DESS Codes, Cryptologie, Sécurité Informatique

Module M5

<u>Traitement numérique et compression de données</u>

Épreuve théorique (Année 2001-2002)

On s'attachera à développer les points de cours suivants en répondant d'une part aux questions posées, et en ayant d'autre part le souci constant de présenter ces points de manière <u>la plus didactique possible</u>, l'idée sous-jacente étant de pouvoir les expliquer à un non-spécialiste. Tous les documents de cours (en particulier les deux fascicules correspondant aux parties II et III) sont utilisables, mais l'épreuve ne saurait se limiter au simple recopiage de ces notes ; un recul par rapport à leur contenu s'impose dans le présentation à un béotien que l'on vous demande ici d'en faire.

1. Les concepts d'"entropie" et de "meilleure base"

a. Qu'entend-t'on par entropie de Shannon d'un vecteur (dans un espace de Hilbert) relativement à une décomposition de cet espace ? Dans une base hilbertienne (c'est-à-dire un système orthonormé complet) de cet espace ?

b. Quel est le but pratique de l'opération consistant à déterminer, étant donné un élément s d'un espace de Hilbert donné (ici soit un signal digital, soit une image digitale) une base orthonormée de l'espace dans laquelle l'entropie de s soit minimale ?

c. La structure s (signal ou image) se trouve-t'elle à votre avis fragilisée ou au contraire rendue plus robuste après son écriture dans une base optimale (au sens où l'entropie de Shannon est minimale) ?

d. On se donne deux suites bornées $(h(n))_{n\in\mathbb{Z}}$ et $(g(n))_{n\in\mathbb{Z}}$ telles que les deux opérateurs R et D de $l^2(\mathbb{Z})$ dans lui-même définis par

$$R[s](k) := \sum_{\nu\in\mathbb{Z}} s(\nu)\overline{h(\nu-2k)}\,, \quad k\in\mathbb{Z}$$

et

$$D[s](k) := \sum_{\nu\in\mathbb{Z}} s(\nu)\overline{g(\nu-2k)}\,, \quad k\in\mathbb{Z}$$

vérifient $R^*R + D^*D = \mathrm{Id}_{l^2(\mathbb{Z})}$. Comment peut-on à partir de ces deux opérateurs R et D (agissant sur les signaux digitaux 1D) générer une méthode de recherche de bases hilbertiennes dans lesquels décomposer une image digitale

$$(k_1,k_2)\mapsto I(k_1,k_2)\,?$$

On expliquera pourquoi R et D induisent une décomposition de I comme somme de quatre images orthogonales (lues à une échelle 2). Essayez d'imaginer ce que serait un algorithme du type "recherche de base optimale" pour une image (2D) et non plus un signal (1D).

2. La transformation de Fourier discrète.

a. Rappeler, N étant un entier naturel non nul, quelle est la matrice $N \times N$ (notée M_N) telle que

$$DFT_N(s(0),...,s(N-1)) = \begin{pmatrix} \widehat{s}(0) \\ \vdots \\ \widehat{s}(N-1) \end{pmatrix} = M_N \begin{pmatrix} s(0) \\ \vdots \\ s(N-1) \end{pmatrix};$$

quelle est l'inverse de cette matrice ? Quelle est l'inverse de la transformation DFT_N ? Pourquoi les puissances de 2 sont-elles intéressantes au niveau algorithmique ?

b. Soit $\sum_{k=0}^{N-1} z(k)X^k$ le reste dans la division euclidienne par $X^N - 1$ de

$$\Big(\sum_{k=0}^{N-1} x(k)X^k\Big)\Big(\sum_{k=0}^{N-1} y(k)X^k\Big)$$

(si $(x(0),...,x(N-1), y(0),...,y(N-1)$ sont des entrées complexes données). Comment peut-on calculer simplement la suite $(z(0),...,z(N-1))$ à partir des deux vecteurs d'entrées $(x(0),...,x(N-1))$ et $(y(0),...,y(N-1))$ en utilisant comme seules opérations la transformation de Fourier discrète d'ordre N, son inverse, et la multiplication terme à terme des vecteurs de $\mathbb{C}^N$?

3. Analyse temps-fréquences

a. Expliquer les défauts inhérents à l'analyse de Fourier d'un signal (en motivant vos explications avec quelques exemples bien sentis). En quoi le codage musical (développé depuis la Renaissance) propose-t'il un modèle plus réaliste pour le traitement des signaux numérique (comparé à la simple analyse du spectre via la transformation de Fourier globale) ? Comment pourriez vous traduire l'idée du codage musical sous forme d'un algorithme mathématique (on essaiera d'expliquer à un non-spécialiste le concept d'*analyse temps-fréquences*) ? Le concept d'analyse temps-fréquences se confond-t-il avec celui d'analyse temps-échelles ?

b. Suggérer quelques pistes exloitant ces idées d'analyse de Fourier, d'analyse temps-fréquences, d'analyse temps-échelles dans les méthodes de compression, de tatouage, ou de watermarking.

4. Algorithme pyramidal.

Donner une présentation (si possible au niveau vulgarisation pour un non mathématicien) de ce que l'on entend par *algorithme pyramidal* (agissant sur un signal 1D) et *décomposition de Franklin* d'un signal 1D. Quel est l'intérêt de telles opérations ? Tentez de mentionner quelques ponts entre ces techniques d'analyse du signal et la cryptographie (watermarking, tatouage de signaux numériques).