REMARQUES SUR LE CALCUL DE LA TRANSFORMATION D'HADAMARD

par

Robert Rolland

Résumé. — On présente en détail la transformation d'Hadamard rapide sur les fonctions à m variables booléennes en la mettant en relation avec la transformation de Fourier-Walsh sur les fonctions définies sur le compact de Cantor. On explique comment peut se faire le calcul. La preuve de l'algorithme est présentée de deux façons. D'une part à partir des sommes définissant la transformation, d'autre part à partir des matrices d'Hadamard et du produit tensoriel appelé aussi dans notre cas, produit de Kronecker.

Table des matières

1. Introduction

On rappelle que le compact de Cantor est le produit $\Omega = \{0,1\}^{\mathbb{N}^*}$ muni de la topologie produit des topologies discrètes. Il est aussi muni de la structure de groupe obtenue comme groupe produit. On a ainsi un groupe compact dont les caratères, appelés fonctions de Walsh, sont

définis à partir des suites $u = (u_1, \cdots, u_n, 0, \cdots)$ à support fini par la relation

$$W_u(v) = (-1)^{\langle u,v\rangle}.$$

La mesure dx est définie à partir de la probabilité produit lorsqu'on muni $\{0,1\}$ de la probabilité discrète équirépartie.

Soit un entier $\nu \geq 0$ et un entier $1 \leq j \leq 2^\nu$. On écrit $j-1 = \sum_{k=1}^{\nu} w_{\nu-k+1} 2^{k-1}$, ou encore $\frac{j-1}{2^\nu} = \sum_{k=1}^{\nu} \frac{w_k}{2^k}$ et on pose

$$\Omega_{j,\nu} = \{w_1\} \times \cdots \times \{w_\nu\} \times \prod_{i=\nu+1}^{\infty} \{0,1\}.$$

Remarques :

(1) Pour ν fixé, les 2^ν ensembles $\Omega_{j,\nu}$ forment une partition de Ω

(2) On obtient les $\Omega_{j,\nu+1}$ à partir des $\Omega_{j,\nu}$ par un découpage en deux. Plus précisément $\Omega_{j,\nu} = \Omega_{2j-1,\nu+1} \cup \Omega_{2j,\nu+1}$.

(3) La mesure de $\Omega_{j,\nu}$ est $1/2^\nu$.

(4) On peut dessiner une représentation approchée du compact de Cantor à partir du segment $[0,1]$, en positionnant le point $x = (x_1, x_2, \cdots)$ en

$$\sum_{i=1}^{\infty} \frac{x_i}{2^i}.$$

Les point dyadiques de $[0,1]$, qui ont deux représentation binaires, représentent donc deux points qui sont confondus sur le dessin mais éloignés dans Ω. On a ainsi un trou « topologique » en chacun de ces points dyadiques.

2. Ordonnons les fonctions de Walsh

2.1. Ordre sur les fonctions de Walsh. — Soit

$$u = (u_1, \cdots, u_m, 0, \cdots)$$

un élément à support fini de Ω. On associe à u l'entier

$$i(u) = \sum_{k=1}^{m} u_k 2^{k-1}.$$

La fonction de Walsh W_u sera numérotée $i(u)$ et on la notera aussi $W_{i(u)}$.

2.2. Série de Fourier-Walsh. — Les fonctions de Walsh étant numérotées, on peut définir la série de Fourier Walsh par

$$S(f) \sim \sum_{n=0}^{\infty} a_n(f) W_n$$

où

$$a_n(f) = \widehat{f}(n) = \int_\Omega f(x) W_n(x) \mathrm{d}x.$$

pour les fonctions pour lesquelles les intégrales définissant les coefficients existent.

2.3. Fonctions de Rademacher. — Les fonctions de Rademacher sont les fonctions de Walsh particulières suivantes :

(1) $r_0 = W_0 = 1$,
(2) $r_k(x) = W_{2^{k-1}}(x) = (-1)^{x_k}$.

Toute fonction de Walsh est produit de fonctions de Rademacher. En effet, soit $u \in \Omega$ un élément à support fini, notons $S(u)$ son support, c'est-à-dire :

$$S(u) = \{i \mid u_i = 1\}.$$

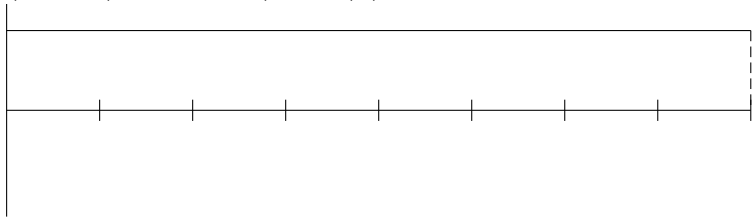
Nous avons alors :

$$W_u(x) = (-1)^{\langle u,x\rangle} = (-1)^{\sum_{i\in S(u)} x_i} = \prod_{i\in S(u)} (-1)^{x_i} = \prod_{i\in S(u)} r_i(x),$$

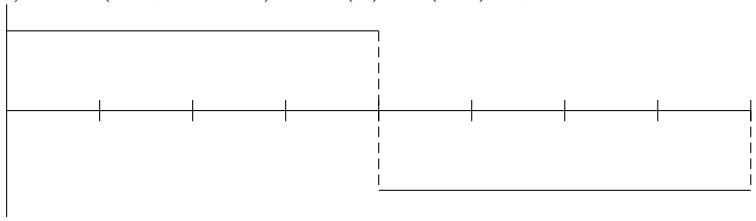
$$W_u = \prod_{i\in S(u)} r_i.$$

2.4. Bestiaire. — Nous donnons ici les dessins des 8 premières fonctions de Walsh.

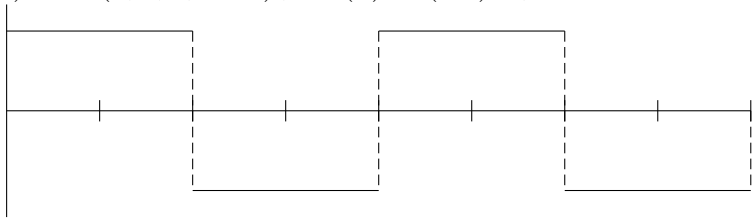
(1) $u = (0,0,0,0\cdots)$; $W_0(x) = 1$; $W_0 = r_0$:



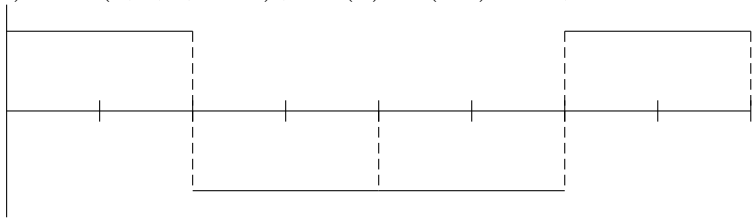
(2) $u = (1, 0, 0, 0 \cdots)$; $W_1(x) = (-1)^{x_1}$; $W_1 = r_1$:



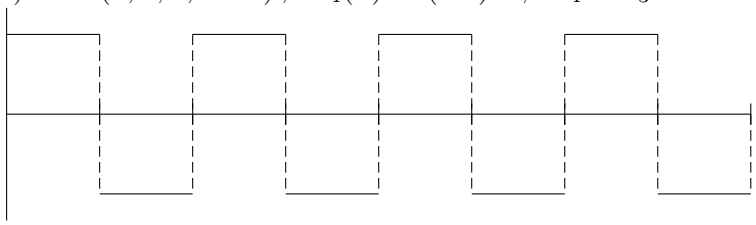
(3) $u = (0, 1, 0, 0 \cdots)$; $W_2(x) = (-1)^{x_2}$; $W_2 = r_2$:



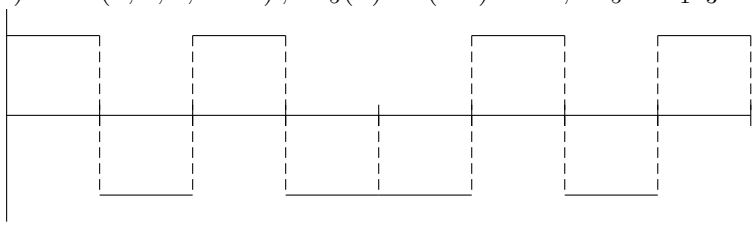
(4) $u = (1, 1, 0, 0 \cdots)$; $W_3(x) = (-1)^{x_1+x_2}$; $W_2 = r_1 r_2$:



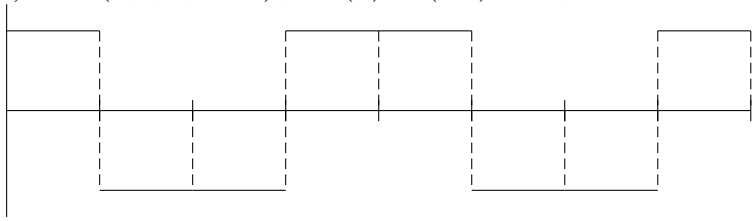
(5) $u = (0, 0, 1, 0 \cdots)$; $W_4(x) = (-1)^{x_3}$; $W_4 = r_3$:



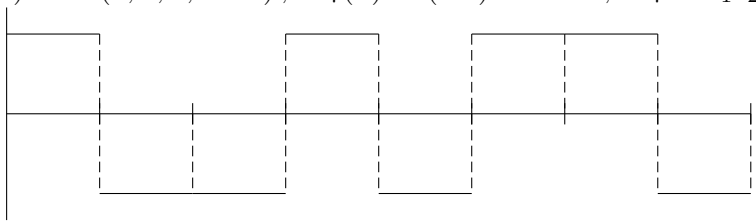
(6) $u = (1, 0, 1, 0 \cdots)$; $W_5(x) = (-1)^{x_1+x_3}$; $W_5 = r_1 r_3$:



(7) $u = (0, 1, 1, 0 \cdots)$; $W_6(x) = (-1)^{x_2+x_3}$; $W_6 = r_2 r_3$:



(8) $u = (1, 1, 1, 0 \cdots)$; $W_7(x) = (-1)^{x_1+x_2+x_3}$; $W_7 = r_1 r_2 r_3$:



3. Fonctions à m variables booléennes

Soit $E_m = \{0, 1\}^m$. Dans la suite nous noterons

$$V_m = E_m \times \{0\} \times \{0\} \times \cdots$$

Si f est une fonction définie sur $E_m = \{0, 1\}^m$ on peut considérer la fonction définie sur V_m qui vaut $f(x_1, \cdots x_m)$ au point $((x_1, \cdots x_m, 0, 0, \cdots)$. Par abus nous noterons encore f cette fonction. Si $x \in V_m$ notons Ω_x l'ensemble $\Omega_{j,m}$ qui contient x. À la fonction f on peut alors associer la fonction en escalier $\tilde{f}$ qui vaut $f(x)$ sur Ω_x. On dit que la fonction $\tilde{f}$ est une fonction localement constante. Elle peut s'écrire en utilisant les fonctions caractéristiques $\mathcal{I}_{\Omega_x}$ des 2^m ensembles $\Omega_{j,m}$ sous la forme

$$\tilde{f} = \sum_{x \in V_m} f(x) \mathcal{I}_{\Omega_x}.$$

Si u est aussi un élément de V_m alors la fonction W_u est aussi constante sur les $\Omega_{j,m}$. De ce fait les coefficients de Fourier pour $u \in V_m$ sont

$$a_u(\tilde{f}) = \int_\Omega \tilde{f}(t)(-1)^{\langle u,t \rangle} \mathrm{d}t,$$

$$a_u(\tilde{f}) = \frac{1}{2^m} \sum_{x \in V_m} f(x)(-1)^{\langle u,x \rangle}.$$

Remarquons que si $u \notin V_m$ alors

$$a_u(\tilde{f}) = 0.$$

On vient donc d'interpréter la transformée d'Hadamard de la fonction f définie sur E_m comme la transformée de Fourier-Walsh de la fonction $\tilde{f}$ définie sur Ω.

4. Questions d'indexation

Aussi bien les fonctions de Walsh que les points de E_m sont indexés par un élément de $V_m \subset \Omega$. Si on veut une numérotation de ces objets, il faut définir la façon de les indexer par un entier. Pour les fonctions de Walsh (les u donc) on a déjà choisi

$$i(u) = \sum_{k=1}^{m} u_k 2^{k-1}.$$

Pour les éléments de E_m qu'on a considéré comme des éléments de V_m et donc de Ω, il est naturel de les numéroter de telle sorte que l'ordre de leurs images dans le segment $[0, 1]$ soit respecté. On posera donc

$$j(x) = \sum_{k=1}^{m} x_{m-k+1} 2^{k-1},$$

ce qui donne

$$\frac{j(x)}{2^m} = \sum_{k=1}^{m} \frac{x_k}{2^k}.$$

Néammoins ces deux numérotations distinctes vont poser des problèmes et on sera amené à utiliser l'application r, « reverse bit » qui transforme un entier ayant une représentation binaire $\sum_{k=1}^{m} \alpha_k 2^{k-1}$ en l'entier qui a pour représentation binaire $\sum_{k=1}^{m} \alpha_{m-k+1} 2^{k-1}$. De ce fait on aura $r(j(x)) = i(x)$.

Exemple détaillé : On prend $m = 3$. Les points de E_3 sont tous les $x = (x_1, x_2, x_3)$, que nous allons écrire dans l'ordre :

$j(x)$	x_1	x_2	x_3
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	0	0
5	1	0	1
6	1	1	0
7	1	1	1

La fonction $\tilde{f}$ définie sur Ω est

$$\tilde{f} = f(0)\mathcal{I}_{\Omega_{1,3}} + f(1)\mathcal{I}_{\Omega_{2,3}} + f(2)\mathcal{I}_{\Omega_{3,3}} + f(3)\mathcal{I}_{\Omega_{4,3}} +$$

$$f(4)\mathcal{I}_{\Omega_{5,3}} + f(5)\mathcal{I}_{\Omega_{6,3}} + f(6)\mathcal{I}_{\Omega_{7,3}} + f(7)\mathcal{I}_{\Omega_{8,3}}.$$

5. Pratique de la transformation d'Hadamard

5.1. Notations. — Pour ne pas alourdir les calculs intermédiaires on va calculer $\mathcal{H}_{2^m}(f) = 2^m \widehat{f}$. Les valeurs de cette transformée sont données par

$$\mathcal{H}_{2^m}(f)(u) = \sum_{x=0}^{2^m-1} f(x)(-1)^{\langle u,x\rangle}.$$

On introduira la constante $\frac{1}{2^m}$, si besoin est, à la fin des calculs. On notera H_{2^m} la matrice qui effectue la transformation quand la fonction f est donnée par le vecteur colonne $(f(x))$ où *les composantes sont ordonnées suivant les valeurs de* $i(x)$ *(et non pas suivant les valeurs de* $j(x)$*)* et que le résultat est donné par le vecteur colonne $(\mathcal{H}_{2^m}(f)(u))$ où les composantes sont ordonnées suivant les valeurs de $i(u)$.

La matrice H_{2^m} est telle que

$$H_{2^m} = \left((-1)^{\langle u,x\rangle}\right)_{0\le i(u),i(x)\le 2^m-1}.$$

5.2. La transformation, étude directe. — Notons

$$\overline{x} = (x_1, x_2, \cdots, x_{m-1}) \text{ et } \overline{u} = (u_1, u_2, \cdots, u_{m-1}).$$

Nous avons alors

$$\mathcal{H}_{2^m}(f)(u) = \sum_{x=0}^{2^{m-1}-1} f(x)(-1)^{\langle u,x\rangle} + \sum_{x=0}^{2^{m-1}-1} f(x+2^{m-1})(-1)^{\langle u,x\rangle}.$$

Dans la première somme du membre de droite, $x_m = 0$, tandis que dans la deuxième somme $x_m = 1$ si bien que

$$\mathcal{H}_{2^m}(f)(u) = \sum_{x=0}^{2^{m-1}-1} f(x)(-1)^{\langle \overline{u},\overline{x}\rangle} + (-1)^{u_m} \sum_{x=0}^{2^{m-1}-1} f(x+2^{m-1})(-1)^{\langle \overline{u},\overline{x}\rangle}.$$

Notons f_1 et f_2 les fonctions définies pour $0 \leq x \leq 2^{m-1}-1$ par

$$f_1(x) = f(x) + f(x+2^{m-1}) \quad f_2(x) = f(x) - f(x+2^{m-1}).$$

On voit alors que pour $0 \leq u \leq 2^{m-1}-1$ on a

$$\mathcal{H}_{2^m}(f)(u) = \mathcal{H}_{2^{m-1}}(f_1)(u),$$

$$\mathcal{H}_{2^m}(f)(u+2^m) = \mathcal{H}_{2^{m-1}}(f_2)(u).$$

Compte tenu de ces relations, l'algorithme de calcul est alors le suivant :

(1) On met les 2^m valeurs prises par f dans un tableau de taille 2^m après avoir fait un reverse bit. Plus précisément à la position $i(x)$ on met $f(j(x))$. Les composantes de ce tableau sont appelées $a_0, a_1, \cdots, a_{2^m-1}$.

(2) On construit un tableau de même taille 2^m de la façon suivante : dans la première moitié du tableau on met $a_i + a_{i+2^{m-1}}$ à la position i et dans la deuxième moitié du tableau on met $a_i - a_{i+2^{m-1}}$ à la position $i + 2^{m-1}$ (remarquons qu'ici on fait varier x entre 0 et $2^{m-1}-1$).

(3) On itère cette transformation sur chacun des deux tableaux moitiés du tableau qu'on vient de construire. Chacune de ces transformations se fait maintenant sur des tableaux de taille moitié, et ceci jusqu'à obtenir des tableaux de taille 1 auquel cas il n'y a plus rien à faire, on a les coefficients d'Hadamard.

Remarque : Au début on a un tableau de taille 2^m, ensuite on obtient un tableau de taille 2^m coupé en deux tableaux de taille 2^{m-1}, à l'étape suivante on aura un tableau de taille 2^m coupé en 4 tableaux de taille

2^{m-2} et ainsi de suite, jusqu'à l'étape m où l'on obtient un tableau de taille 2^m découpé en 2^m tableaux de taille 1.

Ainsi le calcul demande exactement m étapes à chaque étape on fait 2^{m-1} sommes et 2^{m-1} différences. Le calcul se fait donc en $m2^m$ opérations élémentaires c'est-à-dire que si on note $n = 2^m$ la taille du vecteur des valeurs prises par f on a un algorithme qui demande $n \log_2(n)$ opérations élémentaires.

Décrivons l'algorithme par un dessin (le papillon) pour le cas $m = 3$. Notons les valeurs prises par f (remarquer le reverse bit) :

$$f(0) = f(0,0,0) = a_0, f(4) = f(1,0,0) = a_1,$$
$$f(2) = f(0,1,0) = a_2, f(6) = f(1,1,0) = a_3,$$
$$f(1) = f(0,0,1) = a_4, f(5) = f(1,0,1) = a_5,$$
$$f(3) = f(0,1,1) = a_6, f(7) = f(1,1,1) = a_7.$$

La transformation se fait conformément à la figure 1. À chaque étape (ici 3 étapes) on ne fait que des additions et des soustractions.

5.3. La transformation, étude matricielle. — Revenons à la transformation vue sous sa forme matricielle. On rappelle que la matrice de la transformation est

$$H_{2^m} = \left((-1)^{\langle u,x\rangle}\right)_{0\leq u,x\leq 2^m-1}.$$

Il est facile de montrer directement sur la forme des coefficients de la matrice que

$$H_{2^m} = \begin{pmatrix} H_{2^{m-1}} & H_{2^{m-1}} \\ H_{2^{m-1}} & -H_{2^{m-1}} \end{pmatrix}.$$

En particulier,

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

et de ce fait on peut écrire en utilisant le produit tensoriel (ou produit de Kronecker) des matrices :

$$H_{2^m} = H_2 \otimes H_{2^{m-1}}.$$

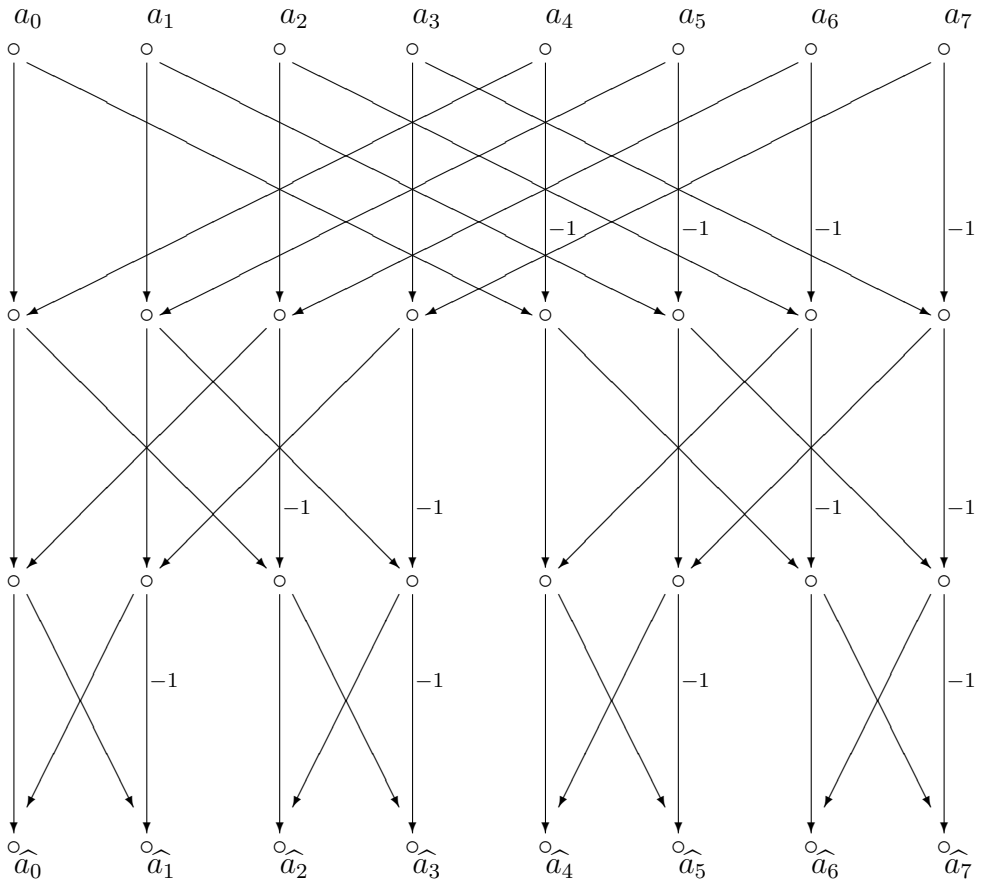


FIGURE 1. La FHT sur 8 points

Introduisons les m matrices suivantes qui correspondent aux m étapes du paragraphe précédent.

$$M_{2^m}^1 = H_2 \otimes I_{2^{m-1}}$$

$$M_{2^m}^2 = I_2 \otimes M_{2^{m-1}}^1 = I_2 \otimes H_2 \otimes I_{2^{m-2}}$$

$$M_{2^m}^k = I_{2^{k-1}} \otimes M_{2^{m-k+1}}^1 = I_{2^{k-1}} \otimes H_2 \otimes I_{2^{m-k}}.$$

$$M_{2^m}^m = I_{2^{m-1}} \otimes M_2^1 = I_{2^{m-1}} \otimes H_2.$$

Pour $m = 3$ on a

$$M_8^1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$M_8^2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

$$M_8^3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

Les démonstrations faites dans le paragraphe précédent prouvent que

$$H_{2^m} = M_{2^m}^m . M_{2^m}^{m-1} \cdots M_{2^m}^2 . M_{2^m}^1 \tag{1}$$

Cependant, ceci peut se redémontrer directement par le calcul sur les produits de Kronecker en utilisant les résultats généraux suivants :

Théorème 5.1. — *Sous réserve de la cohérence des tailles des matrices carrées A, B, C, D nous avons les relations suivantes :*

(1) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
(2) $(A + B) \otimes C = (A \otimes C) + (B \otimes C)$

(3) $(A \otimes B).(C \otimes D) = (A.C) \otimes (B.D)$

Démontrons directement la relation (1). On va montrer que pour $1 \leq k \leq m$ on a

$$M_{2^m}^k . M_{2^m}^{k-1} \cdots M_{2^m}^1 = H_{2^k} \otimes I_{2^{m-k}}.$$

On remarque que cette relation est vraie pour $k = 1$, et si on la suppose pour $1 < k < m$ alors on a successivement

$$M_{2^m}^{k+1} . M_{2^m}^k \cdots M_{2^m}^1 = (I_{2^k} \otimes H_2 \otimes I_{2^{m-k-1}}).(H_{2^k} \otimes I_{2^{m-k}})$$
$$M_{2^m}^{k+1} . M_{2^m}^k \cdots M_{2^m}^1 = (I_{2^k}.H_{2^k}) \otimes ((H_2 \otimes I_{2^{m-k-1}}).I_{2^{m-k}}),$$
$$M_{2^m}^{k+1} . M_{2^m}^k \cdots M_{2^m}^1 = H_{2^k} \otimes H_2 \otimes I_{2^{m-k-1}} = H_{2^{k+1}} \otimes I_{2^{m-k-1}}.$$

La relation est donc vraie à l'ordre $k+1$ et par suite pour tout $1 \leq k \leq m$. En particulier pour $k = m$ on obtient la relation (1).

De la même façon on peut montrer la relation suivante qui prouve qu'on peut aussi calculer les coefficients d'Hadamard en prenant les transformations précédentes dans l'ordre inverse :

$$H_{2^m} = M_{2^m}^1 . M_{2^m}^2 \cdots M_{2^m}^{m-1} . M_{2^m}^m \tag{2}$$

---

30 Décembre 2008

R. Rolland, Association ACrypTA, 50 Rue Edmond Rostand 13006 Marseille,
E-mail : robert.rolland@acrypta.fr