UNE CONSTRUCTION DE MATRICES DE HADAMARD

par Roland BACHER

Je dédie cet article à la mémoire de François Jaeger

RÉSUMÉ . — Le but de ce papier est de présenter une construction de matrices de Hadamard à partir de certaines suites à valeurs dans $\{\pm 1\}$.
L'existence de telles suites est liée à l'arithmétique de certains corps cyclotomiques et des corps finis.

0. Introduction

DÉFINITION 0.1. — Une suite $s = (s_1, \ldots, s_{2m-1})$ est *de type Hadamard* si elle vérifie les conditions suivantes :

(i) $s_1, \ldots, s_{2m-1} \in \{\pm 1\}$,

(ii) $s_{2m-k} = (-1)^{m+k} s_k$ pour $k = 1, \ldots, 2m-1$ (supersymétrie),

(iii) $\mathrm{Corr}_k(s) = \mathrm{Corr}_{2m-k}(s)$ pour $k = 1, \ldots, 2m-1$ où

$$\mathrm{Corr}_k(s) = \sum_{i=1}^{2m-1-k} s_i s_{i+k}$$

est la $k-$ième autocorrélation (apériodique) de la suite s.

L'étude de ces suites et de leur liens avec des objets combinatoires bien connus (matrices de conférence, matrices de Hadamard, codes) constitue le contenu de ce papier.

La section 1 rappelle les définitions et quelque faits bien connus sur les matrices de conférence et les matrices de Hadamard.

La section 2 donne deux constructions de matrices de conférence à partir d'une suite de type Hadamard.

Classification math. : 05B20.
Mots-clés : matrice de conférence, matrice de Hadamard.

La section 3 étudie les rapports entre l'existence de suites de type Hadamard de longueur donnée et l'arithmétique des corps cyclotomiques et des corps finis.

La section 4 est une brève digression sur les liens entre suites de type Hadamard et codes.

La section 5 contient essentiellement la liste complète de toutes les suites de type Hadamard de longueur ≤ 61.

1. Matrices de Hadamard et matrices de conférence

DÉFINITION 1.1. — Une *matrice de Hadamard d'ordre n* est une matrice $H \in M_{n\times n}$ à coefficients ± 1 telle que $HH^t = n\,\mathrm{Id}$.

Pour qu'une matrice de Hadamard d'ordre $n > 2$ existe, il faut que n soit divisible par 4. On conjecture que cette condition est également suffisante (voir chapitre 18 dans [**vLW**]).

DÉFINITION 1.2. — Une *matrice de conférence d'ordre n* est une matrice $C \in M_{n\times n}$ à coefficients ± 1 hors diagonale et zéro sur la diagonale telle que $CC^t = (n-1)\,\mathrm{Id}$.

Une matrice de conférence d'ordre $n > 1$ ne peut exister que pour n pair. Une matrice de conférence d'ordre n est toujours équivalente à une matrice de conférence symétrique pour $n \equiv 2 \pmod 4$ respectivement antisymétrique pour $n \equiv 0 \pmod 4$ (deux matrices de conférences C et C' sont équivalentes s'il existe des matrices diagonales D, D' à coefficients ± 1 et une matrice de permutation P telles que $C' = PDCD'P^t$).

Le lemme suivant permet la construction de matrices de Hadamard à partir de matrices de conférence.

LEMME 1.3.

(i) Soit C une matrice de conférence. Alors les matrices

$$\begin{pmatrix} \mathrm{Id}_n + C & -\mathrm{Id}_n + C^t \\ -\mathrm{Id}_n + C & -\mathrm{Id}_n - C^t \end{pmatrix} \qquad et \qquad \begin{pmatrix} -\mathrm{Id}_n + C & \mathrm{Id}_n + C^t \\ \mathrm{Id}_n + C & \mathrm{Id}_n - C^t \end{pmatrix}$$

et leurs transposées sont des matrices de Hadamard.

(ii) Soit C une matrice de conférence antisymétrique. Alors les matrices $C + \mathrm{Id}_n$ *et* $C - \mathrm{Id}_n$ *sont des matrices de Hadamard.*

La preuve de ce lemme facile et bien connu est laissée au lecteur (voir aussi les théorèmes 18.2 et 18.3 dans [**vLW**]).

Voici une construction classique de matrices de conférence :

Exemple 1.4. Les matrices de Paley. — Soit $\mathbf{F}_q$ un corps fini de caractéristique différente de 2. Soit

$$\psi : \mathbf{F}_q^* \longrightarrow \{\pm 1\}$$

l'homomorphisme donné par $\psi(x) = x^{(q-1)/2}$ que nous étendons à $\mathbf{F}_q$ en posant $\psi(0) = 0$.

Soient $v_0, v_1, \ldots, v_q \in \mathbf{F}_q^2$ des représentants de tous les points de la droite projective $\mathbf{P}^1\mathbf{F}_q$ et soit $\omega : \mathbf{F}_q^2 \longrightarrow \mathbf{F}_q$ une forme symplectique non-dégénérée sur $\mathbf{F}_q^2$.

La matrice $A_{ij} = \psi(\omega(v_i, v_j))$ est alors une matrice de conférence symétrique pour $q \equiv 1 \pmod 4$ et une matrice de conférence antisymétrique pour $q \equiv 3 \pmod 4$.

On peut donc associer une matrice de Hadamard à chaque corps fini F_q de caractéristique impair. Cette matrice est d'ordre $q+1$ pour q congru à 3 modulo 4 (utiliser (ii) du lemme 1.3) et elle est d'ordre $2q+2$ pour q congru à 1 modulo 4 (utiliser (i) du lemme 1.3).

Citons pour terminer une construction, due à VFR. Jones, qui généralise le produit de Kronecker (voir théorème 18.4 dans [**vLW**]) de deux matrices. Cette construction permet de construire beaucoup de matrices de Hadamard d'ordre nm à partir de deux matrices de Hadamard d'ordres n et m.

Proposition 1.5. (Produit tordu de VFR. Jones). — *Soit $A = (a_{i,j})_{0\le i,j<n}$ une matrice de Hadamard d'ordre n et $B = (b_{i,j})_{0\le i,j<m}$ une matrice de Hadamard d'ordre m et $T = (t_{j,k})_{0\le j<n,\ 0\le k<m}$ une matrice $n\times m$ à coefficients ± 1. Soit $H = (h_{ik,jl})_{0\le i,j<n,\ 0\le k,l<m}$ la matrice $nm \times nm$ définie par*

$$h_{ik,jl} = a_{i,j}t_{j,k}b_{k,l} \quad .$$

Alors H est une matrice de Hadamard.

Preuve. — On a

$$\begin{aligned}
\sum_{u,v} h_{ik,uv}h_{jl,uv} &= \sum_{uv} a_{i,u}t_{u,k}b_{k,v}a_{j,u}t_{u,l}b_{l,v} \\
&= \sum_{u} a_{i,u}t_{u,k}a_{j,u}t_{u,l}\sum_{v} b_{k,v}b_{l,v} \\
&= \sum_{u} a_{i,u}t_{u,k}a_{j,u}t_{u,l}m\delta_{k,l} \\
&= m\delta_{k,l}\sum_{u} a_{i,u}a_{j,u} = m\delta_{k,l}n\delta_{i,j} \\
&= mn\delta_{ik,jl}
\end{aligned}$$

2. Construction de matrices de conférence

Soit m un entier naturel et soit $s = (s_1, \ldots, s_{2m-1})$ une suite finie de longueur impaire $2m-1$. Soit $C(s) \in M_{2m\times 2m}$ la matrice suivante associée à la suite s :

Si m est impair, la matrice $C(s)$ est la matrice symétrique suivante :

$$C(s) = \begin{pmatrix} 0 & s_1 & s_2 & s_3 & s_4 & s_5 & \ldots \\ s_1 & 0 & -s_1 & -s_2 & -s_3 & -s_4 & \ldots \\ s_2 & -s_1 & 0 & s_1 & s_2 & s_3 & \ldots \\ s_3 & -s_2 & s_1 & 0 & -s_1 & -s_2 & \\ s_4 & -s_3 & s_2 & -s_1 & 0 & s_1 & \\ s_5 & -s_4 & s_3 & -s_2 & s_1 & 0 & \\ \vdots & \vdots & \vdots & & & & \end{pmatrix},$$

si m est pair la matrice $C(s)$ est la matrice antisymétrique suivante :

$$C(s) = \begin{pmatrix} 0 & s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & \ldots \\ -s_1 & 0 & -s_1 & -s_2 & -s_3 & -s_4 & -s_5 & -s_6 & \ldots \\ -s_2 & s_1 & 0 & s_1 & s_2 & s_3 & s_4 & s_5 & \ldots \\ -s_3 & s_2 & -s_1 & 0 & -s_1 & -s_2 & -s_3 & -s_4 & \\ -s_4 & s_3 & -s_2 & s_1 & 0 & s_1 & s_2 & s_3 & \\ -s_5 & s_4 & -s_3 & s_2 & -s_1 & 0 & -s_1 & -s_2 & \\ -s_6 & s_5 & -s_4 & s_3 & -s_2 & s_1 & 0 & s_1 & \\ -s_7 & s_6 & -s_5 & s_4 & -s_3 & s_2 & -s_1 & 0 & \\ \vdots & \vdots & \vdots & & & & & & \end{pmatrix}.$$

Le coefficient $c_{i,j}$ ($0 \leq i, j < 2m$) de la matrice $C(s)$ est donc donné par

$$\begin{array}{lcll} c_{i,j} & = & (-1)^i s_{j-i} & \text{si} \quad i < j\,, \\ c_{i,i} & = & 0\,, & \\ c_{i,j} & = & (-1)^{j+m+1} s_{i-j} & \text{si} \quad i > j\,. \end{array}$$

THÉORÈME 2.1. — *Soit $s = (s_1, \ldots, s_{2m-1})$ une suite de longueur $2m-1$. Alors $C(s)$ est une matrice de conférence si et seulement si s est de type Hadamard.*

Ce théorème est un corollaire facile des lemmes 2.2 et 2.3 ci-dessous.

On dira qu'une suite $s = (s_1, \ldots, s_{2m-1})$ de longueur $2m-1$ est *supersymétrique* si on a

$$s_k = (-1)^{m+k} s_{2m-k}$$

pour $k = 1, \ldots, 2m-1$.

LEMME 2.2. — *Soit $s = (s_1, \ldots, s_{2m-1})$ une suite à valeurs dans $\mathbf{R} \setminus \{0\}$.*

Les deux assertions suivantes sont équivalentes :

(i) Deux vecteurs lignes quelconques de la matrice $C(s)$ construite ci-dessus dont les indices n'ont pas la même parité sont orthogonaux.

(ii) La suite s est supersymétrique.

Preuve. — On a pour $0 \leq 2i < 2j+1 < 2m$:

$$\begin{aligned}
&\sum_{k=0}^{2m-1} c_{2i,k}\, c_{2j+1,k} \\
&\quad = \sum_{k=0}^{2i-1} \big((-1)^{k+m+1} s_{2i-k}\big)\big((-1)^{k+m+1} s_{2j+1-k}\big) \\
&\qquad + \sum_{k=2i+1}^{2j} s_{k-2i}\big((-1)^{k+m+1} s_{2j+1-k}\big) \\
&\qquad + \sum_{k=2j+2}^{2m-1} s_{k-2i}\big(-s_{k-2j-1}\big) \\
&\quad = (s_{2i}s_{2j+1} + s_{2i-1}s_{2j} + \ldots + s_1 s_{2j-2i+2}) \\
&\qquad + (-1)^m (s_1 s_{2j-2i} - s_2 s_{2j-2i-1} + s_3 s_{2j-2i-2} - \ldots \\
&\qquad \ldots + s_{2j-2i-1}s_2 - s_{2j-2i}s_1\big) \\
&\qquad - \big(s_{2j-2i+2}s_1 + s_{2j-2i+3}s_2 + \ldots + s_{2m-2i-1}s_{2m-2j-2}\big) \\
&\quad = (s_{2i}s_{2j+1} + s_{2i-1}s_{2j} + \ldots + s_1 s_{2j-2i+2}) - (s_{2j-2i+2}s_1 + s_{2j-2i+3}s_2 + \ldots \\
&\qquad \ldots + s_{2m-2i-1}s_{2m-2j-2}\big) \\
&\quad = \begin{cases} s_{2m-2j-1}s_{2m-2i} + s_{2m-2j}s_{2m-2i+1} + \ldots + s_{2i}s_{2j+1} & \text{si } i+j \geq m-1 \\ -\big(s_{2i+1}s_{2j+2} + s_{2i+2}s_{2j+3} + \ldots + s_{2m-2j-2}s_{2m-2i-1}\big) & \text{si } i+j < m-1 \end{cases}
\end{aligned}$$

Un calcul analogue donne pour $0 < 2i+1 < 2j < 2m-1$:

$$\begin{aligned}
&\sum_{k=0}^{2m-1} c_{2i+1,k}\, c_{2j,k} \\
&\quad = \sum_{k=0}^{2i} \big((-1)^{k+m+1} s_{2i-k+1}\big)\big((-1)^{k+m+1} s_{2j-k}\big) \\
&\qquad + \sum_{k=2i+2}^{2j-1} \big(-s_{k-2i-1}\big)\big((-1)^{k+m+1} s_{2j-k}\big)
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{k=2j+1}^{2m-1} \big(- s_{k-2i-1}\big) s_{k-2j} \\
&= (s_{2i+1}s_{2j} + s_{2i}s_{2j-1} + \ldots + s_1 s_{2j-2i}) \\
&\quad + (-1)^m (s_1 s_{2j-2i-2} - s_2 s_{2j-2i-3} + s_3 s_{2j-2i-4} - \ldots + s_{2j-2i-3}s_2 - s_{2j-2i-2}s_1\big) \\
&\quad - \big(s_{2j-2i}s_1 + s_{2j-2i+1}s_2 + \ldots + s_{2m-2i-2}s_{2m-2j-1}\big) \\
&= (s_{2i+1}s_{2j} + s_{2i}s_{2j-1} + \ldots + s_1 s_{2j-2i}) - \big(s_{2j-2i}s_1 + s_{2j-2i+1}s_2 + \ldots \\
&\quad \ldots + s_{2m-2i-2}s_{2m-2j-1}\big) \\
&= \begin{cases} s_{2m-2j-1}s_{2m-2i} + s_{2m-2j}s_{2m-2i+1} + \ldots + s_{2i}s_{2j+1} & \text{si } i+j \geq m-1 \\ -\big(s_{2i+1}s_{2j+2} + s_{2i+2}s_{2j+3} + \ldots + s_{2m-2i-1}s_{2m-2j-2}\big) & \text{si } i+j < m-1 \end{cases}
\end{aligned}
$$

Supposons maintenant que la matrice $C(s)$ associée à la suite $s = (s_1, \ldots, s_{2m-1})$ satisfasse la condition (i) du lemme 2.2.

Si m est pair on obtient donc

$$0 = \sum_{k=0}^{2m-1} c_{m,k}c_{m+1,k} = s_{m-1}s_m + s_m s_{m+1} = s_m(s_{m-1} + s_{m+1})$$

et ceci montre l'identité $s_{m+1} = -s_{m-1}$.

On a de même

$$
\begin{aligned}
0 &= \sum_{k=0}^{2m-1} c_{m-1,k}c_{m,k} = s_{m-1}s_{m-2} + s_m s_{m-1} + s_{m+1}s_m + s_{m+2}s_{m+1} \\
&= s_{m-1}(s_{m-2} - s_{m+2})
\end{aligned}
$$

ce qui implique $s_{m+2} = s_{m-2}$.

$$
\begin{aligned}
0 &= \sum_{k=0}^{2m-1} c_{m,k}c_{m+3,k} = s_{m-3}s_m + s_{m-2}s_{m+1} + s_{m-1}s_{m+2} + s_{m+3}s_m \\
&= s_m(s_{m-3} + s_{m+3})
\end{aligned}
$$

ce qui implique $s_{m+3} = -s_{m-3}$. En itérant on obtient donc l'assertion (ii).

Si m est impair on a

$$0 = \sum_{k=0}^{2m-1} c_{m-1,k}c_{m,k} = (s_m s_m + 1 + s_{m-1}s_m) = s_m(s_{m+1} + s_{m-1})$$

ce qui montre $s_{m+1} = -s_{m-1}$. Puis

$$
\begin{aligned}
0 &= \sum_{k=0}^{2m-1} c_{m,k}c_{m+1,k} = s_{m-1}s_{m-2} + s_m s_{m-1} + s_{m+1}s_m + s_{m+2}s_{m+1} \\
&= s_{m-1}(s_{m-2} - s_{m+2})
\end{aligned}
$$

ce qui implique $s_{m+2} = s_{m-2}$ etc.

L'implication (ii) $\Longrightarrow$ (i) est un petit calcul laissé au lecteur. QED

LEMME 2.3. — *Si la suite* $s = (s_1, \ldots, s_{2m-1})$ *est supersymétrique, alors on a pour* $k = 1, \ldots, m-1$, $i = 0, \ldots, 2m-2k-1$

$$\sum_{l=0}^{2m-1} c_{i,l} c_{i+2k,l} = \mathrm{Corr}_{2k}(s) - \mathrm{corr}_{2m-2k}(s) \quad .$$

Preuve. — On a

$$\begin{aligned}
\sum_{l=0}^{2m-1} c_{i,l} c_{i+2k,l} = &\sum_{l=0}^{i-1} (-1)^{l+m+1} s_{i-l} (-1)^{l+m+1} s_{i+2k-l} \\
&+ \sum_{l=i+1}^{i+2k-1} (-1)^{i} s_{l-i} (-1)^{l+m+1} s_{i+2k-l} \\
&+ \sum_{l=i+2k+1}^{2m-1} (-1)^{i} s_{l-i} (-1)^{i+2k} s_{l-i-2k} \\
=&(s_i s_{i+2k} + s_{i-1} s_{i+2k-1} + \ldots + s_{2k-1} s_1) \\
&+ (-1)^m (s_1 s_{2k-1} - s_2 s_{2k-2} + \ldots + s_1 s_{2k-1}) \\
&+ (s_{2k+1} s_1 + s_{2k+2} s_2 + \ldots + s_{2m-i-1} s_{2m-i-2k-1}) \\
=&(s_{2m-i} s_{2m-i-2k} + s_{2m-i+1} s_{2m-i-2k+1} + \ldots + s_{2m-1} s_{2m-2k-1}) \\
&+ (-1)^m (s_1 s_{2k-1} - s_2 s_{2k-2} + \ldots + s_1 s_{2k-1}) \\
&+ (s_{2k+1} s_1 + s_{2k+2} s_2 + \ldots + s_{2m-i-1} s_{2m-i-2k-1}) \\
=&\ \mathrm{Corr}_{2k}(s) - (s_1 s_{2m-2k+1} + s_2 s_{2m-2k+2} + \ldots + s_{2k-1} s_{2m-1} \\
=&\ \mathrm{Corr}_{2k}(s) - \mathrm{Corr}_{2m-2k}(s)
\end{aligned}$$

ce qui démontre le lemme. QED

Voici quelques transformations simples qui préservent les suites de type Hadamard.

PROPOSITION 2.4.

(i) Si la suite $s = (s_1, \ldots, s_{2m-1})$ *est de type Hadamard, alors* $(-s_1, -s_2, -s_3, \ldots, -s_{2m-1})$ *est de type Hadamard.*

(ii) Si $s = (s_1, \ldots, s_{2m-1})$ *est de type Hadamard, alors* $t = (t_1, \ldots, t_{2m-1}) = (-s_1, s_2, -s_3, \ldots, -s_{2m-1})$ *est de type Hadamard où* $t_l = (-1)^l s_l$.

(iii) Si $s = (s_1, \ldots, s_{4n-1})$ *est une suite de longueur* $4n-1$ *qui est de type Hadamard, alors la suite* $t = (t_1, \ldots, t_{4n-1})$ *définie par*

$$\begin{array}{ll}
t_{2l} = (-1)^l s_{2l} & \text{pour } l = 1, \ldots, 2n-1, \\
t_{2l+1} = (-1)^l s_{2n+2l+1} & \text{pour } l = 0, \ldots, n-1, \\
t_{4n-l} = (-1)^l t_l & \text{pour } l = 1, \ldots, 2n-1
\end{array}$$

est aussi de type Hadamard.

Preuve. — Les assertions (i) et (ii) sont faciles à vérifier. L'assertion (iii) résulte du lemme suivant :

LEMME 2.5. — *Soit* $s = (s_1, s_2, \ldots, s_{4n-1})$ *une suite supersymétrique.*

Soit $t = (t_1, t_2, \ldots, t_{4n-1})$ *la suite supersymétrique définie par*

$$\begin{array}{ll} t_{2l} = (-1)^l s_{2l} & \text{pour } l = 1, \ldots, 2n-1, \\ t_{2l+1} = (-1)^l s_{2n+2l+1} & \text{pour } l = 0, \ldots, n-1, \\ t_{4n-l} = (-1)^l t_l & \text{pour } l = 1, \ldots, 2n-1 \end{array}$$

Alors on a

$$(-1)^k \big(\mathrm{Corr}_{2k}(t) - \mathrm{Corr}_{4n-2k}(t) \big) = \mathrm{Corr}_{2k}(s) - \mathrm{Corr}_{4n-2k}(s)$$

pour $k = 1, \ldots, 2n-1$.

Preuve. — Il suffit de démontrer la proposition pour $k = 1, \ldots, n-1$.

En utilisant $s_{4n-l} = (-1)^l s_l$ et $t_{4n-l} = (-1)^l t_l$ on obtient alors pour $1 \leq k \leq n-1$:

$$\begin{array}{rcl} \mathrm{Corr}_{2k}(s) & = & 2(s_1 s_{2k+1} + s_3 s_{2k+3} + \ldots + s_{2n-2k-1} s_{2n-1}) \\ & & -(s_{2n-2k+1} s_{2n-1} + s_{2n-2k+3} s_{2n-3} + \ldots + s_{2n-1} s_{2n-2k+1}) \\ & & +(s_2 s_{2k+2} + s_4 s_{2k+4} + \ldots + s_{4n-2k-2} s_{4n-2}) \\ \mathrm{Corr}_{4n-2k}(s) & = & -(s_1 s_{2k-1} + s_3 s_{2k-3} + \ldots + s_{2k-1} s_1) \\ & & +(s_2 s_{4n-2k+2} + s_4 s_{4n-2k+4} + \ldots + s_{2k-2} s_{4n-2}) \end{array}$$

et

$$\begin{array}{rcl} (-1)^k \mathrm{Corr}_{2k}(t) & = & 2(s_1 s_{2k+1} + s_3 s_{2k+3} + \ldots + s_{2n-2k-1} s_{2n-1}) \\ & & +(s_{2k-1} s_1 + s_{2k-3} s_3 + \ldots + s_1 s_{2k-1}) \\ & & +(s_2 s_{2k+2} + s_4 s_{2k+4} + \ldots + s_{4n-2k-2} s_{4n-2}) \\ (-1)^k \mathrm{Corr}_{4n-2k}(t) & = & (s_{2n-1} s_{2n-2k+1} + s_{2n-3} s_{2n-2k+3} + \ldots + s_{2n-2k+1} s_{2n-1}) \\ & & +(s_2 s_{4n-2k+2} + s_4 s_{4n-2k+4} + \ldots + s_{2k-2} s_{4n-2}) \end{array}$$

ce qui démontre le lemme. QED

Remarque 2.6. — Étant donné une suite supersymétrique $s = (s_1, \ldots, s_{2m-1})$ la suite $\tilde{s} = (\tilde{s}_1, \ldots, \tilde{s}_{2m-1})$ définie par $\tilde{s}_{2i+1} = (-1)^i s_{2i+1}$ et $\tilde{s}_{2i} = (-1)^i s_{2i}$ est symétrique (ie vérifie $\tilde{s}_k = \tilde{s}_{2m-k}$). De plus, la suite s est de type Hadamard si et seulement si la suite symétrique $\tilde{s}$ est à coefficients ± 1 et vérifie

$$\mathrm{Corr}_{2k}(\tilde{s}) = (-1)^m \mathrm{Corr}_{2m-2k}(\tilde{s})$$

pour $k = 1, \ldots, m-1$.

Étant donné une suite symétrique $\tilde{s}$ qui satisfait les conditions ci-dessus, on obtient une matrice de conférence (antisymétrique pour m pair et symétrique pour m impair) $\tilde{C}(\tilde{s})$ en considérant

$$\begin{pmatrix} 0 & \tilde{s}_1 & \tilde{s}_2 & \tilde{s}_3 & \tilde{s}_4 & \tilde{s}_5 & \dots \\ \mp\tilde{s}_1 & 0 & \tilde{s}_1 & -\tilde{s}_2 & \tilde{s}_3 & -\tilde{s}_4 & \dots \\ \mp\tilde{s}_2 & \mp\tilde{s}_1 & 0 & \tilde{s}_1 & \tilde{s}_2 & \tilde{s}_3 & \dots \\ \mp\tilde{s}_3 & \pm\tilde{s}_2 & \mp\tilde{s}_1 & 0 & \tilde{s}_1 & \tilde{s}_2 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Je ne développe pas ce point de vue car on a toujours $\tilde{C}(\tilde{s}) = DC(s)D$ pour D une matrice diagonale à coefficients ± 1 convenable. On n'obtient donc rien de nouveau du point de vue des matrices de conférence (ou des matrices de Hadamard).

Pour terminer cette section, voici une construction encore plus simple de matrices de conférence à partir de suites de type Hadamard.

DÉFINITION 2.7. — Une suite $s = (s_1, \dots, s_{2m-1})$ est *de type Hadamard faible* si elle satisfait les conditions (i) et (iii) dans la définition 0.1, ie. si on a $s_1, \dots, s_{2m-1} \in \{\pm 1\}$ et $\mathrm{Corr}_k(s) = \mathrm{Corr}_{2m-k}(s)$ pour $k = 1, \dots, 2m-1$.

Les suites de type Hadamard sont donc les suites de type Hadamard faible qui sont en plus supersymétriques. Je ne connais cependant aucune suite de type Hadamard faible qui ne soit pas supersymétrique. En effet, une recherche exhaustive par machine montre que toutes les suites de type Hadamard faible de longueur ≤ 23 sont supersymétriques.

Pour $s = (s_1, \dots, s_{2m-1})$ considérons la matrice

$$C'(s) = \begin{pmatrix} 0 & s_1 & s_2 & s_3 & \dots & s_{2m-2} & s_{2m-1} \\ -s_{2m-1} & 0 & s_1 & s_2 & \dots & s_{2m-3} & s_{2m-2} \\ -s_{2m-2} & -s_{2m-1} & 0 & s_1 & \dots & s_{2m-4} & s_{2m-3} \\ \vdots & \vdots & & \ddots & \vdots & \vdots & \\ -s_1 & -s_2 & -s_3 & -s_4 & \dots & -s_{2m-1} & 0 \end{pmatrix}$$

THÉORÈME 2.8. — *La matrice $C'(s)$ est une matrice de conférence si et seulement si s est une suite de type Hadamard faible.*

Preuve. — C'est un calcul facile laissé au lecteur.

3. Arithmétique

À une suite $s = (s_1, \ldots, s_{2m-1})$ de longueur $2m-1$ nous associons le polynôme

$$P(x) = P_s(x) = \sum_{k=1}^{2m-1} s_i x^i$$

de degré $2m-1$.

PROPOSITION 3.1. — *Soit $P(x) = P_s(x)$ le polynôme associé comme ci-dessus à la suite $s = (s_1, \ldots, s_{2m-1})$.*

Supposons qu'on ait l'égalité $\mathrm{Corr}_k(s) = \mathrm{Corr}_{2m-k}(s)$ pour $k = 1, \ldots, 2m-1$. Alors on a

$$P(\zeta)P(\zeta^{-1}) = P(\zeta)P(\overline{\zeta}) = \sum_{i=1}^{2m-1} s_i^2$$

pour tout $\zeta \in \mathbf{C}$ tel que $\zeta^{2m} + 1 = 0$.

Preuve. — On a

$$\begin{aligned} P(x)\big(x^{2m}P(\tfrac{1}{x})\big) &= \sum_i s_i x^i \quad \sum_j s_j x^{2m-j} \\ &= x^{2m}\Big(\sum_{i=1}^{2m-1} s_i^2 + \sum_{k=1}^{2m-2} \mathrm{Corr}_k(s)(x^k + x^{-k})\Big) \quad . \end{aligned}$$

L'égalité $\mathrm{Corr}_{2m-k}(s) = \mathrm{Corr}_k(s)$ entraîne donc

$$\begin{aligned} & \mathrm{Corr}_k(s)(x^k + x^{-k}) + \mathrm{Corr}_{2m-k}(s)(x^{2m-k} + x^{k-2m}) \\ = \quad & \mathrm{Corr}_k(s)\big(x^k(1 + x^{-2m}) + x^{-k}(1 + x^{2m})\big) \end{aligned}$$

ce qui montre que

$$\zeta^{2m}P(\zeta)P(\frac{1}{\zeta}) = \zeta^{2m}\sum_{i=1}^{2m-1} s_i^2$$

pour ζ racine du polynôme $x^{2m} + 1$. QED

La proposition 3.1 implique immédiatement le résultat suivant :

COROLLAIRE 3.2. — *Soit ζ une racine du polynôme $x^{2m} + 1$.*

Chaque suite $s = (s_1, \ldots, s_{2m-1})$ de type Hadamard fournit alors une factorisation

$$2m - 1 = \alpha\overline{\alpha}$$

avec $\alpha = P_s(\zeta) \in \mathbf{Z}[\zeta]$ un entier algébrique dans le corps cyclotomique $\mathbf{Q}[\zeta]$ (et $\overline{\alpha}$ le conjugué complexe de α).

Exemples 3.3.

(i) Si m est impair on peut prendre $\zeta = e^{i\pi/2} = i$ et on a alors

$$\alpha = \sum_{j=1}^{m-1}(-1)^j s_{2j} + i\sum_{j=0}^{m-1}(-1)^j s_{2j+1}\,.$$

Pour qu'une suite $s = (s_1,\ldots,s_{2m-1}) \in \{\pm 1\}^{2m-1}$ de type Hadamard avec m impair puisse exister il faut donc que $2m-1$ soit somme de deux carrés d'entiers. Ceci explique en particulier l'absence de suites de type Hadamard à valeurs ± 1 de longueur $2m-1$ pour $m = 11, 17, 29, 35, 39, 47, \ldots$.

(ii) Pour $m = 2m'$ avec m' impair on peut prendre $\zeta = e^{i\pi/4}$. L'existence d'une suite $s \in \{\pm 1\}^{4m'-1}$ de type Hadamard fournit

$$\alpha = (a_1(\zeta - \zeta^3) + a_2\zeta^2) \in \mathbf{Z}[\zeta]$$

avec

$$a_k = \sum_{j=0}^{m'-1}(-1)^j s_{4j+k} \quad \text{pour} \quad k = 1, 2$$

et l'égalité $\alpha\overline{\alpha} = 4m' - 1$ équivaut à

$$2a_1^2 + a_2^2 = 4m' - 1$$

(les entiers a_1, a_2 sont impairs et vérifient $-m' \le a_1, a_2 \le m'$).

(iii) Pour $m = 3m'$ avec m' impair on peut prendre $\zeta = e^{i\pi/6}$. L'existence d'une suite $s \in \{\pm 1\}^{6m'-1}$ de type Hadamard donne

$$\alpha = (a_0 + a_1(\zeta + \zeta^5) + a_2(\zeta^2 - \zeta^4) + a_3\zeta^3) \in \mathbf{Z}[\zeta]$$

avec

$$a_0 = \sum_{j=1}(-1)^j s_{6j} \quad \text{et}$$
$$a_k = \sum_{j=0}(-1)^j s_{6j+k} \quad \text{pour} \quad k = 1, 2, 3$$

et $\alpha\overline{\alpha} = 6m' - 1$ équivaut à

$$(a_0 + a_2)^2 + (a_1 + a_3)^2 = 6m' - 1$$

avec $(a_0, a_1, a_2, a_3, a_4, a_5) \in \mathbf{Z}^4$, a_0 pair et a_1, a_2, a_3 impair

De plus, on a également

$$(a_0 - 2a_2)^2 + (2a_1 - a_3)^2 = 6m' - 1$$

en considérant la racine $i = e^{i\pi/4}$ de $x^{6m'} + 1$ (cf 4.3 (i)).

(iv) Pour $m = 4m'$ avec m' impair on peut prendre $\zeta = e^{i\pi/8}$. L'existence d'une suite $s \in \{\pm 1\}^{4m'-1}$ de type Hadamard fournit

$$\alpha = (a_1(\zeta - \zeta^7) + a_2(\zeta^2 + \zeta^6) + a_3(\zeta^3 - \zeta^5) + a_4\zeta^4) \in \mathbf{Z}[\zeta]$$

avec

$$a_k = \sum_{j=0}^{m'-1} (-1)^j s_{8j+k} \quad \text{pour} \quad k = 1,2,3,4\,.$$

et on a $\alpha\overline{\alpha} = 8m' - 1 \Longleftrightarrow$

$$\begin{aligned} 2a_1^2 + 2a_2^2 + 2a_3^2 + a_4^2 &= 8m' - 1 \\ a_1^2 - a_3^2 + 2a_1a_3 + 2a_2a_4 &= 0 \end{aligned}$$

où $-m' \leq a_1, a_2, a_3, a_4 \leq m'$ sont des entiers impairs.

On peut également utiliser la proposition 3.1 autrement en se ramenant à l'étude des corps finis.

En effet, une suite $s = (s_1, \ldots, s_{2m-1})$ de type Hadamard fournit un polynôme $P(x) = P_s(x) \in \mathbf{Z}[x]$ de degré $2m-1$ tel que $(x^{2m}+1)$ divise le polynôme

$$P(x)\big(x^{2m}P(\frac{1}{x})\big) - (2m-1)x^{2m} \quad .$$

Soit p un diviseur premier de $2m-1$. On a donc

$$P(x)\big(x^{2m}P(\frac{1}{x})\big) = (x^{2m}+1)\tilde{q}(x) \in \mathbf{F}_p[x]$$

en réduisant les coefficients de tous les polynômes modulo p. Tout facteur irréductible dans $\mathbf{F}_p[x]$ de $(x^{2m}+1)$ divise donc soit $P(x)$ soit $x^{2m}P(\frac{1}{x})$.

Soit

$$x^{2m}+1 = \prod_{i=1}^{r} a_i(x)\overline{a}_i(x) \prod_{j=1}^{t} b_j(x)$$

la décomposition de $x^{2m}+1$ en facteurs irréductibles sur $\mathbf{F}_p[x]$ où les $a_i(x), \overline{a}_i(x)$ sont tels que $a_i(\xi) = 0 \Longleftrightarrow \overline{a}_i(\xi^{-1}) = 0$ et les $b_j(x)$ vérifient $b_j(\xi) = 0 \Longleftrightarrow b_j(\xi^{-1}) = 0$. On voit alors qu'il existe un sous-ensemble $I \subset \{1, \ldots, r\}$ tel que

$$P(x) = xq(x) \prod_{i\in I} a_i(x) \prod_{i\notin I} \overline{a}_i(x) \prod_{j=1}^{t} b_j(x) \in \mathbf{F}_p[x] \quad .$$

La proposition suivante décrit les factorisation de $x^{p+1}+1 \in \mathbf{F}_p[x]$ pour p un nombre premier.

PROPOSITION 3.4. — *Soit $p = 2m-1$ un nombre premier impair.*

(i) Si p est congru à 1 modulo 4 alors

$$x^{2m}+1 = (x-\alpha)(x+\alpha) \prod_{l=1}^{(p-1)/4} (x^2 + c_l x - 1)(x^2 - c_l x - 1) \in \mathbf{F}_p[x]$$

où $\alpha^2 = -1$, $1 \leq c_1 < c_2 < \ldots < c_{(p-1)/4} \leq (p-1)/2$ *(en identifiant les entiers avec les éléments correspondants dans* $\mathbf{F}_p$*) et les polynômes* $x^2 \pm c_l x - 1$ *sont irréductibles.*

(ii) Si p est congru à 3 modulo 4 alors

$$x^{2m} + 1 = \prod_{l=1}^{(p+1)/4} (x^2 + c_l x - 1)(x^2 - c_l x - 1) \in \mathbf{F}_p[x]$$

où $1 \leq c_1 < c_2 < \ldots < c_{(p+1)/4} \leq (p-1)/2$ *et les polynômes* $x^2 \pm c_l x - 1$ *sont irréductibles.*

Preuve. — On a

$$(x^{p^2-1} - 1) = (x^{p+1} + 1)(x^{(p-2)(p+1)} - x^{(p-3)(p+1)} + (x^{(p-4)(p+1)} - \ldots - 1)$$

ce qui montre que toute racine ζ de $x^{2m} + 1 = x^{p+1} + 1$ est également racine de $x^{p^2} - x$ et ζ appartient donc à l'extension de degré 2 de $\mathbf{F}_p$. Tous les facteurs irréductibles de $x^{2m} + 1$ sont donc au plus de degré 2. Pour $y \in \mathbf{F}_p \setminus \{0\}$ on a $y^{2m} + 1 = y^{p-1}y^2 + 1 = y^2 + 1$ ce qui démontre que les seules racines de $x^{2m} + 1$ qui sont dans le corps primaire $\mathbf{F}_p$ sont les deux racines de -1 si elles existent.

Soit maintenant ζ une racine d'un diviseur g monique irréductible de $x^{2m}+1$. Alors ζ^p est aussi racine de g et si g est de degré 2 on a

$$g = (x - \zeta)(x - \zeta^p) = x^2 - (\zeta + \zeta^p)x + \zeta\zeta^p = x^2 - (\zeta + \zeta^p)x - 1$$

car $\zeta\zeta^p = \zeta^{2m} = -1$ ce qui termine la preuve. QED

La factorisation de $x^{p+1} + 1 \in \mathbf{F}_p[x]$ est donc facile à trouver en utilisant le fait que $\{c_1, \ldots, c_{(p\mp1)/4}\} = \{1 \leq x < p/2 \mid x^2 + 4 \text{ n'est pas un carré dans } \mathbf{F}_p\}$.

On peut également montrer que si $2m - 1 = q = p^f$ est une puissance d'un nombre premier p, alors les facteurs irréductibles de $x^{2m} + 1 \in \mathbf{F}_p[x]$ sont au plus de degré $2f$.

Remarque 3.5. — Si la longueur $2m$ d'une suite de type Hadamard est de la forme $p + 1$ avec p congru à 1 modulo 4 on saît que $(x - \alpha)$ divise le polynôme $P_s(x) \in \mathbf{F}_p[x]$ pour α une des deux racines de $x^2 + 1$. On peut alors montrer assez facilement que dans ce cas $P(x)$ est même divisible par $(x - \alpha)^2$.

4. Codes cycliques et anticycliques

Un *code linéaire de dimension d et de longueur l* est un sous-espace vectoriel $C \subset$

$\mathbf{F}_p^l$ qui est de dimension d. Le *code dual* $C^\perp$ d'un code linéaire C est le code

$$C^\perp = \{(x_1, \ldots, x_l) \in \mathbf{F}_p^l \mid \sum_i x_i c_i = 0 \; \forall (c_1, \ldots, c_l) \in C\} \quad .$$

On dira que le code C est *isotrope* si $C \subset C^\perp$ et C est *autodual* si $C = C^\perp$.

Un *code cyclique* est un code dans $\mathbf{F}_p[x]/(x^l - 1)$ qui est aussi un idéal pour la structure d'anneau sur $\mathbf{F}_p[x]/(x^l - 1)$. Si la longueur l d'un code cyclique C n'est pas divisible par la caractéristique du corps fini $\mathbf{F}_p$ alors l'anneau $\mathbf{F}_p[x]/(x^l - 1)$ est principal et C est engendré (en tant qu'idéal) par un générateur $g(x) \in \mathbf{F}_p[x]$ qui divise $(x^l - 1)$.

Un code C de longueur l est donc cyclique si et seulement si il est invariant par permutations cycliques des coordonnées, ie. si on a $c = (c_0, c_1, \ldots, c_{l-1}) \in C \Longleftrightarrow (c_1, c_2, \ldots, c_{l-1}, c_0) \in C$.

On supposera dans la suite que l n'est jamais divisible par la caractéristique de $\mathbf{F}_p$.

DÉFINITION 4.1. — On dira qu'un code C de longueur l est *anticyclique* si on a $(c_1, c_2, \ldots, c_{l-1}, -c_0) \in C$ pour tout $c = (c_0, c_1, c_2, \ldots, c_{l-1}) \in C$.

PROPOSITION 4.2. — *Les codes anticycliques de longueur l (non-divisible par la caractéristique de $\mathbf{F}_p$) sur $\mathbf{F}_p$ sont en bijection avec les diviseurs de $x^l + 1 \in \mathbf{F}_p[x]$.*

Preuve. — L'application linéaire

$$c = (c_0, c_1, \ldots, c_{l-1}) \longrightarrow \psi(c) = (c_0, c_1, \ldots, c_{l-1}, -c_0, -c_1, \ldots, -c_{l-1})$$

envoie un code anticyclique de longueur l sur un code cyclique de longueur $2l$ et de même dimension.

Le code $\psi(C)$ est engendré (en tant qu'idéal de $\mathbf{F}_p[x]/(x^{2l} - 1)$) par un élément de la forme

$$g(x) = (x^l - 1)\tilde{g}(x)$$

avec $\tilde{g}(x)$ un diviseur de $x^l + 1$.

On vérifie facilement que ψ induit une bijection entre codes anticycliques de longueur l et codes cycliques de longueur $2l$ engendré par un élément comme ci-dessus.QED

On dira que le code anticyclique C est engendré par $\tilde{g}(x)$ si le code cyclique $\psi(C)$ est engendré par $(x^l - 1)\tilde{g}(x)$. Le diviseur $\tilde{g}(x)$ de $x^l + 1$ est le *générateur* du code anticyclique C.

La proposition suivante permet de construire des codes anticycliques isotropes.

PROPOSITION 4.3. — *Soit C un code anticyclique de longueur l engendré par $\tilde{g}(x) = \sum \gamma_i x^i \in \mathbf{F}_p[x]$ de degré d.*

Si $x^l + 1$ divise $\tilde{g}(x)x^d\tilde{g}(x^{-1})$ alors C est isotrope.

Preuve. — Une base du code C est donnée par les polynômes

$$\tilde{g}(x), x\tilde{g}(x), \ldots, x^{l-d-1}\tilde{g}(x)$$

et il suffit de montrer que $\langle \tilde{g}(x), x^k\tilde{g}(x)\rangle = 0$ pour $k = 0, \ldots, l-d-1$. Or $\langle \tilde{g}(x), x^k\tilde{g}(x)\rangle$ est le coefficient de degré $d+k$ (ou $d-k$) du polynôme

$$f(x) = \tilde{g}(x)x^d\tilde{g}(x^{-1}) = (x^l+1)r(x) = \sum_k \sum_i \gamma_{i+k}\gamma_i x^{k+d}$$

avec $r(x) \in \mathbf{F}_p[x]$ un polynôme de degré au plus $2d-l$.

Les coefficients de degré j avec $2d - l < j < l$ du polynôme $f(x)$ sont tous nuls. Ceci montre que $\langle \tilde{g}(x), x^k\tilde{g}(x)\rangle = 0$ pour $d - l < 0 \leq k < l - d$. QED

Cette proposition et sa preuve sont en fait des adaptations de résultats bien connus dans le cas des codes cycliques.

COROLLAIRE 4.4. — *Soit $s = (s_1, \ldots, s_{2m-1})$ une suite de type Hadamard à valeurs ± 1 et soit p un diviseur premier de $2m-1$. Alors le plus petit code anticyclique de longueur $2m$ qui contient l'élément $(0, s_1, \ldots, s_{2m-1})$ est isotrope.*

Preuve. — Ceci résulte de la fin de la section précédente et de la proposition précédente.

On peut également le montrer par un petit calcul direct ou le déduire du théorème 2.8.

Exemples 4.5. — Nous donnons ici les factorisations de $x^{2m}+1$ et de $\sum s_i x^i$ dans $\mathbf{F}_p$ pour toutes les suites de type Hadamard de longueurs ≤ 13 dont la table se trouve dans la section suivante.

Cette table ne contient pas vraiment toutes les suites mais les suites omises sont obtenues par des transformations très simples et les factorisations correspondantes se déduisent facilement de celles données ici.

Remarquons que ces factorisations permettent facilement de trouver le gérérateurs des codes anticycliques isotropes décrit par le corollaire 4.4. Une inspection montre que ces codes sont souvent autoduaux (voir la remarque 4.6 (iii) ci-dessous).

$m = 2, \quad p = 3:$

$$x^4 + 1 = (x^2 + x - 1)(x^2 - x - 1)$$

$$-x + x^2 + x^3 = x(x^2 + x - 1)$$

$m = 3, \quad p = 5:$

$$x^6 + 1 = (x + 2)(x + 3)(x^2 + 2x - 1)(x^2 - 2x - 1)$$

$$x - x^2 + x^3 + x^4 + x^5 = x(x + 2)^2(x^2 + 2x - 1)$$

$m = 4, \quad p = 7:$

$$x^8 + 1 = (x^2 + x - 1)(x^2 - x - 1)(x^2 + 3x - 1)(x^2 - 3x - 1)$$

$$-x - x^2 - x^3 + x^4 + x^5 - x^6 + x^7 = x(x^2 + x - 1)(x^2 + 3x - 1)(x - 3)(x - 2)$$
$$x + x^2 - x^3 + x^4 + x^5 + x^6 - x^7 = -x(x^2 + x - 1)^2(x^2 - 3x - 1)$$

$m = 5, \quad p = 3:$

$$x^{10} + 1 = (x^2 + 1)(x^4 + x^3 - x + 1)(x^4 - x^3 + x + 1)$$

$$-x - x^2 + x^3 - x^4 + x^5 + x^6 + x^7 + x^8 - x^9 = -x(x^2 + 1)^2(x^4 - x^3 + x + 1)$$

$m = 6, \quad p = 11:$

$$x^{12} + 1 = (x^2 + 2x - 1)(x^2 - 2x - 1)(x^2 + 3x - 1)(x^2 - 3x - 1)(x^2 + 5x - 1)(x^2 - 5x - 1)$$

$$\begin{aligned} x - x^2 + x^3 + x^4 - x^5 + x^6 + x^7 + x^8 - x^9 - x^{10} - x^{11} \\ = -x(x^2 + 3x - 1)(x^2 - 5x - 1)(x^2 - 2x - 1)(x + 4)(x - 5)(x - 3)(x - 2) \end{aligned}$$
$$\begin{aligned} x - x^2 + x^3 - x^4 - x^5 + x^6 + x^7 - x^8 - x^9 - x^{10} - x^{11} \\ = -x(x^2 + 2x - 1)(x^2 + 3x - 1)(x^2 + 5x - 1)(x^4 + 2x^3 - 3x^2 - 2x + 1) \end{aligned}$$

$m = 7, \quad p = 13:$

$$x^{14}+1=(x+5)(x-5)(x^2+x-1)(x^2-x-1)(x^2+2x-1)(x^2-2x-1)(x^2+4x-1)(x^2-4x-1)$$

$$\begin{aligned} x - x^2 + x^3 - x^4 - x^5 - x^5 + x^7 + x^8 - x^9 + x^{10} + x^{11} + x^{12} + x^{13} \\ = x(x - 5)^2(x^2 - x - 1)(x^2 - 2x - 1)(x^2 - 4x - 1)(x^2 + 2x + 8)(x^2 + 3x + 5) \end{aligned}$$
$$\begin{aligned} -x + x^2 + x^3 - x^4 + x^5 - x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} - x^{12} - x^{13} \\ = -x(x + 5)^2(x^2 + 2x - 1)(x^2 - 4x - 1)(x^2 - x - 1)^2(x + 2)(x + 6) \end{aligned}$$
$$\begin{aligned} -x + x^2 - x^3 + x^4 - x^5 - x^6 + x^7 + x^8 - x^9 - x^{10} - x^{11} - x^{12} - x^{13} \\ = -x(x - 5)^2(x^2 + x - 1)(x^2 + 2x - 1)(x^2 - 4x - 1)(x + 3)(x + 4)(x - 6)(x - 2) \end{aligned}$$

Remarque 4.6.

(i) Le code anticyclique associé à une suite de type Hadamard considéré ci-dessus est le code engendré (sur $\mathbf{F}_p$) par les vecteurs lignes de la matrice de conférence $C'(s)$ construite à la fin de la section 2.

Ce code est aussi isomorphe au code engendré par les vecteurs colonnes de $C'(s)$ (car $C'(s)$ est équivalent à une matrice de conférence symétrique ou antisymétrique).

(ii) Un autre code isotrope associé à une suite de type Hadamard est obtenu en considérant les vecteurs lignes de la matrice de conférence $C(s)$ considéré au début de la section 2.

(iii) Si le nombre premier p considéré est égal à la longueur $2m-1$ d'une suite de type Hadamard, alors le code anticyclique associé ainsi que le code défini par le point (ii) ci-dessus sont tous les deux autoduaux (car les réseaux entiers associés à ces codes sont alors $\mathbf{Z}^{p+1}$ qui est unimodulaire).

5. Tables

La liste suivante permet de construire toutes les suites de type Hadamard de longueur $2m-1 \leq 61$.

Les données sont organisées comme suit : Pour une valeur de m donnée la table indique d'abord le nombre total de telles suites de longueur $2m-1$. En cas d'absence de suite une raison simple est parfois donnée (par exemple pour m impair la longueur $2m-1$ doit être somme de deux carrés).

La table contient ensuite une liste incomplète de ces suites. La liste complète est obtenu en prenant chaque fois aussi les suites obtenus en changeant tous les signes, en changeant tous les signes d'indices impairs respectivement en changeant tous les signes d'indices pairs (la transformation (iii) de la proposition 2.4 n'a pas été utilisée pour raccourcir la liste dans le cas où m est pair).

Une suite est seulement représentée par les signes de ses coefficients. Ainsi $+\ -\ +\ +\ +$ représente par exemple la suite $(1,-1,1,1,1)$ de longueur 5 avec $m=3$.

Les listes ont été construites par un programme d'ordinateur assez simple qui a parcouru toutes les suites supersymétriques à valeurs ± 1 pour trouver celles qui sont de type Hadamard.

Les résultat obtenus semblent indiquer que de telles suites existent exactement pour toutes les longueurs $2m-1$ qui sont puissances d'un nombre premier ie. qui apparaissent comme cardinalité d'un corps fini.

$m = 1$: 2 suites :

$$+$$

$m = 2$: 4 suites :

$$-++$$

$m = 3$: 4 suites :

$$+-+++$$

$m = 4$: 8 suites :

$$---+-+$$
$$++-+++-$$

$m = 5$: 4 suites :

$$--+-++++-$$

$m = 6$: 8 suites :

$$+-++-+++---$$
$$+-+--++----$$

$m = 7$: 12 suites :

$$+-+---++-++++$$
$$-++-+-+++++--$$
$$-+-+--++-----$$

$m = 8$: 0 suites.

$m = 9$: 12 suites :

$$++-+-++-+++-----+$$
$$----+++-+++-+-+-$$
$$---+-----++-+---+-$$

$m = 10$: 16 suites :

$$-+-+++---+++-+++++$$
$$-++-+++++-+++-+--++$$
$$+-----+--++--+-+--$$
$$+-+++--+-+++++--+---$$

$m = 11$: 0 suites. 21 n'est pas somme de deux carrés.

$m = 12$: 16 suites :

− − + + − + − + − − − + + − + + + + + + − − +
− − + + + − + − + − − + + − − − − − − + − − +
+ + − + + − − + − + − + + + + + + − − + + + −
+ + + + − + + − − + − + + + + − − + + + − + −

$m = 13$: 8 suites :

+ + + + + − + − − + + − + + + − − + + + + − + − +
− − + − − + − − + − + − + + + + + + − − − + + + −
− − − + − − + − − − − − + + − + − + + + − − − + −

$m = 14$: 8 suites :

− + + + − − − − − + − − − + + − + + + − + − + + − + +
− + + − − − + + − + − + − + + + + + + + − − + − − + +

$m = 15$: 16 suites :

+ − − − + − + − + + − + − − + + − − − − + + + + + + − + +
+ − − − + + + − + − − − − − + + − + − + + + + − + + − + +
− + − − + − − + + + + + + − + + + − + − + − − + + + − − −
− + − − + + − + + − + − + − + + + + + + + − − − + + − − −

$m = 16$: 32 suites :

− − − + − + + − + − − − + − − + + − − − + − − − − + + + + − +
− − − − − − + + − + + − − + − + + + + − − + + + − − + − + − +
− − − − + + + − − + − + + + − + + + − + + + + − − + − − + − +
− − + + − + + + + + + + − − − + + − + + − + − + − + + + − − +
+ + − + − − + + − − − + − + − + + + + + + − + + − − + + + + −
+ + − − − + − + − − − − + − − + + − − − + − + + + + + − + + −
+ + + + + − + − − + − − + + − + + + − − + + + − − − − + − + −
+ + + − + − − − − − + + + − − + + − − + − − + − + − − − − + −

$m = 17$: 0 suites. 33 n'est pas une somme de deux carrés.

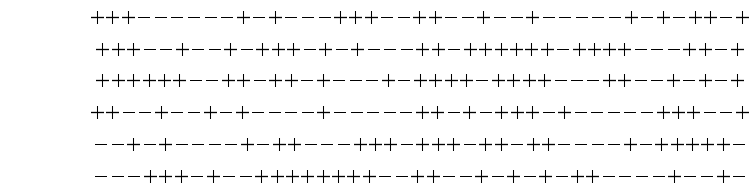
$m = 18$: 0 suites. 35 n'est pas de la forme $2a^2 + b^2$.

$m = 19$: 36 suites :

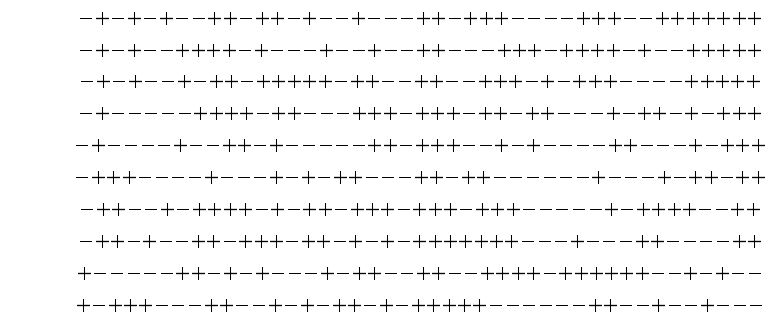
+−+−+++++−−−+−++−−++−−++++−++−+−+++++
+−+++−++−+++++−−+−++++−−+−+−−−+++−+++
+−−−+++−−+−+−+−−−−++−+−−−−−−−++−++−++
+−−−−−−−−++++−−+−−++−−−++−+−−+−+−+−++
+−−+−−−−+−+−−++++−+++−+−−+++++−+−−−++
−++−++−+−+−−+++++−+++−+−++−−−−−−+++−−
−++−−−−−+−−−−+−−+−++++−−−+−+++−+−++−−
−+−−−−+++−−++++++−+++−+−+−−++−++−+−−−
−+−+++−++−++−−−−−−++−+−+−−+++−−−+−−−−

$m = 20$: 0 suites. Pas de solutions aux équations 3.3 (iv).

$m = 21$: 24 suites :

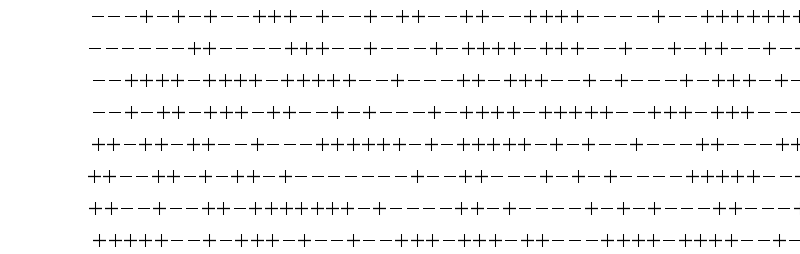


$m = 22$: 40 suites :

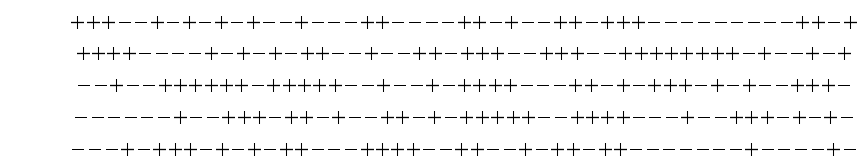


$m = 23$: 0 suites.

$m = 24$: 32 suites :

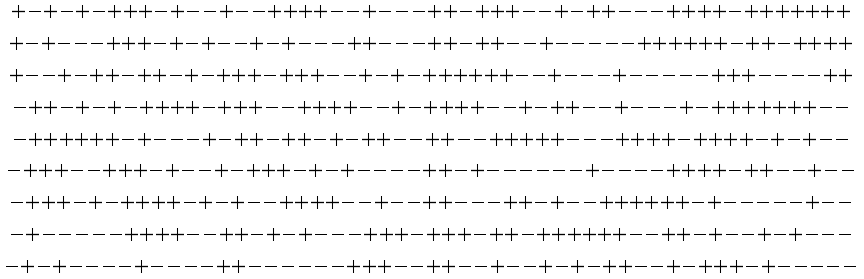


$m = 25$: 20 suites :



$m = 26$: 0 suites.

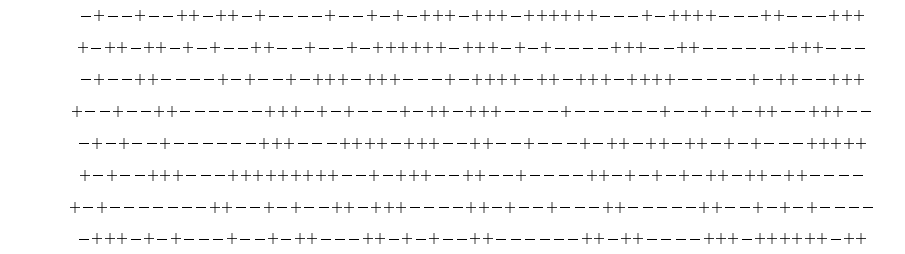
$m = 27$: 36 suites :



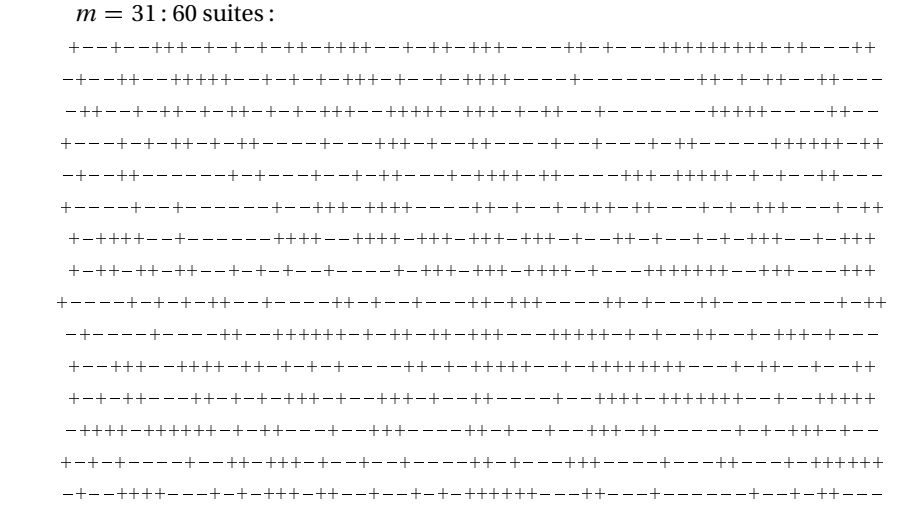
$m = 28$: 0 suites. Pas de solutions aux équations 3.3 (iv).

$m = 29$: 0 suites. 57 n'est pas somme de deux carrés.

$m = 30$: 32 suites :



$m = 31$: 60 suites :



Je remercie Pierre De la Harpe, Jacques Helmstetter et Boris Venkov pour leurs remarques et suggestions.

Références

[**vLW**] J.H. van Lint, R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press (1992).

Roland BACHER
Université de Grenoble I
Institut Fourier
UMR 5582 CNRS-UJF
38402 St. Martin d'Hères Cedex (France)

e-mail: Roland.Bacher@ujf-grenoble.fr