Portail Descartes

Introduction à la science info : TD 1

Algorithmes non formalisés

amU Faculté des sciences Aix Marseille Université

Exercice 1 (Somme de l'école primaire)

1. Calculer la somme $321 + 12345$ avec l'algorithme de l'école primaire. Combien d'opérations élémentaires (sommes d'entiers de deux chiffres) sont nécessaires pour calculer ce résultat ?
2. Supposons vouloir calculer la somme de deux entiers naturels de m et n chiffres respectivement. Supposons également que dans ce calcul il n'y ait jamais de retenue. Combien d'opérations sont nécessaires pour calculer le résultat ?

Exercice 2 (Somme avec la retenue)

1. Calculer la somme $2138 + 764$. Combien d'opérations élémentaires sont nécessaires pour calculer ce résultat ?
2. Supposons vouloir calculer la somme de deux entiers naturels de m et n chiffres respectivement, cette fois-ci en admettant des retenues *sauf dans la dernière colonne à gauche*. Combien d'opérations élémentaires sont nécessaires pour calculer le résultat *dans le meilleur et dans le pire des cas* ? Identifiez de quel cas il s'agit et donnez un exemple qui donne un nombre maximum d'opérations pour toute longueur m et n.

Exercice 3 (Somme avec la retenue dans la dernière colonne)

1. Calculer la somme $8024 + 2077$. Combien d'opérations élémentaires sont nécessaires pour calculer ce résultat ?
2. Supposons vouloir calculer la somme de deux entiers naturels de m et n chiffres respectivement, cette fois-ci dans le cas général. Combien de chiffres peut avoir le résultat de cette somme ? Combien d'opérations élémentaires sont nécessaires pour calculer le résultat *dans le meilleur et dans le pire des cas* ? Identifiez de quel cas il s'agit et donnez un exemple qui donne un nombre maximum d'opérations pour toute longueur m et n.

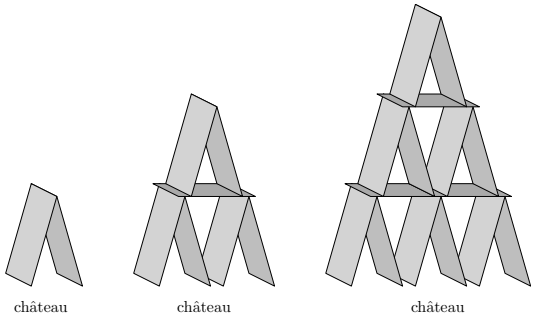
Exercice 4 (Énigme de la bergère)

1. Donner une solution pour l'énigme de la bergère, sous forme de liste d'opérations élémentaires du type « transporter x » (où x est le loup, le mouton ou le chou) et « traverser ».
2. Existe-t-il une solution alternative ?

Exercice 5 (Énigme de la bergère généralisée) Supposons maintenant que la bergère a ℓ loups, m moutons et c choux, où ℓ, m, c sont des entiers naturels (possiblement 0). On a déjà résolu le problème pour $\ell = m = c = 1$.

1. Si on a une solution pour certaines valeurs de ℓ, m, c, est-ce qu'on en a une aussi en diminuant une (ou plusieurs) de ces valeurs ?
2. Existe-t-il une solution au problème pour $\ell = 2, m = 1, c = 1$, pour $\ell = 1, m = 1, c = 2$ et pour $\ell = 1, m = 2, c = 1$?
3. Si le problème n'admet pas de solution pour certaines valeurs de ℓ, m, c, est-ce qu'on peut le rendre résolvable en *ajoutant* des animaux ou des choux ?
4. Est-ce qu'on peut rendre résolvable une situation impossible *en ajoutant d'autres bergères* (qui peuvent aussi être transportées avec le bateau) ? Combien de bergères suffiraient en fonction du nombre d'animaux et de choux ?

Exercice 6 (Châteaux de cartes) Un château de cartes est une structure où des niveaux de paires de cartes sont placés en équilibre en triangle, surmontés par des cartes placées horizontalement :



château à 1 niveau — château à 2 niveaux — château à 3 niveaux

1. Supposons que le château à n niveaux (du niveau 1 au niveau n) soit construit devant vous, pour une valeur quelconque fixée de $n \geq 1$. Expliquez en français comment construire le château de cartes à $n+1$ niveaux en ajoutant des cartes au château devant vous. On supposera avoir toujours à disposition assez de cartes.
2. Soit $c(n)$ le nombre de cartes nécessaires pour construire le château à n niveaux. Par exemple, en observant l'illustration en haut, on peut vérifier que $c(1) = 2$, $c(2) = 7$ et $c(3) = 15$. Exprimez $c(n+1)$ en fonction de $c(n)$, pour tout $n \geq 1$.
3. En justifiant votre réponse mathématiquement, combien de niveaux le château construit avec 40 cartes a-t-il ?

Exercice 7 (Chiffrement de César) La cryptologie (étym. science du secret) est un domaine à la frontière des mathématiques et de l'informatique. Elle se sépare en deux pans de même importance. Le premier consiste à transformer une information afin de la rendre secrète, autrement dit à la "crypter" ou "chiffrer". Il s'agit de la *cryptographie* (étym. écriture secrète). Le second consiste à analyser les informations cryptées et trouver des méthodes et techniques afin d'en dévoiler le sens caché. Il s'agit de la *cryptanalyse*.

Historiquement, un procédé de cryptographie bien connu est le *codage de César* que Jules César utilisait dans ses correspondances. Le principe de chiffrement est simple. Étant donné un alphabet (ici, nous utiliserons l'alphabet latin) et un message, le message chiffré s'obtient en remplaçant chacune des lettres du message d'origine par une lettre à distance fixe toujours dans la même direction. Pour les dernières lettres, dans le cas d'une distance à droite, on reprend au début de l'alphabet. Il s'agit d'un chiffrement par décalage. À titre d'exemple, avec un décalage de 5, 'a' devient 'f', 'b' devient 'g', ..., 'y' devient 'd' et 'z' devient 'e'.

1. Soit le message "La vie est un long fleuve tranquille". Donnez ses représentations chiffrées selon le codage de César avec les clés 3 et -7.
2. En utilisant des phrases en langage naturel (en français, dans notre cas), donnez une description la plus précise possible de l'algorithme de chiffrement utilisé pour le codage de César.
3. Quelle est la complexité de l'algorithme de chiffrement de César ? On demande de compter le nombre d'opérations de décalage effectuées par l'algorithme en fonction du nombre n de caractères d'un message donné.
4. Proposez un algorithme de déchiffrement, prenant en entrée le message chiffré et une clé et renvoyant le message décodé. À titre d'exemple, déchiffrez le message « kajex »sachant que la clé de chiffrement vaut 9.
5. Admettons que quelqu'un vous envoie un message chiffré en vous spécifiant qu'il s'agit d'un codage de César mais sans vous donner la clé. Est-il possible de le déchiffrer ? Si oui, comment et est-ce efficace, en termes de temps ?
6. Plus généralement, un tel codage est-il utilisable en pratique ? Autrement dit, est-il efficace en termes de sécurité du secret dans le cas général (imaginez que vous recevez un message chiffré et que vous ne savez pas si c'est le codage de César qui a été utilisé par l'émetteur) ?