
Théorème 20 (Connexité et arbre couvrant) Un graphe G est connexe si, et seulement si, il admet un arbre couvrant.
Un arbre sur n sommets contient n-1 arêtes.
```

• Étant donné un graphe G = (V, E) connexe muni d'une fonction de poids (ou de distance)  $\ell : E \to \mathbb{R}$  sur ses arêtes de G. Le poids d'un arbre couvrant T de G est la somme des poids des arêtes de T:  $\ell(T) = \sum_{e \text{ arête de } T} \ell(e)$ .

• Dans le problème de l'Arbre Couvrant Poids Min un graphe G = (V, E) connexe avec une fonction de poids  $\ell$  sur ses arêtes est fourni en entrée, et on cherche un arbre couvrant de **de poids minimal** parmi tous les arbres couvrants de G.

**Théorème 21 (Analyse de** KRUSKAL) L'algorithme de Kruskal peut s'implémenter en temps  $O(m \log n + n^2)$ , où n désigne le nombre de sommets du graphe G et m son nombre d'arêtes. Il retourne un arbre couvrant de G de poids minimum.

```
Algorithme: VOYAGEURDECOMMERCE<sub>2APPROX</sub>(G, \ell)
\mathcal{A} \leftarrow arbre couvrant de poids minimum de G;
\mathcal{P} \leftarrow parcours en profondeur de \mathcal{A};
Calculer (u_0, \dots, u_{n-1}) \leftarrow sommets de G, dans l'ordre de première apparition dans \mathcal{P};
retourner (u_0, \dots, u_{n-1});
```

```
Théorème 22 (Analyse de VoyageurDeCommerce<sub>2APPROX</sub>) L'algorithme
```

VOYAGEURDECOMMERCE\_2APPROX s'exécute en temps  $O(m \log n)$  et fournit une 2-approximation au problème du VOYAGEUR DE COMMERCE