Le 1er février 2014

Codes

I - Codes de compression

1 - Codes uniquement décodables

On utilise la table de conversion suivante pour encoder des messages.

Exemple : « ENTIER » $\rightarrow 1011 + 1100 + 100 + 10 + 1011 + 1001$
$\rightarrow 101111001001010111001$

A : 1111	E : 1011	I : 10	L : 000	N : 1100
O : 1101	R : 1001	S : 0011	T : 100	U : 0111

1. Choisir un mot ne contenant que les dix lettres considérées et donner le code correspondant.

2. De quels mots la suite 10011010111100 est-elle le code ?
[Attention, il y a plusieurs possibilités.]

On dit qu'une méthode de code est *uniquement décodable* si deux mots différents ne sont jamais codés de la même façon.

2 - Codes instantanés

On admet que les deux codes suivants sont uniquement décodables.

Code 1 :

A : 0110	E : 0000	I : 0001	L : 0010	N : 0111
O : 111	R : 10	S : 0011	T : 110	U : 010

Code 2 :

A : 1001	E : 0000	I : 0001	L : 0101	N : 110
O : 11	R : 1000	S : 010	T : 1101	U : 100

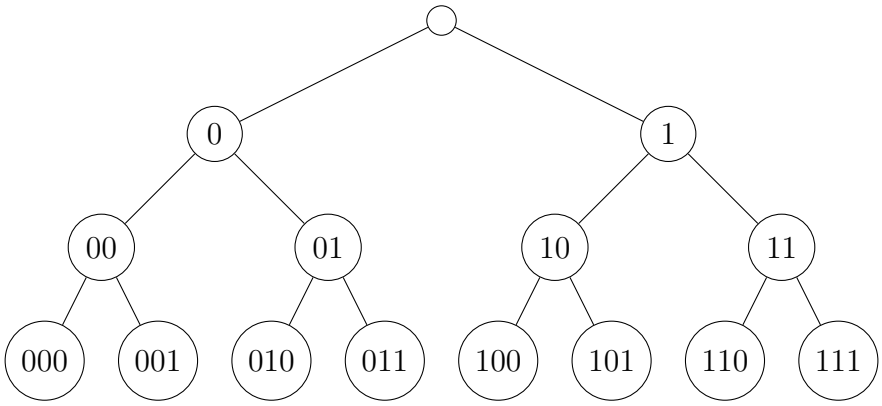
3. On dit qu'un code est *instantané* si le code associé à une lettre n'est jamais le début du code d'une autre lettre.
Par exemple, si A est codé par 00 et E est codé par 001, le code n'est pas instantané, car 00 est le début de 001.
a) Le code 1 est-il instantané ?
b) Le code 2 est-il instantané ?

4. a) On suppose qu'un message codé avec le code 1 commence par 1101110001. Pouvez-vous déterminer avec certitude ses premières lettres ?
b) Même question pour le code 2.

5. Démontrer qu'un code instantané est toujours uniquement décodable.
[Indication : Démontrer par récurrence sur n que deux messages différents dont le plus long contient n lettres sont toujours codés différemment.]

3 - Inégalité de Kraft pour les codes instantanés

On appelle l'objet dessiné ci-dessous un *arbre binaire*. On dit que celui du dessin est de profondeur 4 (parce qu'il y a quatre niveaux verticaux).



On appelle *nœuds* les ronds dans lesquels sont inscrits les nombres. On dit qu'un nœud A est un enfant d'un nœud B s'il existe dans l'arbre un chemin descendant allant de B à A.

6. Combien y a-t-il de nœuds sur le dernier niveau d'un arbre binaire de profondeur n ?

7. a) Dessinez un arbre binaire de profondeur 5.
b) On considère le code 1 du paragraphe précédent. Écrivez chaque lettre à côté du nœud qui contient son code ainsi qu'à côté de tous les enfants de ce nœud.
c) Y a-t-il un nœud à côté duquel vous avez écrit plusieurs lettres différentes ? Pouvez-vous expliquer votre réponse en utilisant le fait que le code 1 est instantané ?

8. Si, dans le code 1, le code d'une lettre X contient l_X chiffres, à côté de combien de nœuds de la dernière couche est écrite la lettre X ?

9. Montrer avec le moins de calculs possibles l'inégalité suivante :

$$\sum_{X \text{ lettre}} \frac{1}{2^{l_X}} \leq 1$$

On appelle cette inégalité l'inégalité de Kraft. On l'a démontrée pour un code spécifique mais la même démonstration est valable pour tous les codes instantanés.

4 - Réciproque de l'inégalité de Kraft

10. Choisissez dix entiers $l_A, l_E, l_I, l_L, l_N, l_O, l_R, l_S, l_T, l_U$, compris entre 1 et 5, tels que :

$$\sum_{X \text{ lettre}} \frac{1}{2^{l_X}} \leq 1$$

11. a) Classez les dix entiers par ordre décroissant.
b) Dessinez un arbre binaire de profondeur 5 puis, pour chaque lettre (en les prenant dans l'ordre dans lequel vous venez de les classer), appliquez la procédure suivante. (On appelle X la lettre considérée.)

– Choisissez un nœud qui n'est pas barré sur le niveau de profondeur l_X.
– Inscrivez la lettre X à côté de ce nœud.
– Barrez le nœud et tous ses enfants.

12. À chaque lettre, on associe le nombre contenu dans le nœud à côté duquel la lettre est inscrite. Vérifiez que le code que vous avez ainsi obtenu est instantané.

5 - Inégalité de Kraft pour les codes uniquement décodables

On considère maintenant un code uniquement décodable quelconque. Pour toute lettre X, on note l_X la longueur du code de la lettre X.
On note $l_{\max}$ le maximum des l_X.

13. Soit k un entier strictement positif.
a) Montrer que :

$$\left(\sum_{X \text{ lettre}} \frac{1}{2^{l_X}}\right)^k = \sum_{(X_1,\ldots,X_k) \text{ lettres}} \frac{1}{2^{l_{X_1}+\ldots+l_{X_k}}}$$

b) Montrer que :

$$\left(\sum_{X \text{ lettre}} \frac{1}{2^{l_X}}\right)^k = \sum_{s=1}^{kl_{\max}} \frac{1}{2^s} \times (\text{nombre de mots de } k \text{ lettres dont le code est de longueur } s)$$

c) Montrer que, pour tous k et s, le nombre de mots de k lettres dont le code est de longueur s est au plus 2^s.
[Indication : Utiliser le fait que le code est uniquement décodable.]
d) Montrer que :

$$\left(\sum_{X \text{ lettre}} \frac{1}{2^{l_X}}\right)^k \leq kl_{max}$$

14. Soit $\alpha > 1$ quelconque. Montrer que, pour tout k assez grand :

$$kl_{\max} \leq \alpha^k$$

15. a) Montrer que, pour tout $\alpha > 1$, $\sum_{X \text{ lettre}} \frac{1}{2^{l_X}} \leq \alpha$.
b) En déduire que l'inégalité de Kraft est vérifiée.

6 - Compression [Difficile]

On suppose que, dans les textes qu'on souhaite encoder, le nombre d'occurence d'une lettre X est en moyenne p_X fois le nombre total de lettres, pour un certain réel $p_X \in]0;1[$.

16. Montrer que, quel que soit le code uniquement décodable qu'on utilise, la longueur moyenne du code d'un texte de N lettres est au moins :

$$N.\left(\sum_{X \text{ lettre}} p_X \log_2(1/p_X)\right)$$

On note $\log_2(1/p_X) = \frac{\log(1/p_X)}{\log(2)}$.

17. Montrer qu'il existe un code instantané tel que, pour ce code, la longueur moyenne du code d'un texte de N lettres est au plus :

$$N.\left(1 + \sum_{X \text{ lettre}} p_X \log_2(1/p_X)\right)$$

II - RSA

1 - Clé publique, clé privée

1. a) Choisir deux nombres premiers p, q (pas trop grands).
b) Calculer $n = pq$ et $s = (p-1)(q-1)$.
c) Choisir un nombre $e < s$ premier avec s.
d) Trouver $d < s$ tel que $ed \equiv 1[s]$.
On appelle (n, e) la « clé publique » et (n, d) la « clé privée ».

2 - Chiffrement et déchiffrement

2. [Chiffrement]
a) Choisir un nombre M compris entre 0 et $n-1$, premier avec n. Ce sera le « message » à encoder.
b) Calculer m, le reste de M^e modulo n. C'est le code.

3. [Déchiffrement]
Calculer m^d.

4. Pouvez-vous justifier le résultat de la question précédente ?
[Indication : On pourra utiliser le fait que, si r est un nombre premier et si k est un entier non-divisible par r, alors $k^{r-1} \equiv 1[r]$.]