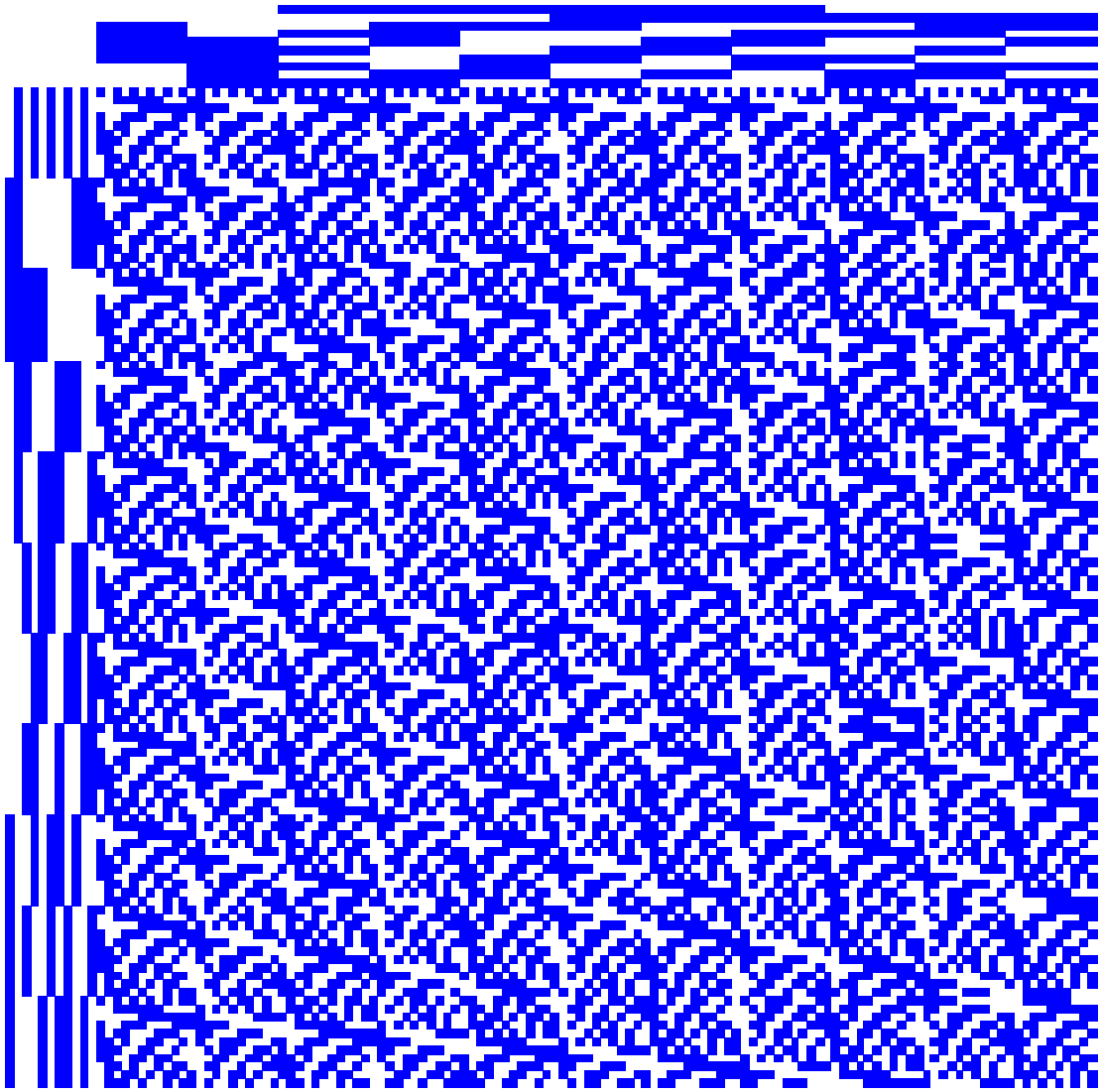
Jacques Cellier

Autour des Matrices de Hadamard



Hadamard 132

Préliminaires

Dans tout ce qui suit :

$\mathbb{R}^n$ désigne l'espace euclidien muni du produit scalaire usuel :

$$\text{pour } X, Y \in \mathbb{R}^n \quad \langle X ; Y \rangle = X^t Y = Y^t X$$

pour lequel la base canonique de $\mathbb{R}^n$ est orthonormale.

Pour $X \in \mathbb{R}^n$, $\|X\|$ désignera la norme euclidienne : $\|X\| = \sqrt{X^t X}$.

$\mathbb{C}^n$ désigne l'espace hermitien muni du produit scalaire hermitien usuel :

$$\text{pour } X, Y \in \mathbb{C}^n \quad \langle X ; Y \rangle = X^* Y$$

pour lequel la base canonique de $\mathbb{C}^n$ est orthonormale.

On rappelle que, contrairement au cas euclidien, les scalaires $\langle X ; Y \rangle$ et $\langle Y ; X \rangle$ ne sont pas égaux mais conjugués.

Pour $X \in \mathbb{C}^n$, $\|X\|$ désignera la norme euclidienne : $\|X\| = \sqrt{X^* X}$.

Les notations utilisées dans ce texte sont détaillées à la fin du document.

Sur le produit tensoriel (alias de Kronecker) de matrices

1. Définition

Soit K un corps commutatif, $A = (a_{i,j}) \in \mathcal{M}_{n,p}(K)$, $B = (b_{i,j}) \in \mathcal{M}_{n',p'}(K)$, le produit tensoriel (alias de Kronecker) est défini par :

$$A \otimes B = \left(\begin{array}{c|c|c} a_{1,1}B & \cdots & a_{1,p}B \\ \hline \vdots & & \vdots \\ \hline a_{n,1}B & \cdots & a_{n,p}B \end{array} \right) \in \mathcal{M}_{nn',pp'}(K)$$

Par la suite, nous aurons besoin des propriétés suivantes faciles à vérifier :

- ✓ Pour $\alpha \in K$: $(\alpha A) \otimes B = A \otimes (\alpha B) = \alpha (A \otimes B)$.
- ✓ $A \otimes (B + C) = A \otimes B + A \otimes C$ et $(A + B) \otimes C = A \otimes C + B \otimes C$.
- ✓ Si les tailles des matrices sont compatibles avec la multiplication usuelle :

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD) .$$

- ✓ $(A \otimes B)^t = A^t \otimes B^t$

Sur les corps finis

On rappelle que selon le théorème de Wederburn, tous les corps finis sont commutatifs. Pour $q = p^r$, p premier il existe un corps de caractéristique p ayant q élément noté F_q. On admettra les propriétés suivantes :

1. Pour q donné, F_q est unique à un isomorphisme près.
2. Les F_q sont les seuls corps finis.
3. Le groupe multiplicatif F_q^* est cyclique d'ordre $q-1$.

4. $F_q \simeq {\mathbb{Z}_p[X]}\big/{(P)}$ où $P \in \mathbb{Z}_p[X]$ est irréductible sur $\mathbb{Z}_p[X]$ de degré $r-1$. Il s'en suit que tout élément a de F_q peut s'écrire : $a = a_o + a_1 X + \cdots + a_{r-1} X^{r-1}$ où $a_i \in \mathbb{Z}_p$ et peut être représenté, en tant qu'élément de l'espace vectoriel $\left(\mathbb{Z}_p\right)^r$ par ses coordonnées $\begin{pmatrix} a_0 \\ \vdots \\ a_{r-1} \end{pmatrix}$.

Matrices de Hadamard

2. Définition

Une matrice de Hadamard de taille n *est une matrice notée* H_n *ou plus simplement* $H=\left(h_{i,j}\right)\in\mathcal{M}_n(\mathbb{R})$ *avec* $h_{i,j}=\pm 1$ *vérifiant une des conditions équivalentes suivantes :*

1. $H\,H^t=n\,I_n$.
2. $H^tH=n\,I_n$.
3. *Deux colonnes distinctes de H sont orthogonales.*
4. *Deux lignes distinctes de H sont orthogonales.*

L'équivalence de ces assertions résulte du fait qu'elles signifient toutes que la matrice $\frac{1}{\sqrt{n}}H$ est orthogonale.

Dans la suite les matrices de Hadamard seront notées H ou H_n.

Exemples :

Si on omet le cas trivial $H_1=(1)$, on a $H_2=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

Commentaire :

La propriété 3. équivaut au fait que entre deux colonnes distinctes j, j' on a autant d'accords ($h_{i,j}=h_{i,j'}$) que de désaccords ($h_{i,j}\neq h_{i,j'}$). La propriété 4. dit la même chose pour les lignes. Cela permet d'étendre la notion de matrice de Hadamard à toute situation binaire telle que : $h_{i,j}\in\{0,1\}$ ou $h_{i,j}\in\{\text{blanc},\text{bleu}\}$ (bien que dans ce dernier cas on n'obtienne pas une matrice à proprement parler). La figure de la couverture illustre ce dernier cas : armé d'une très bonne loupe et de beaucoup de patience, on peut le vérifier…

3. Propriétés immédiates :

Si H_n *est une matrice de Hadamard, alors :*

1. H_n^t *est une matrice de Hadamard.*
2. H_n *est inversible et* $H_n^{-1}=\frac{1}{n}H_n^t$.
3. *Si l'on permute les lignes (resp. colonnes) de* H_n *on obtient une matrice de Hadamard.*
4. *Si on multiplie par* -1 *une ligne (resp. colonne) de* H_n, *on obtient une matrice de Hadamard.*
5. $-H_n$ *est une matrice de Hadamard.*
6. $\left|Det\left(H_n\right)\right|=n^{\frac{n}{2}}$.

DEMONSTRATION :

1. Évident.

2. Évident.
3. Il suffit de le monter pour les transpositions. Si on transpose 2 lignes (resp . colonnes), la propriété d'orthogonalité 2 à 2 est bien évidemment conservée.
4. Si on multiplie une ligne (resp. colonne) par -1, la nouvelle ligne est colinéaire à l'ancienne et la propriété d'orthogonalité 2 à 2 est bien évidemment conservée.
5. Il suffit d'appliquer 4. à chaque ligne.
6. On a d'une part :

$$Det\left(H_n H_n^t\right) = Det\left(H_n\right) \times Det\left(H_n^t\right) = \left(Det\left(H_n\right)\right)^2,$$

de l'autre :

$$Det\left(H_n H_n^t\right) = Det\left(n\, I_n\right) = n^n$$

4. Corollaire

Partant d'une matrice de Hadamard H, on peut obtenir une matrice de Hadamard (dite de forme standard) dont la première ligne et la première colonne ne contiennent que des 1.

DEMONSTRATION :

1. Considérons la première ligne $H_{1,\bullet}$. D'après 3.4, on peut multiplier par -1 chaque colonne j telle que : $H_{1,j} = -1$.
2. On procède de façon analogue avec la première colonne $H_{\bullet,1}$.

Construction de Sylvester

5. Proposition : construction de Sylvester

Si H_m est une matrice de Hadamard de taille m, et H_n est une matrice de Hadamard de taille n alors : $H_m \otimes H_n$ est une matrice de Hadamard de taille mn.

En particulier si H_n est une matrice de Hadamard de taille n, alors :

$$H_{2n} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes H_n = \left(\begin{array}{c|c} H_n & H_n \\ \hline H_n & -H_n \end{array}\right)$$ *est une matrice de Hadamard de taille $2n$.*

Il existe des matrices de Hadamard de taille $2^k, k \in \mathbb{N}$.

DEMONSTRATION :

$(H_m \otimes H_n)(H_m \otimes H_n)^t = (H_m \otimes H_n)(H_m^t \otimes H_n^t) = (H_m H_m^t) \otimes (H_n H_n^t) = mI_m \otimes nI_n = mn\, I_m \otimes I_n$.

Or $I_m \otimes I_n$ est la matrice constituée de m fois la matrice I_n répétée le long de la diagonale et est donc égale à I_{mn}.

La deuxième assertion est l'application de la première avec $H_m = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Et la dernière assertion en découle immédiatement.

Application :

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Et H_{16} en couleur :

H_{16}																
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1
1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1
1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1
1	1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1
1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1
1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	1	-1
1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1
1	-1	1	-1	1	-1	1	-1	-1	1	-1	1	-1	1	-1	1
1	1	-1	-1	1	1	-1	-1	-1	-1	1	1	-1	-1	1	1
1	-1	-1	1	1	-1	-1	1	-1	1	1	-1	-1	1	1	-1
1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1	1	1	1
1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	1	-1	1	-1
1	1	-1	-1	-1	-1	1	1	-1	-1	1	1	1	1	-1	-1
1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	1	-1	-1	1

Existe-t-il des matrices de Hadamard de taille autre que $2^k, k \in \mathbb{N}$? La réponse viendra plus tard. Mais on peut d'ores et déjà limiter les tailles possibles pour ces matrices :

6. Proposition

La taille d'une matrice d'Hadamard est 1, 2 ou un multiple de 4.

DEMONSTRATION :

Pour $n \in 1 \cdots 2$, c'est déjà réglé.

Soit H une matrice de Hadamard de taille $n > 2$. On peut toujours mettre la matrice sous forme standard avec $H_{1,\bullet} = (1,1,\cdots,1)$. Pour respecter l'orthogonalité des lignes, la deuxième ligne $H_{2,\bullet}$ de la matrice doit comporter autant de 1 que de -1, ce qui implique la parité de n.

Le même argument s'applique pour prouver que la troisième ligne $H_{3,\bullet}$ comporte autant de 1 que de -1.

Soit :

- ✓ a le nombre d'indices j tel que : $h_{2,j} = 1$ et $h_{3,j} = 1$
- ✓ b le nombre d'indices j tel que : $h_{2,j} = 1$ et $h_{3,j} = -1$
- ✓ c le nombre d'indices j tel que : $h_{2,j} = -1$ et $h_{3,j} = 1$
- ✓ d le nombre d'indices j tel que : $h_{2,j} = -1$ et $h_{3,j} = -1$

$\langle H_{2,\bullet}; H_{3,\bullet} \rangle = a \times 1 + b \times (-1) + c \times (-1) + d \times 1$. L'orthogonalité de $H_{2,\bullet}$ et $H_{3,\bullet}$ implique :

$$a + d = b + c \quad (1).$$

L'égalité du nombre de 1 et de -1 dans $H_{2,\bullet}$ et dans $H_{3,\bullet}$ permet d'écrire :

$$a + b = c + d \quad (2)$$

$$a + c = b + d \quad (3)$$

$(1) - (2) \Rightarrow d - b = b - d \Rightarrow b = d$

$(1) - (3) \Rightarrow d - c = c - d \Rightarrow c = d$

Et finalement : $a = b = c = d$ et $n = a + b + c + d = 4a$.

Hadamard a conjecturé l'existence de matrices de Hadamard de taille $n = 4a$ pour tout $a \in \mathbb{N}*$. Mais la question reste ouverte.

Matrices de Hadamard-Walsh

Notation :

Pour une matrice $M \in \mathcal{M}_n(\mathbb{R})$, on notera α_M l'application $1\cdots n \xrightarrow{\alpha_M} 0\cdots n-1$ définie par :

$\alpha_M(i) =$ nombre de changement de signe sur la ligne i de M.

On définit de même une application β_M pour les colonnes.

7. Définition

On appelle matrice de Hadamard-Walsh une matrice de Hadamard obtenue par la construction de Sylvester à partir de H_2.

Exemples :

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Par construction, il va de soi que ces matrices sont symétriques et de forme standard et que n est une puissance de 2. Voici deux propriétés moins immédiates :

8. Proposition

Pour une matrice de Hadamard-Walsh H_n les applications α_{H_n} et β_{H_n} sont bijectives.

DEMONSTRATION :

L'énoncé est vérifié pour H_2 et H_4, on va montrer : α_{H_n} bijective $\Rightarrow \alpha_{H_{2n}}$ bijective.

$$H_{2n} = \left(\begin{array}{c|c} H_n & H_n \\ \hline H_n & -H_n \end{array}\right)$$

Considérons pour $i \in 1\cdots n$ les lignes i et $i+n$ de H_{2n}

$$\begin{aligned} i &\to x_1 \cdots x_n \quad x_1 \cdots \quad x_n \\ i+n &\to x_1 \cdots x_n \; -x_1 \cdots -x_n \end{aligned}$$

Pour une matrice de Hadamard-Walsh, on a toujours $x_1 = 1$

Si $x_n = 1$ (ce qui a lieu une ligne sur 2) :

- ✓ le nombre de changement de signe de la ligne i de H_{2n} est : $\alpha_{H_{2n}}(i) = 2\alpha_{H_n}(i)$
- ✓ le nombre de changement de signe de la ligne $i+n$ de H_{2n} est : $\alpha_{H_{2n}}(i+n) = 2\alpha_{H_n}(i)+1$

Si $x_n = -1$:

- ✓ le nombre de changement de signe de la ligne i de H_{2n} est : $\alpha_{H_{2n}}(i) = 2\alpha_{H_n}(i)+1$
- ✓ le nombre de changement de signe de la ligne $i+n$ de H_{2n} est : $\alpha_{H_{2n}}(i+n) = 2\alpha_{H_n}(i)$

Dans tous les cas $\alpha_{H_{2n}}(\{i, i+n\}) = \{2\alpha_{H_n}(i), 2\alpha_{H_n}(i)+1\}$.

Lorsque i va parcourir $1\cdots n$, $\alpha_{H_n}(i)$ prendra toutes les valeurs de $0\cdots n-1$ et $\alpha_{H_{2n}}(\{i, i+n\})$ toutes les valeurs de $0\cdots 2n-1$.

Plus formellement les $\{i, i+n\}$, $i \in 1\cdots n$ forment une partition de $1\cdots 2n$ et l'on a :

$$\alpha_{H_{2n}}(1\cdots 2n)=\alpha_{H_{2n}}\left(\bigcup_{i=1}^{n}\{i,i+n\}\right)=\bigcup_{i=1}^{n}\alpha_{H_{2n}}\left(\{i,i+n\}\right)=\bigcup_{i=1}^{n}\left\{2\alpha_{H_n}(i),2\alpha_{H_n}(i)+1\right\}$$

Et en posant $\alpha_{H_n}(i)=k$: $\alpha_{H_{2n}}(1\cdots 2n)=\bigcup_{k=0}^{n-1}\{2k,2k+1\}=0\cdots 2n-1$. Donc $\alpha_{H_{2n}}$ est surjective, donc bijective puisqu'il s'agit d'une application entre deux ensembles finis de même cardinal.

Par symétrie, $\beta_{H_{2n}}(j)=\alpha_{H_{2n}}(j)$.

Exemple :

H_{16}																α
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	15
1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	7
1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	8
1	1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	3
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	12
1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1	4
1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	1	-1	11
1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1
1	-1	1	-1	1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	14
1	1	-1	-1	1	1	-1	-1	-1	-1	1	1	-1	-1	1	1	6
1	-1	-1	1	1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	9
1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1	1	1	1	2
1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	1	-1	1	-1	13
1	1	-1	-1	-1	-1	1	1	-1	-1	1	1	1	1	-1	-1	5
1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	1	-1	-1	1	10
β	0	15	7	8	3	12	4	11	1	14	6	9	2	13	5	10

Et rien n'interdit de réordonner les lignes selon le nombre de changement de signe :

H_{16}																α
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1
1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	1	1	1	1	2
1	1	1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	3
1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	-1	-1	1	1	4
1	1	-1	-1	-1	-1	1	1	-1	-1	1	1	1	1	-1	-1	5
1	1	-1	-1	1	1	-1	-1	-1	-1	1	1	-1	-1	1	1	6
1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	7
1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	1	-1	-1	1	8
1	-1	-1	1	1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	9
1	-1	-1	1	-1	1	1	-1	-1	1	1	-1	1	-1	-1	1	10
1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	1	-1	11
1	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1	-1	1	12
1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	1	-1	1	-1	13
1	-1	1	-1	1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	14
1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	15
β	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

De fait, les colonnes se trouvent elles aussi réordonner. Cela reste à prouver…

✋ La propriété α_M bijective n'est pas vérifiée pour des matrices de Hadamard construites par d'autres procédés que Sylvester. Ainsi la matrice H_{12} obtenue par la méthode de Gilman exposée en aval :

	H_{12}												α
	1	1	1	1	1	1	1	1	1	1	1	1	0
	1	-1	1	-1	1	1	1	-1	-1	-1	1	-1	7
	1	-1	-1	1	-1	1	1	1	-1	-1	-1	1	6
	1	1	-1	-1	1	-1	1	1	1	-1	-1	-1	5
	1	-1	1	-1	-1	1	-1	1	1	1	-1	-1	7
	1	-1	-1	1	-1	-1	1	-1	1	1	1	-1	7
	1	-1	-1	-1	1	-1	-1	1	-1	1	1	1	6
	1	1	-1	-1	-1	1	-1	-1	1	-1	1	1	6
	1	1	1	-1	-1	-1	1	-1	-1	1	-1	1	6
	1	1	1	1	-1	-1	-1	1	-1	-1	1	-1	5
	1	-1	1	1	1	-1	-1	-1	1	-1	-1	1	6
	1	1	-1	1	1	1	-1	-1	-1	1	-1	-1	5
β	0	6	5	6	6	6	5	7	7	6	5	7	

Notation :

Pour $a, b \in \mathbb{N}$, on notera :

- ✓ $\underline{a} = a_{k-1} \cdots a_1 a_0, \underline{b} = b_{k-1} \cdots b_1 b_0, \ a_i \ b_i \in \{0,1\}$ leur écriture binaire.
- ✓ $\langle a \, ; b \rangle = \sum_{i=0}^{k-1} a_i b_i$

9. *Proposition*

Pour une matrice de Hadamard-Walsh H_n, le terme situé ligne i colonne j est :

$$h_{i,\,j} = (-1)^{\langle i-1\,;\,j-1 \rangle}.$$

DEMONSTRATION :

Pour simplifier les écritures on supposera les lignes et colonnes numérotées à partir de 0. La formule à démontrer s'écrit alors : $h_{i,\,j} = (-1)^{\langle i\,;\,j \rangle}$.

La formule étant manifestement vérifiée pour $n = 2$, on va montrer :

$$\text{vrai pour } n = 2^k \ \Rightarrow \text{ vrai pour } 2n = 2^{k+1}.$$

$$H_{2n} = \left(\begin{array}{c|c} H_n & H_n \\ \hline H_n & -H_n \end{array} \right)$$

1. Pour le bloc Nord-Ouest, c'est directement l'hypothèse de récurrence.

2. Pour le bloc Sud-Ouest, le terme $h_{i+n,\,j}$, $0 \le i < n, 0 \le j < n$ est égal à $h_{i,\,j}$ lequel, selon l'hypothèse de récurrence, est égal à $h_{i,\,j} = (-1)^{\langle i\,;\,j\rangle}$. Si $\underline{j} = j_{k-1}\cdots j_0$, $\underline{i} = i_{k-1}\cdots i_0$, on a : $\underline{i+n} = 1 i_{k-1}\cdots i_0$. D'où : $\langle i+n\,;\,j\rangle = \langle i\,;\,j\rangle$ et $h_{i+n,\,j} = (-1)^{\langle i+n;\,j\rangle}$.
3. Pour le bloc Nord-Est, par symétrie et en tenant compte de $\langle a\,;b\rangle = \langle b\,;a\rangle$ on aboutit à la même conclusion.

Pour le bloc Sud-Est, le terme $h_{i+n,\,n+j}$, $0 \le i < n, 0 \le j < n$ est égal à $-h_{i,\,j}$. Si $\underline{j} = j_{k-1}\cdots j_0$, $\underline{i} = i_{k-1}\cdots i_0$, on a : $\underline{i+n} = 1 i_{k-1}\cdots i_0$ et $\underline{j+n} = 1 j_{k-1}\cdots j_0$. D'où : $\langle i+n\,;\,j+n\rangle = 1 + \langle i\,;\,j\rangle$. Et finalement $h_{i+n,\,n+j} = -h_{i,\,j} = -(-1)^{\langle i\,;\,j\rangle} = (-1)^{\langle i\,;\,j\rangle+1} = (-1)^{\langle i+n\,;\,j+n\rangle}$.

Déterminant d'une matrice de Hadamard

On a déjà vu que $\left|Det\left(H_n\right)\right| = n^{\frac{n}{2}}$. On va montrer que cette propriété est caractéristique des matrices de Hadamard.

10. Proposition

Soit $A = \left(a_{i,\,j}\right) \in \mathcal{M}_n(\mathbb{R})$, *alors :*

$$\left|Det(A)\right| \le \left\|A_{\bullet,1}\right\| \times \left\|A_{\bullet,2}\right\| \times \cdots \left\|A_{\bullet,n}\right\|$$

où $\|\ \|$ *désigne la norme euclidienne.*

L'égalité ayant lieu si et seulement si les colonnes de la matrice A sont orthogonales 2 à 2.

DEMONSTRATION :

Si les vecteurs colonnes de la matrice A sont liés, $Det(A) = 0$ et l'inégalité est vérifiée.

Sinon $\left(A_{\bullet,1}, A_{\bullet,2}, \cdots, A_{\bullet,n}\right)$ est une base de $\mathbb{R}^n$. Alors le procédé d'orthogonalisation de Gram-Schmidt fournit une base : $\left(B_1, B_2, \cdots, B_n\right)$ orthonormale de $\mathbb{R}^n$ telle que pour $j \in 1\cdots n$:

$$Vec\left(A_{\bullet,1}, \cdots, A_{\bullet,\,j}\right) = Vec\left(B_1, \cdots, B_j\right)$$
$$\text{Et } \forall j \in 1\cdots n : \left\|B_j\right\| = 1$$

Il en résulte que dans la base $\left(B_1, B_2, \cdots, B_n\right)$, la matrice A' semblable à A est triangulaire supérieure. On a alors :

- ✓ $Det(A) = Det(A') = a'_{1,1} \times \cdots \times a'_{n,n}$
- ✓ $a'_{j,\,j} = \left\langle A_{\bullet,\,j}\,;\,B_j\right\rangle$

Par ailleurs on sait que (Cauchy-Schwarz) :

1. $\left|a'_{j,\,j}\right| = \left|\left\langle A_{\bullet,\,j}\,;\,B_j\right\rangle\right| \le \left\|A_{\bullet,\,j}\right\| \times \left\|B_j\right\| = \left\|A_{\bullet,\,j}\right\|$
2. Et que l'égalité a lieu si et seulement si les vecteurs $A_{\bullet,\,j}$ et B_j sont colinéaires.

Il en résulte que :

$\left|Det(A)\right| \le \left\|A_{\bullet,1}\right\| \times \left\|A_{\bullet,2}\right\| \times \cdots \left\|A_{\bullet,n}\right\|$

L'égalité a lieu si et seulement si, pour tout $j \in 1\cdots n$ $A_{\bullet,\,j}$ et B_j sont colinéaires. Mais comme $\left(B_1, B_2, \cdots, B_n\right)$ est une base orthonormale, $\left(A_{\bullet,1}, A_{\bullet,2}, \cdots, A_{\bullet,n}\right)$ est une base orthogonale.

Remarque :

On peut donner une interprétation géométrique de ce dernier résultat dans un espace de dimension 3 où le déterminant de 3 vecteurs peut être interprété (au signe près) comme le volume du parallélépipède défini par ces 3 vecteurs. Si la norme de ces vecteurs est fixée, le volume maximal est obtenu lorsque les vecteurs sont orthogonaux 2 à 2.

11. Corollaire

Soit $A=\left(a_{i,j}\right)\in\mathcal{M}_n\left(\mathbb{R}\right)$, *où* $a_{i,j}=\pm 1$, *alors A est une matrice de Hadamard si et seulement si* $\left|Det\left(H_n\right)\right|=n^{\frac{n}{2}}$.

DEMONSTRATION :

Il suffit d'appliquer la proposition précédente en sachant que $\left\|A_{\bullet,j}\right\|=\sqrt{n}$.

Constructions de Gilman et Paley

Symbole de Legendre

12. Définition

Soit p premier impair, on appelle symbole de Legendre l'application notée χ_p ou plus simplement χ du corps de $\mathbb{Z}_p$ dans lui-même définie par $\chi_p(x)=x^{\frac{p-1}{2}}$.

Remarques :

Le symbole de Legendre se note aussi $\left(\frac{x}{p}\right)$.

Le symbole de Legendre, ou plus exactement sa restriction à $\mathbb{Z}_p^*$, est aussi appelé caractère quadratique.

Si $x\in\mathbb{Z}$, et $\bar{x}$ est sa projection dans $\mathbb{Z}_p$ on notera, par un (léger) abus de langage $\chi(x)$ pour $\chi(\bar{x})$.

13. Lemme

Dans $\mathbb{Z}_p^*$, il existe $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés.

DEMONSTRATION :

L'application $\mathbb{Z}_p^* \xrightarrow{c} \mathbb{Z}_p^* \quad x\mapsto x^2$ est un morphisme de groupe de noyau $\{1,-1\}$ et d'image les carrés de $\mathbb{Z}_p^*$. On a donc $\mathbb{Z}_p^*/\{1,-1\} \simeq \mathrm{Im}(c)$. Il en résulte que dans $\mathbb{Z}_p^*$ le nombre des carrés de est égal au nombre de non-carrés, donc à $\frac{p-1}{2}$.

14. Proposition

χ vérifie les propriétés suivantes :

1. $\mathrm{Im}(\chi)=\{-1,0,1\}$.
2. *La restriction de χ au groupe multiplicatif $\mathbb{Z}_p^*$ est un morphisme de groupe.*
3. $\chi(x)=\begin{cases}0 \text{ si } x=0\\ 1 \text{ si } x\neq 0 \text{ est un carré}\\ -1 \text{ si } x\neq 0 \text{ n'est pas un carré}\end{cases}$
4. $\sum_{x\in\mathbb{Z}_p}\chi(x)=0$

DEMONSTRATION :

1. Si $x=0$, $\chi(x)=0$. Sinon $(\mathbb{Z}_p^*,\times)$ est groupe cyclique d'ordre $p-1$. Pour tout $x\in\mathbb{Z}_p^*$ on a : $x^{p-1}=1$. D'où : $\chi(x)^2=x^{p-1}=1$ et $\chi(x)=\pm 1$.
2. Si $x,y\in\mathbb{Z}_p^*$, $\chi(xy)=(xy)^{\frac{p-1}{2}}=(x)^{\frac{p-1}{2}}(y)^{\frac{p-1}{2}}=\chi(x)\chi(y)$

3. . Si $x=y^2\neq 0$, $\chi(x)=\chi\left(y^2\right)=(x)^{\frac{p-1}{2}}(y)^{\frac{p-1}{2}}=\left(\chi(y)\right)^2=\left((y)^{\frac{p-1}{2}}\right)^2=y^{p-1}=1$. Comme l'équation $(x)^{\frac{p-1}{2}}=1$ a au plus $\frac{p-1}{2}$ solutions, on peut conclure que, pour $x\neq 0$, $\chi(x)=1$ si et seulement si x est un carré.
4. C'est une conséquence due l'égalité entre le nombre des carrés de est égal au nombre de non-carrés.

Exemple dans $\mathbb{Z}_{11}^*$ *:*

x	1	2	3	4	5	6	7	8	9	10
	$=1^2$		$=5^2$	$=2^2$	$=4^2$				$=3^2$	
$\chi(x)$	1	-1	1	1	1	-1	-1	-1	1	-1

Remarque :

Comme $\mathrm{Im}(\chi)=\{-1,0,1\}$, on peut identifier ces trois éléments aux éléments correspondants de $\mathbb{Z}$

Matrice de Jacobsthal

15. Définition

Pour p premier impair, on appelle matrice de Jacobsthal de taille p la matrice notée A_p *ou plus simplement A définie par :* $A=\left(a_{i,j}\right)\in\mathcal{M}_p(\mathbb{R})$ *où* $a_{i,j}=\chi(i-j)$

Exemples calculés par Maple avec $p=3$ *et* $p=5$

$$A3:=\begin{bmatrix}0&-1&1\\1&0&-1\\-1&1&0\end{bmatrix}\quad A5:=\begin{bmatrix}0&1&-1&-1&1\\1&0&1&-1&-1\\-1&1&0&1&-1\\-1&-1&1&0&1\\1&-1&-1&1&0\end{bmatrix}$$

16. Propriétés immédiates

$A=\left(a_{i,j}\right)\in\mathcal{M}_p(\mathbb{R})$ *matrice de Jacobsthal de taille p vérifie :*

1. $a_{i,j}\in\{-1,0,1\}$ *et* $a_{i,j}=0\Leftrightarrow i=j$.
2. $AU_p=\begin{pmatrix}0\\\vdots\\0\end{pmatrix}$ *et* $U_p^t A^t=\left(AU_p\right)^t=(0\quad\cdots\quad 0)$
3. *La matrice A est circulante.*
4. *La matrice A est symétrique si* $\frac{p-1}{2}$ *est pair, antisymétrique si* $\frac{p-1}{2}$ *est impair.*

DEMONSTRATION :

1. Évident compte tenu des propriétés de χ.
2. Soit la ligne $A_{i,\bullet}=\left(\chi(i-1),\chi(i-2),\cdots,\chi(i-p)\right)$. Or $\{i-1,i-2,\cdots,i-p\}=\mathbb{Z}_p$. On a donc sur la ligne $\frac{p-1}{2}$ 1 et $\frac{p-1}{2}$ -1.

3. Il suffit d'observer le petit schéma suivant en se souvenant que $i-p=i$ dans $\mathbb{Z}_p$:

	1	2	…	j	$j+1$	…	p
$A_{i,\bullet}$	$\chi(i-1)$	$\chi(i-2)$	…	$\chi(i-j)$	$\chi(i-j-1)$	…	$\chi(i-p)$
$A_{i+1,\bullet}$	$\chi(i)$	$\chi(i-1)$	…	$\chi(i+1-j)$	$\chi(i-j)$	…	$\chi(i+1-p)$

4. $\chi(-x)=(-x)^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}(x)^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}\chi(x)$

17. Lemme

$$\sum_{x\in\mathbb{Z}_p}\chi(x)\chi(x+d)=\begin{cases}p-1 \text{ si } d=0\\ -1 \text{ si } d\neq 0\end{cases}$$

DEMONSTRATION :

Dans le premier cas : $\sum_{x\in\mathbb{Z}_p}\chi(x)\chi(x+d)=\sum_{x\in\mathbb{Z}_p}\left(\chi(x)\right)^2=0+\sum_{x\in\mathbb{Z}_p^*}1=p-1$.

Dans le deuxième cas :

$$\sum_{x\in\mathbb{Z}_p}\chi(x)\chi(x+d)=\sum_{\substack{x\in\mathbb{Z}_p\\ x\notin\{0,-d\}}}\chi(x)\chi(x+d)=\sum_{\substack{x\in\mathbb{Z}_p\\ x\notin\{0,-d\}}}\chi\left(x^2+xd\right)=\sum_{\substack{x\in\mathbb{Z}_p\\ x\notin\{0,-d\}}}\underbrace{\chi\left(x^2\right)}_{=1}\chi\left(1+x^{-1}d\right)=\sum_{\substack{x\in\mathbb{Z}_p\\ x\notin\{0,-d\}}}\chi\left(1+x^{-1}d\right).$$

L'application $\mathbb{Z}_p\longrightarrow\mathbb{Z}_p$ définie par $x\mapsto 1+x^{-1}d$ est injective :

$1+x^{-1}d=1+y^{-1}d\Rightarrow x=y$ puisque $d\neq 0$.

Et bijective puisque $\mathbb{Z}_p$ fini. Lorsque x va parcourir $\mathbb{Z}_p-\{0,-d\}$, $t=1+x^{-1}d$ va parcourir $\mathbb{Z}_p-\{1,0\}$.

Au final : $\sum_{\substack{x\in\mathbb{Z}_p\\ x\notin\{0,-d\}}}\chi\left(1+x^{-1}d\right)=\sum_{t\in\mathbb{Z}_p-\{0,1\}}\chi(t)=\underbrace{\sum_{y\in\mathbb{Z}_p}\chi(t)}_{=0}-\underbrace{\chi(0)}_{=0}-\underbrace{\chi(1)}_{=1}=-1$.

18. Proposition

$A=\left(a_{i,j}\right)\in\mathcal{M}_p(\mathbb{R})$ matrice de Jacobsthal de taille p vérifie :

$$AA^t=pI_p-U_pU_p^t=\begin{pmatrix}p-1 & -1 & \cdots & -1\\ -1 & p-1 & \ddots & \vdots\\ \vdots & \ddots & \ddots & -1\\ -1 & \cdots & -1 & p-1\end{pmatrix}$$

DEMONSTRATION :

Pour $l,k\in 1\cdots p$, le coefficient de la matrice AA^t situé ligne l, colonne k est :

$$\left(AA^t\right)_{l,k}=A_{l,\bullet}A^t_{k,\bullet}=\sum_{j=1}^{p}a_{l,j}a_{k,j}=\sum_{j=1}^{p}\chi(l-j)\chi(k-j)$$

1° cas : $l=k$

$$\left(AA^t\right)_{l,l}=\sum_{j=1}^{p}\left(\chi(l-j)\right)^2=\sum_{\substack{j=1\\ j\neq l}}^{p}1=p-1$$

2° cas : $l\neq k$

Lorsque j parcourt $1\cdots p$, $\overline{l-j}$ et $\overline{k-j}$ parcourent $\mathbb{Z}_p$ avec un décalage $\overline{d}=\overline{l-k}\neq 0$. On peut donc écrire :

$\left(AA^t\right)_{l,k} = \sum_{x\in\mathbb{Z}_p} \chi(x)\chi(x+d) = -1$ selon le lemme précédent.

Exemple avec Maple et $p=11$ *:*

```
> A11:=matrix(11,11,(i,j)->legendre(i-j,11));
```

$$A11 := \begin{bmatrix} 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}$$

```
> multiply(A11,transpose(A11));
```

$$\begin{bmatrix} 10 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 10 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 10 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 10 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & 10 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & 10 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & 10 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 10 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 10 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 10 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 10 \end{bmatrix}$$

19. Définition

Pour p premier impair, on appelle matrice de Paley de taille $p+1$ *la matrice notée* P_{p+1} *ou plus simplement P définie par :*

$$P = \left(\begin{array}{c|c} 0 & U_p^t \\ \hline \chi_p(-1)U_p & A \end{array}\right)$$

Remarques :

1. Comme les coefficients de A appartiennent à $\{-1,0,1\}$, il en est de même pour ceux de P.
2. $\chi_p(-1) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } \dfrac{p-1}{2} \text{ est pair} \\ -1 \text{ si } \dfrac{p-1}{2} \text{ est impair} \end{cases}$
3. Il en résulte que, à l'instar de A_p ; la matrice P_{p+1} est symétrique si $\dfrac{p-1}{2}$ est pair, antisymétrique si $\dfrac{p-1}{2}$ est impair.

20. Proposition

La matrice de Paley P_{p+1} de taille $p+1$ vérifie :

$$P_{p+1}\,P_{p+1}^t = p\,I_{p+1}$$

DEMONSTRATION :

$$P\,P^t = \left(\begin{array}{c|c} 0 & U_p^t \\ \hline \chi(-1)U_p & A \end{array}\right)\left(\begin{array}{c|c} 0 & \chi(-1)U_p^t \\ \hline U_p & A^t \end{array}\right) = \left(\begin{array}{c|c} U_p^t U_p & U_p^t A^t \\ \hline AU_p & \left(\chi(-1)\right)^2 U_p U_p^t + A\,A^t \end{array}\right) = \left(\begin{array}{c|c} U_p^t U_p & U_p^t A^t \\ \hline AU_p & U_p U_p^t + A\,A^t \end{array}\right).$$

Or :

- ✓ $U_p^t U_p = \sum_{i=1}^{p} 1 = p$.
- ✓ D'après les propriétés immédiates de A : $AU_p = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ et $U_p^t\,A^t = \left(AU_p\right)^t = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}$.
- ✓ D'après la proposition 18 : $A\,A^t = pI_p - U_p U_p^t$.

Au final : $PP^t = \left(\begin{array}{c|c} p & 0 \\ \hline 0 & p\,I_p \end{array}\right) = p\,I_{p+1}$.

Avec la matrice de Paley nous disposons d'une matrice très proche d'une matrice de Hadamard à ceci près que la diagonale d'une matrice de Paley est nulle.

Exemple avec Maple :

Comme $\frac{11-1}{2} = 5$ est impair, $\chi_p(-1) = -1$

```
> P12:=blockmatrix(2,2,[Z,transpose(U(11)),-U(11),A11]);
```

$$P12 := \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}$$

```
> multiply(P12,transpose(P12));
```

$$\begin{bmatrix} 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 11 \end{bmatrix}$$

21. Théorème de Gilman

Soit p entier premier tel que $p = 3 \bmod 4$, P_{p+1} la matrice de Paley de taille $p+1$, alors la matrice :

$$H_{p+1} = P_{p+1} + I_{p+1}$$

est une matrice de Hadamard de taille $p+1$.

DEMONSTRATION :

Pour commencer, remarquons que les coefficients de H_{p+1} sont tous égaux à ± 1. Ensuite que :

$$p = 3 \bmod 4 \Leftrightarrow \frac{p+1}{2} \text{ pair } \Leftrightarrow \frac{p-1}{2} \text{ impair}$$

et qu'alors la matrice de Paley est antisymétrique.

$$H_{p+1}H_{p+1}^t = \left(P_{p+1} + I_{p+1}\right)\left(P_{p+1}^t + I_{p+1}\right) = P_{p+1}P_{p+1}^t + \underbrace{P_{p+1} + P_{p+1}^t}_{=0} + I_{p+1} = pI_{p+1} + I_{p+1} = (p+1)I_{p+1}$$

H_{p+1} vérifie bien une des propriétés caractéristiques des matrices de Hadamard.

Exemple calculé avec Maple :

```
> H12:=evalm(P12+Id(12));
```

$$H12 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \end{bmatrix}$$

La matrice obtenue n'est pas standardisée, mais il suffit de multiplier par -1 les lignes $2\cdots12$ pour y parvenir.

Quelles sont les tailles possibles des matrices de Hadamard que l'on peut fabriquer selon ce procédé ? Assurément pas tous les multiples de 4, (sinon la conjecture de Hadamard serait prouvé !). 36 est un multiple de 4, mais 35 n'est pas premier et le théorème ne s'applique pas. Voici une liste, calculée par Maple de tailles comprises entre 4 et 1000 pour lesquelles il s'applique.

```
4, 8, 12, 20, 24, 32, 44, 48, 60, 68, 72, 80, 84, 104, 108, 128, 132, 140, 152, 164, 168, 180,
192, 200, 212, 224, 228, 240, 252, 264, 272, 284, 308, 312, 332, 348, 360, 368, 380, 384, 420,
432, 440, 444, 464, 468, 480, 488, 492, 500, 504, 524, 548, 564, 572, 588, 600, 608, 620, 632,
644, 648, 660, 684, 692, 720, 728, 740, 744, 752, 788, 812, 824, 828, 840, 860, 864, 884, 888,
908, 912, 920, 948, 968, 972, 984, 992
```

Construction de Paley

La construction de Paley étend celle de Gilman et permet d'obtenir des tailles de matrices de Hadamard ignorées par Gilman comme : 28, 36, 52... Pour y parvenir, quelques préalables sont nécessaires.

Vers le théorème de Paley

Dans un corps $F_q\left(q=p^r, p\neq 2\right)$ on peut définir un symbole de Legendre $\chi(x)=x^{\frac{q-1}{2}}$ avec les mêmes propriétés que sur $\mathbb{Z}_p$. En particulier le fait qu'il existe $\frac{q-1}{2}$ carrés pour lesquels $\chi(x)=1$ et $\frac{q-1}{2}$ non carrés pour lesquels $\chi(x)=-1$.

Une difficulté subsiste quant à la définition d'une matrice de Jacobsthal de taille q, puisque nous ne disposons plus de la projection canonique de $\mathbb{Z}\longrightarrow\mathbb{Z}_p$. Cependant, on peut procéder de la manière suivante. Comme $\left|F_q\right|=q$, on peut définir une bijection (certes arbitraire) : $\begin{array}{c}1\cdots q\xrightarrow{\alpha}F_q\\ i\mapsto\alpha_i\end{array}$ et définir la matrice de Jacobsthal : $A_q=\left(\chi\left(\alpha_i-\alpha_j\right)\right)_{\substack{i\in1\cdots q\\ j\in1\cdots q}}$

À l'exception de la propriété 3 (circularité, mais elle n'a pas servi), elle possède les mêmes propriétés que celles énumérées dans 16 pour les matrices de Jacobsthal originelles. De plus le lemme 17 sur lequel est fondé la proposition 18 s'applique et $AA^t=pI_p-U_pU_p^t$.

On peut dès lors définir la matrice de Paley P_{q+1} comme précédemment et elle possède les mêmes propriétés. On est alors en mesure de démontrer :

22. Théorème de Paley

Soit $q=p^r$ puissance d'un nombre premier impair p, et P_{q+1} la matrice de Paley de taille $q+1$, alors :

1. *Si $q=3 \bmod 4$, la matrice :*

$$H_{q+1}=P_{q+1}+I_{q+1}$$

est une matrice de Hadamard de taille $q+1$.

2. *Si $q=1 \bmod 4$ La matrice :*

$$H_{2(q+1)} = \left(\begin{array}{c|c} P_{q+1} & P_{q+1} \\ \hline -P_{q+1} & P_{q+1} \end{array}\right) + \left(\begin{array}{c|c} I_{q+1} & -I_{q+1} \\ \hline I_{q+1} & I_{q+1} \end{array}\right)$$

est une matrice de Hadamard de taille $2(q+1)$ *.*

Si n *est un multiple de* 4 *tel que* $n-1$ *ou* $\frac{n}{2}-1$ *est une puissance d'un nombre premier impair, il existe une matrice de Hadamard de taille* n*.*

DEMONSTRATION :

1. Il suffit de reprendre la démonstration faite pour Gilman.
2. Pour alléger les écritures, on supprimera, sauf risque de confusion, les indices de taille.

$$H = \underbrace{\left(\begin{array}{c|c} P & P \\ \hline -P & P \end{array}\right)}_{A} + \underbrace{\left(\begin{array}{c|c} I & -I \\ \hline I & I \end{array}\right)}_{B}, \quad H^t = \underbrace{\left(\begin{array}{c|c} P^t & -P^t \\ \hline P^t & P^t \end{array}\right)}_{A^t} + \underbrace{\left(\begin{array}{c|c} I & I \\ \hline -I & I \end{array}\right)}_{B^t}$$

$HH^t = AA^t + BB^t + AB^t + BA^t$

- ✓ $AA^t = \left(\begin{array}{c|c} P & P \\ \hline -P & P \end{array}\right)\left(\begin{array}{c|c} P^t & -P^t \\ \hline P^t & P^t \end{array}\right) = \left(\begin{array}{c|c} 2PP^t & 0 \\ \hline 0 & 2PP^t \end{array}\right) = \left(\begin{array}{c|c} 2qI & 0 \\ \hline 0 & 2qI \end{array}\right) = 2qI_{2(q+1)}$.
- ✓ $BB^t = \left(\begin{array}{c|c} I & -I \\ \hline I & I \end{array}\right)\left(\begin{array}{c|c} I & I \\ \hline -I & I \end{array}\right) = \left(\begin{array}{c|c} 2I & 0 \\ \hline 0 & 2I \end{array}\right) = 2I_{2(q+1)}$.
- ✓ $AB^t = \left(\begin{array}{c|c} P & P \\ \hline -P & P \end{array}\right)\left(\begin{array}{c|c} I & I \\ \hline -I & I \end{array}\right) = \left(\begin{array}{c|c} 0 & 2P \\ \hline -2P & 0 \end{array}\right)$.
- ✓ $BA^t = \left(AB^t\right)^t = \left(\begin{array}{c|c} 0 & -2P^t \\ \hline 2P^t & 0 \end{array}\right)$.

Or pour $q = 1 \bmod 4$, $\frac{q-1}{2}$ est pair et la matrice P est symétrique ($P = P^t$). D'où :

$$AB^t + BA^t = \left(\begin{array}{c|c} 0 & 2\left(P-P^t\right) \\ \hline -2\left(P-P^t\right) & 0 \end{array}\right) = 0 .$$

Au final : $HH^t = 2qI_{2(q+1)} + 2I_{2(q+1)} = 2(q+1)I_{2(q+1)}$.

Tableau récapitulatif

Le tableau suivant indique, pour les multiples de 4 entre 4 et 1000, la construction qui les certifie comme étant une taille de matrice de Hadamard. Il y a « tuilage » puisque par exemple 8 est certifié par Gilman ($8-1=7$) mais l'était déjà par Sylvester ($8=2^3$).

Sylvester				Gilman				Paley I						Paley II										
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100
104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192	196	200
204	208	212	216	220	224	228	232	236	240	244	248	252	256	260	264	268	272	276	280	284	288	292	296	300
304	308	312	316	320	324	328	332	336	340	344	348	352	356	360	364	368	372	376	380	384	388	392	396	400
404	408	412	416	420	424	428	432	436	440	444	448	452	456	460	464	468	472	476	480	484	488	492	496	500
504	508	512	516	520	524	528	532	536	540	544	548	552	556	560	564	568	572	576	580	584	588	592	596	600
604	608	612	616	620	624	628	632	636	640	644	648	652	656	660	664	668	672	676	680	684	688	692	696	700
704	708	712	716	720	724	728	732	736	740	744	748	752	756	760	764	768	772	776	780	784	788	792	796	800
804	808	812	816	820	824	828	832	836	840	844	848	852	856	860	864	868	872	876	880	884	888	892	896	900
904	908	912	916	920	924	928	932	936	940	944	948	952	956	960	964	968	972	976	980	984	988	992	996	1000

Commentaires :

Entre 4 et 100, seul 92 manque à l'appel, mais il a été certifié par une autre méthode.

Selon la construction de Sylvester si une taille n est certifiée, $2n$ l'est aussi. D'autre nombres peuvent être ainsi certifiés : $112=2\times56$, $176=2\times88$, $248=2\times124$ …

Actuellement, les seuls nombres de ce tableau qui n'ont pas été certifiés sont ceux écrits en caractère rouge.

Intermède : spectre de P_{q+1} et H_{q+1} où $q=3 \bmod 4$

Dans ce qui suit, on se place dans le cas 1 du théorème de Paley où H_{q+1} est définie par :

$$H_{q+1}=P_{q+1}+I_{q+1}.$$

Rappels sur les propriétés spectrales des matrices orthogonales (Cf. [2])

Soit $Q\in\mathcal{M}_n(\mathbb{R})$ une matrice orthogonale, autrement dit vérifiant $QQ^t=Q^tQ=I$, alors :

1. Elle est diagonalisable sur $\mathbb{C}$ dans une base propre orthonormale pour le produit scalaire hermitien canonique de $\mathbb{C}^n$. Ce qui implique que les matrices de changement de base sont unitaires : B et $B^*=B^{-1}$.
2. Si $\lambda\in Spec(Q)$, $|\lambda|=1$.
3. Les sous-espaces propres E_λ sont orthogonaux 2 à 2.

23. Lemme

Soit $A\in\mathcal{M}_n(\mathbb{C})$, alors :

- ✓ *A et $A+I$ ont les mêmes vecteurs propres, donc les mêmes sous-espaces propres.*
- ✓ *$\lambda\in Spec(A)\Leftrightarrow\lambda+1\in Spec(A+I)$*
- ✓ *A diagonalisable $\Leftrightarrow A+I$ diagonalisable.*

DEMONSTRATION :

Soit V vecteur propre de A associé à la valeur propre λ, alors :

$AV = \lambda V \Leftrightarrow AV + V = \lambda V + V \Leftrightarrow (A+I)V = (\lambda+1)V$.

A est diagonalisable si et seulement si elle possède une base de vecteurs. Il en est alors de même pour $A+I$

24. Lemme

Soit $A \in \mathcal{M}_n(\mathbb{R})$, *alors :*

1. $\lambda \in Spec(A) \Rightarrow \overline{\lambda} \in Spec(A)$.
2. *Si* $V \in \mathbb{C}^n$ *est un vecteur propre associé à* λ, $\overline{V}$ *est un vecteur propre associé à* $\overline{\lambda}$.
3. $Dim(E_\lambda) = Dim(E_{\overline{\lambda}})$.

DEMONSTRATION :

$AV = \lambda V$ entraine par conjugaison $\overline{A}\overline{V} = \overline{\lambda}\overline{V}$ et comme $A \in \mathcal{M}_n(\mathbb{R})$, $A = \overline{A}$ ce qui prouve les deux premières assertions.

$V \mapsto \overline{V}$ définit une application[1] de $E_\lambda \longrightarrow E_{\overline{\lambda}}$. Si $(V_1, \cdots, V_k)$ est une base de E_λ, $(\overline{V_1}, \cdots, \overline{V_k})$ est une liste libre de $E_{\overline{\lambda}}$ donc $k \leq Dim(E_{\overline{\lambda}})$ et en procédant en sens inverse, on obtient l'égalité.

25. Proposition

Soit $q = p^r$ *puissance d'un nombre premier impair* p, $q = 3 \bmod 4$ *et* P_{q+1} *la matrice de Paley de taille* $q+1$ *et soit la matrice de Hadamard* $H_{q+1} = P_{q+1} + I_{q+1}$, *alors :*

1. P_{q+1} *et* H_{q+1} *sont diagonalisables.*
2. $Spec(P_{q+1}) = \left\{ i\sqrt{q}, -i\sqrt{q} \right\}$ *et* $Spec(H_{q+1}) = \left\{ 1 + i\sqrt{q}, 1 - i\sqrt{q} \right\}$.
3. *Les sous-espaces propres de* P_{q+1} *:* $E_{i\sqrt{q}}$ *et* $E_{-i\sqrt{q}}$, *identiques aux sous-espaces propres correspondant de* H_{q+1} *sont orthogonaux et de dimension* $\frac{q+1}{2}$.

DEMONSTRATION :

Pour alléger les écritures, on va omettre les indices.

1. De $PP^t = qI$ et $HH^t = (q+1)I$, on déduit que $\frac{1}{\sqrt{q}}P$ et $\frac{1}{\sqrt{q+1}}H$ sont orthogonales donc diagonalisables, donc aussi P et H.

2. De plus :

- ✓ $\lambda \in Spec\left(\frac{1}{\sqrt{q}}P\right) \Leftrightarrow \sqrt{q}\,\lambda \in Spec(P)$
- ✓ $\lambda \in Spec\left(\frac{1}{\sqrt{q+1}}H\right) \Leftrightarrow \sqrt{q+1}\,\lambda \in Spec(H)$.

Comme les valeurs propres de $\frac{1}{\sqrt{q}}P$ et $\frac{1}{\sqrt{q+1}}H$ sont de module 1 :

[1] Une telle application est dite sesquilinéaire.

- ✓ les valeurs propres de P sont de module $\sqrt{q}$,
- ✓ les valeurs propres de H sont de module $\sqrt{q+1}$.

Mais par ailleurs $H = P + I$ et selon le lemme précédent :

$$\lambda \in Spec(P) \Leftrightarrow \lambda + 1 \in Spec(H)$$

Comme $|\lambda| = \sqrt{q}$, on peut poser $\lambda = \sqrt{q}(\cos\theta + i\sin\theta)$. On a alors :

$$|\lambda+1|^2 = \left|\sqrt{q}(\cos\theta + i\sin\theta)+1\right|^2 = \left(\left(\sqrt{q}\cos\theta+1\right)^2 + q\sin^2\theta\right) = q+1+2\sqrt{q}\cos\theta .$$

Or $|\lambda+1|^2 = q+1$, d'où : $q+1 = q+1+2\sqrt{q}\cos\theta \Rightarrow \cos\theta = 0 \Rightarrow \lambda = \pm\sqrt{q}\,i$. Au final :

$$Spec(P) = \left\{i\sqrt{q}, -i\sqrt{q}\right\} \text{ et } Spec(H) = \left\{1+i\sqrt{q}, 1-i\sqrt{q}\right\}.$$

4. C'est une conséquence immédiate du rappel et des lemmes.

Exemple :

```
> H12:=evalm(P12+Id(12));
```

$$H12 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \end{bmatrix}$$

```
> {eigenvalues(H12)};
```

$$\{1+\sqrt{11}\,I, 1-\sqrt{11}\,I\}$$

Attention 💣

Cette proposition ne concerne que les matrices de Hadamard obtenues par la construction de Paley de type 1.

Elle est fausse, par exemple, pour les matrices de Hadamard-Walsh $H_n \in \mathcal{M}_n(\mathbb{R})$:

1. $\frac{1}{\sqrt{n}}H$ est symétrique. Donc toutes ses valeurs propres sont réelles.
2. $\frac{1}{\sqrt{n}}H$ est orthogonale : $\frac{1}{\sqrt{n}}H^t\frac{1}{\sqrt{n}}H = I_n$. Donc toutes ces valeurs propres sont de module 1.

Il en résulte que : $Spec(H_n) = \left\{-\sqrt{n}, \sqrt{n}\right\}$.

Application au « Block Design »

Dans toute cette section, le vocabulaire et les notations propres au « Block Design » seront utilisées.

Définitions

Soit $X=\{x_1, x_2, \cdots, x_v\}$ un ensemble de v éléments que l'on appellera des « points », b sous-ensembles $B_1, \cdots, B_b$ de E que l'on appellera des blocs. L'appartenance des points aux blocs est entièrement décrite par une matrice, dite matrice d'incidence :

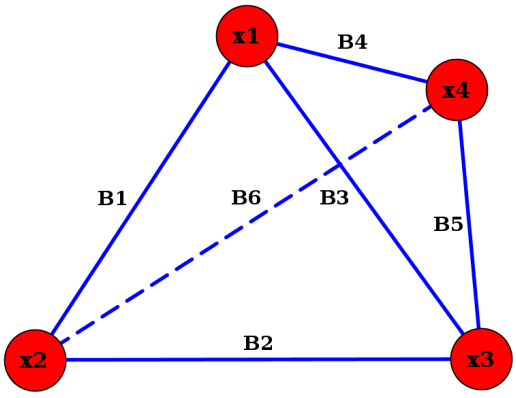
$$M=\left(m_{i,j}\right)_{\substack{i\in 1\cdots v\\ j\in 1\cdots b}} \in \mathcal{M}_{v\times b}(\mathbb{R}) \text{ où } m_{i,j}=\begin{cases}1 \text{ si } x_i \in B_j\\ 0 \text{ sinon}\end{cases}$$

Cette matrice d'incidence fournit les informations suivantes :

- ✓ $M_{i,\bullet}U_b=\sum_{j=1}^{b} m_{i,j}$ est le nombre de blocs auxquels appartient le point x_i.
- ✓ $U_v^t M_{\bullet,j}=\sum_{i=1}^{v} m_{i,j}$ est le nombre de points contenus dans le bloc B_j.
- ✓ Pour une paire de points distincts[2] $\{x_i, x_{i'}\}$ de X, $M_{i,\bullet}M_{i',\bullet}^t=\sum_{j=1}^{b} m_{i,j}m_{i',j}$ est le nombre de blocs contenant les deux points.
- ✓ Pour une paire de blocs distincts $\{B_j, B_{j'}\}$, $M_{\bullet,j}^t M_{\bullet,j'}=\sum_{i=1}^{v} m_{i,j}m_{i,j'}$ est le nombre de points contenus dans ces 2 blocs $\left|B_j \cap B_{j'}\right|$.

On appellera un <u>bloc design</u> une répartition des points dans les blocs définie par une telle matrice.

Exemple 1 tétraède :



L'ensemble X est constitué des 4 sommets, les 6 blocs sont définis par les arêtes. La matrice d'incidence est :

[2] Pléonasme : si ils n'étaient pas distincts, il ne formeraient pas une paire !

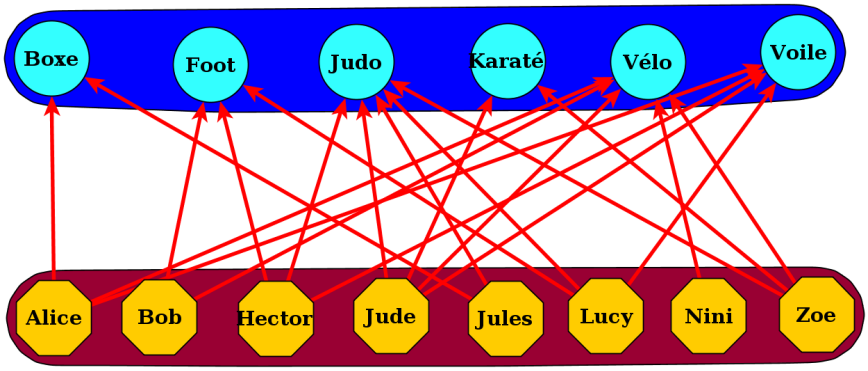
$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

La répartition peut être qualifiée de régulière :

- ✓ Chaque point appartient à 3 blocs.
- ✓ Chaque bloc contient 2 points.
- ✓ Une paire de points appartient à un et un seul bloc.

Exemple 2 un peu de sport :

X est un ensemble de 8 sportifs[ves] : {*Alice, Bob, Hector, Jude, Jules, Lucy, Nini, Zoe*}qui pratiquent au moins un des sports suivants :{*Boxe, Foot, Judo, Karaté, Vélo, Voile*}. Les pratiques sont représentés par le graphe bi-parti suivant :



Les blocs sont définis comme l'ensemble des pratiquants d'un sport. La matrice d'incidence est :

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

La répartition est beaucoup moins régulière :

- ✓ Le nombre de sports pratiqués par une personne varie de 1 à 4.
- ✓ Le nombre de pratiquants d'un sport varie de 2 à 5.

26. Définition

On appelle BIBD (Balanced Incomplete Block Design) de paramètres entiers (v, b, r, k, λ) $v, b \geq 2, r, k, \lambda \geq 1$ *un block design tel que :*

1. *v est le nombre de points.*
2. *b est le nombre de blocs.*
3. *r est le nombre de blocs contenant un point donné quelconque $r < b$.*
4. *k est le nombre de points contenu dans un bloc quelconque $k < v$.*

5. λ *est le nombre de blocs incluant une paire quelconque de points.*

Un BIBD *est dit symétrique si* $v = b$.

Commentaires :

1. L'exemple 1 est un BIBD de paramètres $(4, 6, 3, 2, 1)$, l'exemple 2 n'en est pas un.
2. $r < b$. implique qu'aucun point n'appartient à tous les blocs.
3. $k < v$ implique qu'aucun bloc ne contient tous les points.
4. Les paramètres d'un BIBD ne sont pas indépendants.

Relation entre les paramètres d'un BIBD

27. Proposition

Les paramètres (v, b, r, k, λ) *d'un* BIBD *vérifient les relations suivantes :*

1. $v \times r = b \times k$ *ce qui implique pour un* BIBD *symétrique* $r = k$.
2. $\lambda(v-1) = r(k-1)$.
3. $\lambda < r$

DEMONSTRATION :

1. Sur chacune des v lignes de M, il y a r coefficients égaux à 1. Sur chacune des b colonnes de M, il y a k coefficients égaux à 1. Le nombre de coefficients égaux à 1 dans M est donc : $v \times r = b \times k$.
2. Soit un point x_i, le nombre de blocs incluant une paire contenant x_i peut se calculer de deux manières :
   - ✓ La paire $\{x_i, x\}$ appartient à λ blocs et il existe $v-1$ façons de choisir x. Soit $\lambda(v-1)$
   - ✓ x_i appartient à r blocs et il existe $k-1$ façons de choisir x dans chacun de ces blocs : Soit : $r(k-1)$.
3. Si $\lambda = r$, alors l'égalité précédente implique $v = k$ ce qui est exclu.

28. Proposition

La matrice d'incidence $M \in \mathcal{M}_{v \times b}(\{0,1\})$ *d'un* BIBD *de paramètres* (v, b, r, k, λ) *vérifie :*

1. $\forall i \in 1 \cdots v : M_{i,\bullet} U_b = r \Leftrightarrow M U_b = r U_v$.
2. $\forall j \in 1 \cdots b : U_v^t M_{\bullet,j} = k \Leftrightarrow M^t U_v = k U_b$.
3. $\forall i, i' \in 1 \cdots v : i \neq i' \Rightarrow M_{i,\bullet} M_{i',\bullet}^t = \lambda \Leftrightarrow M M^t = \lambda U_v U_v^t + (r - \lambda) I_v$.
4. $Rg(M) = v$.

DEMONSTRATION :

Soit un BIBD de paramètres (v, b, r, k, λ) et de matrice M.

1. $M_{i,\bullet} U_b^t = \sum_{j=1}^{b} m_{i,j}$ est le nombre de blocs auxquels appartient le point x_i. Comme chacun des points appartient à r blocs, $\forall i \in 1 \cdots v : M_{i,\bullet} U_b^t = r$. Ce qui matriciellement s'écrit : $M U_b = r U_v$.
2. Analogue à 1.

3. $M_{i,\bullet}M_{i',\bullet}^t = \sum_{j=1}^{b} m_{i,j}m_{i',j}$ est le nombre de blocs incluant la paire $\{x_i, x_{i'}\}$. Comme chacune des paires est incluse dans λ blocs, $M_{i,\bullet}M_{i',\bullet}^t = \lambda$. De plus si $i = i'$ $M_{i,\bullet}M_{i,\bullet}^t = \sum_{j=1}^{b}\left(m_{i,j}\right)^2 = \sum_{j=1}^{b} m_{i,j} = r$.

Au final on a :

$$M\,M^t = \left(M_{i,\bullet}M_{i',\bullet}^t\right)_{i,i'\in 1\cdots v} = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{pmatrix} = \lambda U_v U_v^t + (r-\lambda) I_v .$$

4.

$$Det\left(M\,M^t\right) = Det\left(\lambda U_v U_v^t + (r-\lambda) I_v\right) = \begin{vmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{vmatrix} = \underbrace{r + (v-1)\lambda \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{vmatrix}}_{\text{(addition des lignes } 2\cdots v \text{ sur la } 1^\circ)}$$

$$Det\left(M\,M^t\right) = r + (v-1)\lambda \underbrace{\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & r-\lambda & 0 & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & r-\lambda \end{vmatrix}}_{\substack{\text{soustaction de } \lambda \text{ la } 1^\circ \text{ ligne} \\ \text{aux autres}}} = \left(r + (v-1)\lambda\right)(r-\lambda)^{v-1} \neq 0 \text{ puisque } \lambda < r$$

La matrice $M\,M^t$ est donc de rang *v*. Comme $Rg(M) = Rg\left(M\,M^t\right)$, la matrice *M* est de rang *v*.

29. Corollaire : inégalité de Fisher

Soit un BIBD de paramètres (v, b, r, k, λ), alors $v \le b$ et $k \le r$.

DEMONSTRATION :

La matrice d'incidence *M* est de taille $v \times b$ et de rang *r* d'après la proposition précédente. Et on sait que $Rg(M) \le \min(v, b)$. La deuxième inégalité est une conséquence immédiate de $v \times r = b \times k$ (27.1).

La proposition suivante est une manière (car elle ne requière pas ses 4 conditions) de réciproque de la proposition 28.

30. Proposition

Un bloc design dont la matrice d'incidence $M \in \mathcal{M}_{v\times b}(\{0,1\})$ vérifie :

1. $M U_b = r U_v$,
2. $M\,M^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{pmatrix} = \lambda U_v U_v^t + (r-\lambda) I_v$ *où* $\lambda < r$,

est un BIBD de paramètres (v, b, r, k, λ) où $k = \dfrac{v \times r}{b}$.

DEMONSTRATION :

De 1, on déduit que le nombre $M_{i,\bullet}U_b^t$ de blocs auxquels appartient un point x_i est égal à r.

De 2, on déduit que le nombre $M_{i,\bullet}M_{i',\bullet}^t$ de blocs contenant la paire $\{x_i, x_{i'}\}$ est égal à λ.

Le calcul de $Det(M\,M^t)$ tel qu'il a été fait précédemment mène à la même conclusion, à savoir, $Rg(M)=v$. Ce rang implique que $r<b$, sinon toutes les lignes de M seraient remplies de 1 et son rang serait 1.

Il reste à prouver que le nombre $U_v^t M_{\bullet,j}$ de points contenus dans un bloc quelconque B_j est constant.

$$M\,M^t U_v = \left(\lambda U_v U_v^t + (r-\lambda) I_v\right)U_v = \lambda U_v \underbrace{U_v^t U_v}_{=v} + (r-\lambda)U_v = \left(\lambda(v-1)+r\right)U_v .$$

Or $M U_b = r U_v$ d'où : $M\,M^t U_v = \left(\dfrac{\lambda(v-1)+r}{r}\right)U_v$.

Notons que $M\,M^t U_v$ étant à coefficients entiers, $\dfrac{\lambda(v-1)+r}{r}$ est un entier que l'on pose égal à k.

On a alors : $M\left(M^t U_v - k\,U_b\right)=0$.

Or la matrice M est de rang v. et selon le théorème du rang, $Ker(M)=\{0\}$. D'où :

$$M^t U_v = k\,U_b .$$

On savait que le nombre de termes égaux à 1 sur chaque ligne de M est égal à r, On sait, désormais, que le nombre de termes égaux à 1 sur chaque colonne de M est égal à k. Ce qui entraine : $v\times r = b\times k$.

Enfin, il reste à prouver $k<v$ et $r<b$:

$$k<v \Leftrightarrow \frac{\lambda(v-1)+r}{r} < v \Leftrightarrow \lambda < r .$$

$$r<b \Leftrightarrow vr<vb \Leftrightarrow bk<vb \Leftrightarrow k<v$$

BIBD symétrique

31. Proposition

Si M est la matrice d'incidence d'un BIBD symétrique, alors $M\,M^t = M^t M$.

DEMONSTRATION :

Si M est la matrice d'incidence d'un BIBD symétrique, on sait (27.1) que $r=k$ et M est une matrice carrée de taille $v\times v$ et de rang v donc inversible.

Selon 28.3 :

$$\left(M\,M^t\right)M = \left(\lambda U_v U_v^t + (r-\lambda)I_v\right)M = \lambda U_v U_v^t M + (r-\lambda)M .$$

Selon 28.2 , $U_v^t M = \left(M^t U_v\right)^t = kU_v^t$. D'où :

$$\left(M\,M^t\right)M == \lambda k U_v U_v^t + (r-\lambda)M .$$

Par ailleurs :

$$M\left(M\,M^t\right) = M\left(\lambda U_v U_v^t + (r-\lambda)I_v\right) = \lambda M\,U_v U_v^t + (r-\lambda)M .$$

Et selon 28.1 $M U_v = r U_v$. D'où :

$$M\left(M M^t\right) = \lambda r U_v U_v^t + (r-\lambda) M$$

Comme $r = k$, $M M^t M = M M M^t$ et comme M inversible : $M^t M = M M^t$.

32. Corollaire

Soit un BIBD symétrique de paramètres (v, v, r, r, λ), le nombre de points communs à une paire de blocs est $\left|B_j \cap B_{j'}\right| = \lambda$.

DEMONSTRATION :

Pour une paire de blocs distincts $\left\{B_j, B_{j'}\right\}$, $M^t_{\bullet, j} M_{\bullet, j'} = \sum_{i=1}^{v} m_{i,j} m_{i,j'}$ est le nombre de points contenus dans ces 2 blocs $\left|B_j \cap B_{j'}\right|$. Et $M^t M = M M^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{pmatrix}$.

Fabrication de nouveaux BIBD à partir d'un BIBD symétrique :

33. Proposition

Partant d'un BIBD symétrique de paramètres (v, v, r, r, λ) de matrice d'incidence M, on obtient :

1. *En supprimant dans M une colonne j et toutes les lignes i telles que $m_{i,j} = 1$ un BIBD de paramètres $(v-r, v-1, r, r-\lambda, \lambda)$ dit résiduel,*
2. *En supprimant dans M une colonne j et toutes les lignes i telles que $m_{i,j} = 0$ un BIBD de paramètres $(r, v-1, r-1, \lambda, \lambda-1)$ dit dérivé.*

DEMONSTRATION :

Pour simplifier les écritures, on supposera que la colonne supprimée est la dernière v.

Soit Mr la matrice obtenue selon le procédé 1. Elle possède 1 colonne de moins et r lignes de moins et est donc de taille : $(v-r)\times(v-1)$.

Remarque préalable :

La ligne $Mr_{i,\bullet}$, provient d'une ligne de M contenant r termes égaux à 1 et dont le dernier terme est nul. Elle contient elle aussi r termes égaux à 1.

$Mr U_{v-1} = ?$

Selon la remarque préalable : $Mr_{i,\bullet} U_{v-1} = r$. Soit D'où : $Mr U_{v-1} = r U_{v-r}$.

$Mr Mr^t = ?$

Soit $Mr_{i,\bullet}$ et $Mr_{i',\bullet}$.

Si $i = i'$, le résultat précédent montre que $Mr_{i,\bullet} Mr^t_{i,\bullet} = r$.

Si $i \neq i'$, les deux lignes de Mr proviennent de deux lignes distinctes de M, disons L_1 et L_2 se terminant toutes deux par 0. Il en résulte que $Mr_{i,\bullet} Mr_{i',\bullet}^t = L_1 L_2^t$ Or comme M est la matrice d'un BIBD de paramètres (v, v, r, r, λ), $L_1 L_2^t = \lambda$ et :

$$Mr\,Mr^t = \begin{pmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \ddots & \vdots \\ \vdots & \ddots & \ddots & \lambda \\ \lambda & \cdots & \lambda & r \end{pmatrix} \text{ avec } \lambda < r$$

La proposition 30 dit alors que Mr est la matrice d'un BIBD de paramètres : $(v-r, v-1, r, k, \lambda)$ où $k = \frac{(v-r)\times r}{v-1}$. Or k peut s'écrire plus simplement $k = r - \lambda$ comme le montre :

$$k = r - \lambda \Leftrightarrow (v-r)r = (v-1)(r-\lambda) \Leftrightarrow \cancel{vr} - r^2 = \cancel{vr} - v\lambda - r + \lambda \Leftrightarrow v\lambda - \lambda = r^2 - r \Leftrightarrow \lambda(v-1) = r(r-1)$$

La dernière égalité est vraie avec les paramètres du BIBD symétrique initiale.

La deuxième assertion se montre de manière analogue.

Exemples :

Soit le BIBD[3] symétrique de paramètres $(v, v, r, r, \lambda) = (11, 11, 5, 5, 2)$ défini par la matrice d'incidence M_{11} :

0	1	0	1	1	1	0	0	0	1	0	5
0	0	1	0	1	1	1	0	0	0	1	5
1	0	0	1	0	1	1	1	0	0	0	5
0	1	0	0	1	0	1	1	1	0	0	5
0	0	1	0	0	1	0	1	1	1	0	5
0	0	0	1	0	0	1	0	1	1	1	5
1	0	0	0	1	0	0	1	0	1	1	5
1	1	0	0	0	1	0	0	1	0	1	5
1	1	1	0	0	0	1	0	0	1	0	5
0	1	1	1	0	0	0	1	0	0	1	5
1	0	1	1	1	0	0	0	1	0	0	5
5	5	5	5	5	5	5	5	5	5	5	

En appliquant le premier procédé (les lignes et colonnes supprimées sont en blanc), on obtient un BIBD (non symétrique) de paramètres $(v, b, r, k, \lambda) = (6, 10, 5, 3, 2)$ défini par la matrice d'incidence :

0	1	0	1	1	1	0	0	0	1	5
1	0	0	1	0	1	1	1	0	0	5
0	1	0	0	1	0	1	1	1	0	5
0	0	1	0	0	1	0	1	1	1	5
1	1	1	0	0	0	1	0	0	1	5
1	0	1	1	1	0	0	0	1	0	5
3	3	3	3	3	3	3	3	3	3	

[3] Le mystère entourant la fabrication de ce BIBD sera bientôt levé…

En appliquant le deuxième procédé (les lignes et colonnes supprimées sont en bleu), on obtient un BIBD (non symétrique) de paramètres $(v,b,r,k,\lambda)=(5,10,4,2,1)$ défini par la matrice d'incidence :

0	0	1	0	1	1	1	0	0	0	4
0	0	0	1	0	0	1	0	1	1	4
1	0	0	0	1	0	0	1	0	1	4
1	1	0	0	0	1	0	0	1	0	4
0	1	1	1	0	0	0	1	0	0	4
2	2	2	2	2	2	2	2	2	2	

BIDB et Hadamard

Les matrices de Hadamard offrent un processus de fabrication de BIBD symétrique :

34. Proposition

Soit H_n une matrice de Hadamard de taille n (n multiple de 4) mise sous forme standard. La matrice $M \in \mathcal{M}_{n-1}(\{0,1\})$ obtenue à partir de H_n en :

- ✓ *supprimant la 1° ligne et la 1° colonne de H_n,*
- ✓ *remplaçant les -1 par des 0 ,*

est la matrice d'incidence d'un BIDB symétrique de paramètres $\left(n-1, n-1, \frac{n}{2}-1, \frac{n}{2}-1, \frac{n}{4}-1\right)$.

DEMONSTRATION :

La démonstration de la proposition 6 a mis en évidence qu'une matrice de Hadamard H standardisée de taille n possède les propriétés suivantes :

(1) Pour toute ligne $H_{i,\bullet}, i \neq 1$, il existe :

- ✓ $\frac{n}{2}$ indices j tels que $h_{i,j}=1$
- ✓ $\frac{n}{2}$ indices j tels que $h_{i,j}=-1$

(2) Pour toute paire de ligne $H_{i,\bullet}$ et $H_{i',\bullet}$, $i,i' \neq 1, i \neq i'$, il existe :

- ✓ $\frac{n}{4}$ indices j tels que : $h_{i,j}=1$ et $h_{i',j}=1$.
- ✓ $\frac{n}{4}$ indices j tels que : $h_{i,j}=-1$ et $h_{i',j}=1$.
- ✓ $\frac{n}{4}$ indices j tels que : $h_{i,j}=1$ et $h_{i',j}=-1$.
- ✓ $\frac{n}{4}$ indices j tels que : $h_{i,j}=-1$ et $h_{i',j}=-1$.

Pour simplifier les écritures lignes et colonnes de M seront numérotées de 2 à n :

$$M=\left(m_{i,j}\right)_{\substack{i\in 2\cdots n\\ j\in 2\cdots n}} \text{ où } m_{i,j}=\begin{cases}1 \text{ si } h_{i,j}=1\\ 0 \text{ si } h_{i,j}=-1\end{cases}$$

$M\,U_{n-1}=?$

Soit $i\neq 1$, sur la ligne i de H, il existe autant de 1 que de -1. Sachant que $h_{i,1}=1$, le nombre de 1 dans les colonnes $j\in 2\cdots h$ est donc $\frac{n}{2}-1$. Donc :

$$\forall i\in 2\cdots n:\quad \sum_{j=2}^{n} m_{i,j}=M_{i,\bullet}\,U_{n-1}=\frac{n}{2}-1\Rightarrow M\,U_{n-1}=\left(\frac{n}{2}-1\right)U_{n-1}.$$

$M\,M^t=?$

Soit $i,i'\neq 1$

1° cas : $i=i'$

Le raisonnement précédent, montre qu'il existe sur la ligne i de M $\frac{n}{2}-1$ termes non nuls. Donc :

$$\forall i\in 2\cdots n:\quad \sum_{j=2}^{n}\left(m_{i,j}\right)^2=M_{i,\bullet}\,M^t_{i,\bullet}=\frac{n}{2}-1$$

2° cas : $i\neq i'$

En passant de H à M, seuls les indices j tels que : $h_{i,j}=1$ et $h_{i',j}=1$ donneront un produit non nul. Et selon (2) il en existe $\frac{n}{4}$, auquel il faudra retrancher l'indice $j=1$. Donc :

$$\forall i,i'\in 2\cdots n, i\neq i':\quad \sum_{j=2}^{n} m_{i,j}m_{i,j'}=M_{i,\bullet}\,M_{i',\bullet}=\frac{n}{4}-1$$

En rassemblant les deux cas, il vient :

$$M\,M^t=\left(M_{i,\bullet}\,M^t_{i',\bullet}\right)_{\substack{i\in 2\cdots n\\ i''\in 2\cdots n}}=\begin{pmatrix} r & \lambda & \cdots & \lambda\\ \lambda & r & \ddots & \vdots\\ \vdots & \ddots & \ddots & \lambda\\ \lambda & \cdots & \lambda & r\end{pmatrix}\text{ où } r=\frac{n}{2}-1 \text{ et } \lambda=\frac{n}{4}-1.$$

M vérifie donc les 2 conditions de la proposition 30.

Exemple :

Voici la matrice d'incidence obtenue à partir de la matrice de Hadamard H_{12} (après mise sous forme standard) déjà présentée :

```
> M:=subs(-1=0,submatrix(H12,2..12,2..12));
```

$$M:=\begin{bmatrix}0&1&0&1&1&1&0&0&0&1&0\\0&0&1&0&1&1&1&0&0&0&1\\1&0&0&1&0&1&1&1&0&0&0\\0&1&0&0&1&0&1&1&1&0&0\\0&0&1&0&0&1&0&1&1&1&0\\0&0&0&1&0&0&1&0&1&1&1\\1&0&0&0&1&0&0&1&0&1&1\\1&1&0&0&0&1&0&0&1&0&1\\1&1&1&0&0&0&1&0&0&1&0\\0&1&1&1&0&0&0&1&0&0&1\\1&0&1&1&1&0&0&0&1&0&0\end{bmatrix}$$

```
> multiply(transpose(U(11)),M);
```

```
[5  5  5  5  5  5  5  5  5  5  5]
```

Et comme il s'agit d'un BIBD symétrique :

```
> multiply(M,transpose(M)), multiply(transpose(M),M);
```

$$\begin{bmatrix} 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 \end{bmatrix} \begin{bmatrix} 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 & 2 \\ 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 5 \end{bmatrix}$$

À quoi servent les BIBD ?

Ils servent, entre autres, à construire des plans d'expériences. Ces plans ont été initiés par Ronald Fisher dans les années 1930 pour organiser de façon rationnelle l'expérimentation en agronomie. Ces méthodes ont été largement développées et leur champ d'applications s'est élargi à de nombreux autres domaines : contrôles de qualité, efficacité de traitement médicaux, tests de produits…

Petit exemple d'application

Un guide gastronomique dispose de 11 inspecteurs devant tester sur une durée de 5 jours 11 restaurants.

La solution consistant à attribuer un restaurant à chaque inspecteur, en dehors du sous-emploi des inspecteurs, risquerait de conduire à des résultats fortement biaisés.

La solution qui enverrait chaque inspecteur tester les 11 restaurants, en dehors du fait qu'elle serait dispendieuse, risquerait de mettre à rude épreuve le système digestif des inspecteurs au point d'altérer leur faculté de jugement.

Ayant écarté ces solutions extrêmes, on peut envisager d'attribuer à chaque restaurant un bloc d'inspecteurs selon la matrice d'incidence M présentée plus haut. Ainsi :

- ✓ Chaque inspecteur visiterait 5 restaurants.
- ✓ Chaque restaurant serait visité par 5 inspecteurs.
- ✓ Chaque paire d'inspecteurs partageraient 2 restaurants en commun.
- ✓ Chaque paire de restaurants partageraient 2 inspecteurs en commun

Selon cette répartition, voici le tableau des notes totalement fantaisistes (de 0 à 20) attribuées :

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	Moyenne	Variance
S1		9		11	10	6				17		10,6	13,0
S2			12		12	9	16				10	11,8	5,8
S3	14			8		20	13	12				13,4	15,0
S4		17			10		14	12	1			10,8	29,4
S5			18			18		3	18	8		13	40,0
S6				4			14		18	3	14	10,6	35,8
S7	20				5			13		11	8	11,4	25,8
S8	6	0				10			20		10	9,2	42,6
S9	12	10	6				11			9		9,6	4,2
S10		1	14	12				0			7	6,8	31,8
S11	12		6	12	14				20			12,8	20,2
Moyenne	12,8	7,4	11,2	9,4	10,2	12,6	13,6	8	15,4	9,6	9,8		
Variance	20,2	39,4	21,8	9,4	9,0	29,4	2,6	29,2	52,6	20,6	5,8		

Ce tableau suggère l'idée de procéder à une analyse de la variance, laquelle a aussi été initiée par… Ronald Fisher. Les calculs sont facilités par le fait que toutes les classes ont un effectif de 5.

Analyse de la variance (ANOVA)

La moyenne générale est $m \simeq 10{,}91$, la variance totale est $V \simeq 27{,}32$.

Pour les blocs (restaurants) :

Variance des moyennes : V_{inter}	5,49	F=1,107
Moyenne des variances : V_{intra}	21,83	
Variance totale : $V_{inter} + V_{intra}$	27,32	
Rapport de Corrélation : $\eta^2 = \frac{V_{inter}}{V}$	20%	

Pour les inspecteurs :

Variance des moyennes : V_{inter}	3,36	F=0,616
Moyenne des variances : V_{intra}	23,96	
Variance totale : $V_{inter} + V_{intra}$	27,32	
Rapport de Corrélation : $\eta^2 = \frac{V_{inter}}{V}$	12%	

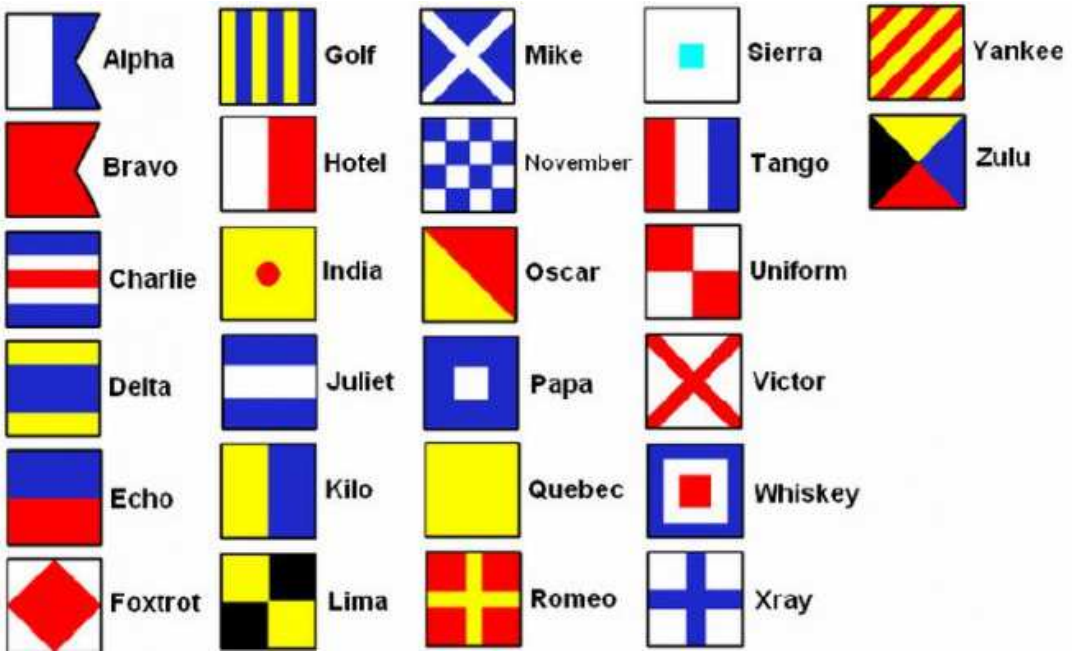
Test de Fisher

Il consiste à calculer $F = \dfrac{\frac{1}{k-1}V_{inter}}{\frac{1}{n-k}V_{intra}} = \dfrac{\eta^2}{1-\eta^2}\dfrac{n-k}{k-1}$, puis à le comparer à une valeur tabulée. Un F calculé supérieur à la valeur tabulée conduit à rejeter l'hypothèse « absence d'effet significatif des facteurs[4] sur les moyennes ». Dans notre exemple, la table à 5% donne pour $k-1=10$ et $n-k=44$, donne $F=2{,}054$. Les deux F calculés sont nettement inférieurs à ce seuil, donc ne permettent d'infirmer cette hypothèse. Ce qui n'a rien d'évident puisque, une première analyse des résultats met en évidence :

- ✓ La sévérité de l'inspecteur *S10*.
- ✓ Le mauvais score du restaurant *R2*.

[4] Les facteurs sont ici : dans un cas les inspecteurs, dans l'autre les restaurants.

Application aux codes



Deux codes dénués de secrets

Les codes sur lesquels nous allons nous pencher visent effectivement un tout autre but que les codes « secrets ». Alors que ces derniers, qu'il convient mieux d'évoquer sous l'appellation de système crypté, visent à la dissimulation, les méthodes que l'on va présenter ambitionnent de détecter et corriger des erreurs de transmission sur des canaux plus ou moins fiables.

Le code radiophonique « Alpha Bravo Charlie » illustré ci-dessus présente deux traits caractéristiques que l'on retrouvera :

- ✓ Les « briques » constitutives du code sont choisies pour être nettement distinctes les unes des autres. Avec une réception brouillée, le risque de confusion, par exemple, entre « Mike » et « November » sera plus faible qu'entre un « M » et « N ». Et mieux, un auditeur entendant « Roneo », pourra corriger de lui-même l'erreur sans solliciter une nouvelle transmission.
- ✓ Mais, cela se paye par un allongement du message. Petite anecdote personnelle. À une époque où les téléphones portables n'avaient pas conquis le monde, il existait pour les bateaux un moyen d'accéder au réseau téléphonique via un émetteur récepteur VHF. La procédure était un peu compliquée. Après avoir contacté un opérateur à terre sur un canal dédié et donner son indicatif, il fallait décliner le nom du bateau en code radiophonique, ce qui donnait pour mon avant-dernier voilier :

  Oscar Sierra Alpha India Sierra Oscar November Sierra
  Oscar Bravo Alpha Tango Echo Alpha Uniform Xray

  Beaucoup plus long que le nom du bateau :

  Ô Saisons, Ô Bateaux !

L'exposé qui va suivre n'a pas du tout la prétention de faire le tour du sujet : il est très vaste et la littérature abondante. Beaucoup plus modestement, après la présentation des notions de base, il s'agit d'exposer des applications des matrices de Hadamard à ce domaine.

Codes détecteurs et correcteurs

Généralités

Soit A un alphabet de $q \geq 2$ lettres. Sur l'ensemble A^n des mots de n lettres on définit la distance de Hamming ainsi :

$$\text{pour } x=(x_1,\cdots,x_n),\ y=(y_1,\cdots,y_n)\in A^n,\ d(x,y)=\left|\{i\in 1\cdots n\ /x_i\neq y_i\}\right|.$$

Dit plus simplement, $d(x,y)$ est le nombre de désaccords entre les mots x et y. Il est facile de vérifier qu'il s'agit d'une « vraie » distance vérifiant, pour tout $x,y,z\in A^n$:

1. $d(x,y)=0\Leftrightarrow x=y$.
2. $d(x,y)=d(y,x)$.
3. $d(x,y)\leq d(x,z)+d(z,y)$.

DEMONSTRATION :

Le 1 et 2 sont évidents. Pour le 3, on va procéder par récurrence :

$\mathcal{H}_1$:

Pour $n=1$, les distances appartiennent à $\{0,1\}$. Si $x=y$, $d(x,y)=0$ et l'inégalité est nécessairement vérifiée. Sinon $x\neq y$ et $d(x,y)=1$. Mais z ne peut être égal à la fois à x et à z ! Un, au moins, des deux termes du membre de droite est égal à 1 et l'inégalité est encore vérifiée.

$\mathcal{H}_{n-1}\Rightarrow\mathcal{H}_n$:

Pour : $x=(x_1,\cdots,x_n),\ y=(y_1,\cdots,y_n),\ z=(z_1,\cdots,z_n)\in A^n$, on notera :

$x'=(x_1,\cdots,x_{n-1}),\ y'=(y_1,\cdots,y_{n-1}),\ z'=(z_1,\cdots,z_{n-1})\in A^{n-1}$. On a :

- ✓ $d(x,y)=d(x',y')+d(x_n,y_n)$
- ✓ $d(x,z)=d(x',z')+d(x_n,z_n)$
- ✓ $d(z,y)=d(z',y')+d(z_n,y_n)$

$d(x,y)\leq d(x,z)+d(z,y)$ se déduit alors de $\mathcal{H}_1$ et $\mathcal{H}_{n-1}$.

Un code C est défini comme un sous-ensemble strict de A^n. Sa distance minimale $\delta(C)$ (ou plus simplement δ) est définie par :

$$\delta(C)=\min_{\substack{x,y\in C\\ x\neq y}} d(x,y).$$

Exemple trivial :

Si C est la diagonale de A^n, autrement dit l'ensemble des mots constitués par la répétition d'une même lettre, alors $\delta(C)=n$.

Détection et correction d'erreurs

Supposons que l'on doive transmettre par un canal plus ou moins fiable un mot de k lettres. En cas d'erreur de transmission, rien ne permet de la détecter. Pour remédier à cette vulnérabilité, on recourt à la méthode suivante :

On choisit un entier $n > k$ et une application injective de $A^k \xrightarrow{f} A^n$, dite application de codage. On définit alors le code $C = \mathrm{Im}(f)$. Comme f injective $|C| = |A^k| = q^k$. Si δ est la distance minimale de C, on dira que le code a pour paramètres (k, n, δ). Le rapport $\frac{n}{k}$ est la redondance du code. Au lieu de transmettre le mot $x \in A^k$, on transmettra $f(x) \in C \subset A^n$.

Dès lors si le mot reçu n'appartient pas à C, on sait qu'il y a eu quelque cafouillage dans la transmission et qu'au moins une lettre du mot transmis est erronée. En sens inverse, l'appartenance du mot reçu à C ne garantit pas l'absence de cafouillage. Tout va dépendre du nombre de lettres erronées et des capacités du code à détecter, puis d'éventuellement corriger des erreurs.

Précision de vocabulaire :

- ✓ Dire qu'un code peut détecter e erreurs signifie que toute erreur affectant un nombre de lettres $\leq e$ est détectée.
- ✓ Dire qu'un code peut corriger c erreurs signifie que toute erreur affectant un nombre de lettres $\leq e$ est corrigée.

1° Exemple : bit de parité

$A = \mathbb{Z}_2 = \{0,1\}$, $k = 8$, $n = 9$. On veut transmettre un octet. On définit $\mathbb{Z}_2^8 \xrightarrow{f} \mathbb{Z}_2^9$ par :

$$x = (x_1, \cdots, x_8) \mid \xrightarrow{f} \left(x_1, \cdots, x_8, \sum_{i=1}^{8} x_i \right) \quad \sum_{i=1}^{8} x_i = \begin{cases} 0 \text{ si } x \text{ contient un nombre paire de 1} \\ 1 \text{ si } x \text{ contient un nombre impaire de 1} \end{cases}$$

La distance minimale δ est de 2. En effet :

- ✓ $d(f(x), f(y)) \geq d(x, y)$.
- ✓ Si $d(x, y) = 1$, $\sum_{i=1}^{8} x_i \neq \sum_{i=1}^{8} y_i$ et $d(f(x), f(y)) = 2$.

Cette méthode utilisée dès le début de l'informatique a le mérite de la simplicité et d'une faible redondance mais reste rudimentaire :

- ✓ Elle permet de détecter 1 erreur mais pas 2.
- ✓ En cas de détection de 1 erreur, elle ne fournit aucune information sur le bit erroné et, de ce fait, est dans l'incapacité de corriger l'erreur

Pour espérer des codes plus performants dans la détection et la correction, il faut se tourner vers des codes dont la distance minimale est plus élevée comme le montre la proposition suivante.

35. Proposition

Un code C de paramètres (k, n, δ) *peut :*

- ✓ *détecter* $\delta - 1$ *erreurs,*
- ✓ *corriger* $\left\lfloor \frac{\delta - 1}{2} \right\rfloor$ *erreurs.*

DEMONSTRATION :

1. Soit $x \in C$ le mot initial et x' le mot reçu. Si x' comporte e lettres erronées, alors $d(x, x') = e$. Comme la distance entre deux mots de C est au moins égal à δ, si $e < \delta$, $x' \notin C$ et l'erreur est détectée.

2. Comme $x' \notin C$, l'idée de la correction est de déterminer le mot de C le plus proche de x' ce qui suppose qu'il est unique. Supposons qu'il existe 2 mots distincts $x, y \in C$ tels que $d(x, x') = d(y, x') = e$. L'inégalité triangulaire permet d'écrire : $d(x, y) \leq d(x, x') + d(x', y) = 2e$.

Si $\delta > 2e$, $d(x, y) > 2e$ pour tous mots distincts de C. L'inégalité $d(x, y) \leq 2e$ est fausse et il existe un seul $x \in C$ tel que $d(x, x') = e$, la correction est donc possible.

$$\delta > 2e \Leftrightarrow \delta - 1 \geq 2e \Leftrightarrow \frac{\delta - 1}{2} \geq e \Leftrightarrow \left\lfloor \frac{\delta - 1}{2} \right\rfloor \geq e .$$

2° Exemple ultra classique fondée sur une matrice de Hadamard

$A=\mathbb{Z}_2=\{0,1\}$, $2\le k, n=2^k$. On sait qu'il existe une matrice de Hadamard H de taille n. Entre 2 lignes distinctes de cette matrice, il existe autant d'accords que de désaccords soit $\frac{n}{2}=2^{k-1}$ Cette propriété est conservé si on remplace dans H les -1 par des 0, pour obtenir une matrice R. On a donc :

$$i\neq i' \Rightarrow d\left(R_{i,\bullet}, R_{i',\bullet}\right)=\frac{n}{2}=2^{k-1} \quad (1)$$

Tout mot $x\in\{0,1\}^k$ peut être considéré comme l'écriture binaire d'un entier $\overline{x}\in 0\cdots 2^k-1$ On peut, dès lors, définir :

$$\mathbb{Z}_2^k \xrightarrow{f} \mathbb{Z}_2^n \text{ par } f(x)=R_{\overline{x}+1,\bullet}.$$

$C=\mathrm{Im}(f)$ est alors l'ensemble des lignes de la matrice R. Et d'après (1) $\delta(C)=2^{k-1}$. Au final, on obtient un code de paramètres : $\left(k, 2^k, 2^{k-1}\right)$ donc capable de détecter $2^{k-1}-1$ erreurs et d'en corriger 2^{k-2}. Par exemple avec $k=5$, les paramètres sont $(5,32,16)$.

$\overline{x}$	x	$f(x)$
0	00000	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1	00001	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
2	00010	1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
3	00011	1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
4	00100	1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
5	00101	1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1
6	00110	1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1
7	00111	1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0
8	01000	1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
9	01001	1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1
10	01010	1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1
11	01011	1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0
12	01100	1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1
13	01101	1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0
14	01110	1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0
15	01111	1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1
16	10000	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
17	10001	1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
18	10010	1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
19	10011	1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
20	10100	1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
21	10101	1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
22	10110	1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0
23	10111	1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1
24	11000	1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
25	11001	1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
26	11010	1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0
27	11011	1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1
28	11100	1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0
29	11101	1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1
30	11110	1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
31	11111	1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0

Sur le bilan avantages/inconvénients, cet exemple se situe à l'opposé du premier. Sa redondance croit de manière exponentielle, en revanche ses capacités de détection/correction sont élevées. Cette méthode est donc réservée à des transmissions peu fiables. Une variante de cette méthode

a été utilisée par les sondes Mariner dans leurs missions sur Mars pour communiquer avec la Terre avec un code de paramètres $(6, 32, 16)$:

3° Exemple : variante Mariner

On se fonde, comme précédemment, sur une matrice de Hadamard *H,* mais, cette fois de taille $n = 2^{k-1}$, On définit alors la matrice S de taille $2n \times n = 2^k \times 2^{k-1}$ par $S = \begin{pmatrix} R \\ \overline{R} \end{pmatrix}$ où R est la matrice définie précédemment à partir de H, $\overline{R}$ la matrice définie à partir de $-H$.

Soit 2 lignes $S_{i,\bullet}, S_{i',\bullet}\ (i < i')$ de *S.* L'égalité des accords et des désaccords entre les lignes de *R,* vaut aussi pour R'. On obtient :

$$d\left(S_{i,\bullet}, S_{i',\bullet}\right) = \begin{cases} \dfrac{n}{2} \text{ si } i, i' \in 1 \cdots n \text{ ou si } i, i' \in n+1 \cdots 2n \\ n \text{ si } i' = i + n \\ \dfrac{n}{2} \text{ sinon} \end{cases} \qquad \text{et dans tous les cas } d\left(S_{i,\bullet}, S_{i',\bullet}\right) \geq \frac{n}{2}$$

En définissant *C,* comme l'ensemble des $2n = 2^k$ lignes de S comme précédemment, on a $\delta(C) = \dfrac{n}{2} = 2^{k-2}$. D'où un code de paramètres $\left(k, 2^{k-1}, 2^{k-2}\right)$, ce qui pour $k = 6$ donne les paramètres de Mariner.

Codes linéaires

Avec les codes linéaires, l'alphabet est un corps fini F_q, où $q = p^r$, p nombre premier. Il en ressort que :

1. L'alphabet a une structure de corps.
2. Les ensembles de mots, F_q^k et F_q^n ont une structure d'espace vectoriel su ce corps de dimension respectives *k*, *n*.

Dans cette section, nous adopterons, par habitude, les conventions usuelles de l'algèbre linéaire : les mots étant des éléments d'un espace vectoriel seront écrits comme des vecteurs colonnes.

Pour $k < n$,un code *C* est alors défini comme l'image $Im(g)$ d'une application linéaire injective :

$$F_q^k \xrightarrow{\ g\ } F_q^n$$

C est donc un sous-espace vectoriel de F_q^n de dimension *k*.

Mais, il peut être aussi défini comme le noyau $Ker(h)$ d'une application linéaire surjective :

$$F_q^n \xrightarrow{\ h\ } F_q^{n-k}$$

Le théorème du rang permet d'écrire :

$$Rg\left(h\right) + Dim\left(Ker(h)\right) = Dim\left(F_q^n\right) \Leftrightarrow n - k + Dim\left(Ker(h)\right) = n \Leftrightarrow Dim\left(Ker(h)\right) = k$$

En passant aux matrices correspondantes, on résume par la définition suivante :

Définition

Un code linéaire C de paramètres $(k, n, \delta(C))$ est un sous espace vectoriel de dimension k de F_q^n. Il peut être défini soit par :

- ✓ *une matrice $G \in \mathcal{M}_{n\times k}(F_q)$ de rang k dite <u>matrice génératrice</u> et $C = Im(G)$,*
- ✓ *une matrice $H \in \mathcal{M}_{k\times n-k}(F_q)$ de rang $n-k$ dite <u>matrice de contrôle</u> et $C = Ker(H)$.*

Question de poids

36. Définition

Pour un mot $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in F_q^n$, on appelle :

- ✓ *support de x, l'ensemble $s(x) = \{i \in 1\cdots n \ / \ x_i \neq 0\}$,*
- ✓ *poids de x, $w(x) = |s(x)|$.*

37. Proposition

Le poids w sur F_q^n vérifie :

1. *$w(x) = 0 \Leftrightarrow x = 0$.*
2. *Pour $x \in F_q^n, \alpha \in F_q^*, w(\alpha x) = w(x)$.*
3. *Pour $x, y \in F_q^n$: $w(x+y) \leq w(x) + w(y)$.*

DEMONSTRATION :

1. Évident.
2. Multiplier par un scalaire non nul ne change pas le nombre de termes non nuls dans x.
3. Posons $z = x + y$. Si $i \in s(z)$, comme $z_i = x_i + y_i$, x_i et y_i ne peuvent être tous deux nuls. Donc $i \in s(x) \cup s(y)$ et $s(z) \subseteq s(x) \cup s(y) \Rightarrow w(z) \leq w(x) + w(y)$.

La définition de la distance minimale δ d'un code, se simplifie avec les codes linéaires via les poids :

38. Proposition

La distance de Hamming sur F_q^n vérifie : $d(x, y) = w(x - y)$ et est invariante par translation :

$$\forall\, x, y, z \in F_q^n : \ d(x, y) = d(x + z, y + z)$$

Pour un code linéaire C : $\delta(C) = \min\limits_{\substack{x \in C \\ x \neq 0}} w(x)$

DEMONSTRATION :

Si $d(x, y) = t$, il existe exactement t indices i tels que $x_i \neq y_i$ donc t indices i tels que $x_i - y_i \neq 0$ et $w(x - y) = t$. L'invariance par translation s'en déduit immédiatement.

$\delta(C) = \min\limits_{\substack{x, y \in C \\ x \neq y}} d(x, y) = \min\limits_{\substack{x, y \in C \\ x \neq y}} w(x - y)$, par invariance par translation. Comme C est un sous espace vectoriel, $z = x - y \in C$ et $\delta(C) = \min\limits_{\substack{z \in C \\ z \neq 0}} w(z)$.

Remarque :

Si $Dim(C)=k$, $|C|=q^k$, la définition initiale de $\delta(C)$ amenait à déterminer la distance minimale de $q^k \times q^k - q^k$ couples d'éléments de C. La nouvelle formule revient à déterminer le poids minimal de $q^k - 1$. C'est encore beaucoup, mais c'est mieux…

39. Proposition inégalité de Singleton

Soit C un code linéaire de paramètres (k,n,δ), *alors* $\delta \le n-k+1$.

DEMONSTRATION :

Soit A le sous-espace de F_q^n formé des vecteurs dont les $k-1$ premières coordonnées sont nulles. Il est de dimension $n-k+1$. Par ailleurs $x \in A \Rightarrow w(x) \le n-(k-1) = n-k+1$.

Comme que le sous-espace A est de dimension $n-k+1$ et le sous-espace C de dimension k, le sous -espace vectoriel $A \cap C$ n'est pas réduit à $\{0\}$. Il existe donc un vecteur x non nul tel que :

1. $x \in A \Rightarrow w(x) \le n-k+1$
2. $x \in C \Rightarrow \delta \le w(x)$

D'où : $\delta \le n-k+1$.

40. Proposition

Soit un code linéaire C de paramètres (k,n,δ) *et de matrice de contrôle H, alors* δ *est la longueur minimale d'une liste de colonnes de H liée.*

DEMONSTRATION :

Soit $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in F_q^n$, $H\,x = \sum_{j=1}^{n} x_j H_{\bullet,j} = \sum_{j \in s(x)} x_j H_{\bullet,j}$.

Soit $x \in C$.

$x \in C \Leftrightarrow \sum_{j \in s(x)} x_j H_{\bullet,j} = 0$. Par définition de $s(x)$, $x_j \in s(x) \Leftrightarrow x_j \neq 0$. Donc la liste $\left(H_{\bullet,j}\right)_{j \in s(x)}$ de longueur $w(x) = |s(x)|$ est liée. Dans C il existe un y de poids minimal $\delta = w(y)$. Donc il existe une liste liée de longueur δ.

Supposons qu'il existe une partie D de $1 \cdots n$, ayant moins de δ éléments telle que telle que $\left(H_{\bullet,j}\right)_{j \in D}$ soit liée. On aurait alors $\sum_{j \in D} \alpha_j H_{\bullet,j} = 0$ avec les α_i non tous nuls. Si on définit le mot $z \in F_q^n$ par $z_i = \begin{cases} \alpha_i \text{ si } i \in D \\ 0 \text{ sinon} \end{cases}$, on a $H\,z = \sum_{j=1}^{n} z_j H_{\bullet,j} = 0 \Rightarrow z \in C$. En contradiction avec $w(z) \le |D| < \delta$.

Toute liste de colonnes de H de longueur $< \delta$ est donc libre.

Exemple :

Les codes « Mariner » définis en amont étaient fondés sur une matrice de Hadamard mais n'utilisait pas la structure d'espace vectoriel sur $\mathbb{Z}_2$. Voici un exemple de code linéaire fondé sur une matrice de Hadamard.

Vocabulaire et notations :

Un vecteur $V \in F_2^n$ sera dit de type (a,b) si il est constitué par une alternance de « paquets » de a « 1 » et de a « 0 » en commençant par les « 1 ». Le nombre de paquets étant égal à b, on a $n = a \times b$.

$$\textit{Exemples :} \begin{pmatrix}1\\1\\1\\1\end{pmatrix} \text{ de type } (4,1), \begin{pmatrix}1\\1\\0\\0\end{pmatrix} \text{ de type } (2,2), \begin{pmatrix}1\\0\\1\\0\end{pmatrix} \text{ de type } (1,4).$$

Pour simplifier les écritures, dans l'énoncé et la démonstration qui vont suivre, les lignes et colonne des matrices seront numérotées à partir de 0.

Si M est une matrice (ou un vecteur) à coefficients dans F_2, $\overline{M}$ désigne la matrice obtenue par inversion des 0 et des 1.

41. Proposition

Soit $R_k \in \mathcal{M}_{2^k \times 2^k}(F_2)$ la matrice obtenue à partir d'une matrice de Hadamard-Walsh en remplaçant les « -1 » par des « 0 ». Soit, pour $j \in 0 \cdots 2^k - 1$, V_j^k la colonne j de R_k. Alors :

1. *V_0^k est de type $(2^k, 1)$. Et pour $j \in \{2^0, 2^1, \cdots, 2^{k-1}\}$, V_j^k est de type $(j, 2^k / j)$*
2. *La liste $(V_0^k, V_1^k, V_2^k, \cdots, V_{2^{k-1}}^k)$ est libre et $C = Vec(V_0^k, V_1^k, V_2^k, \cdots, V_{2^{k-1}}^k)$ est de dimension $k+1$.*
3. *$\delta(C) = 2^{k-1}$*

DEMONSTRATION :

En préambule, pour illustrer et éclaircir, voici la situation pour $k = 4$:

(16,1)	(1,16)	(2,8)		(4 ,4)				(8,2)							
0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1
1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1
1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1
1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	0
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0
1	1	0	0	0	0	1	1	0	0	1	1	1	1	0	0
1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1

Récurrence sur k :

Pour $k=2$, où les trois vecteurs sont : $V_0^2=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, V_1^2=\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, V_2^2=\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$ l'énoncé se vérifie aisément.

$\mathcal{H}_k \Rightarrow \mathcal{H}_{k+1}$

$$R_{k+1}=\left(\begin{array}{c|c} R_k & R_k \\ \hline R_k & \overline{R_k} \end{array}\right)$$

(colonnes indexées $0 \ldots\ldots j \ldots\ldots \mid 2^k \ldots 2^{k+1}-1$; lignes indexées $0, i, \ldots, 2^k, \ldots, 2^{k+1}-1$)

1. On va montrer que pour $j\in\left\{0, 2^0, 2^1, \cdots, 2^{k-1}, 2^k\right\}$, V_j^k est de type $\left(j, 2^{k+1}/j\right)$ en distinguant 3 cas :

   a) $j=0$. Alors $V_0^{k+1}=\begin{pmatrix}V_0^k\\ \hline V_0^k\end{pmatrix}$ ne contient que des 1 et est du type voulu.

   b) $j\in\left\{2^0, 2^1, \cdots, 2^{k-1}\right\}$, alors $V_j^{k+1}=\begin{pmatrix}V_j^k\\ \hline V_j^k\end{pmatrix}$. La taille des paquets ne change pas mais leur nombre est doublé d'où un type $\left(j, 2^{k+1}/j\right)$.

   c) $j=2^k$. Alors $V_{2^k}^{k+1}=\begin{pmatrix}V_0^k\\ \hline \overline{V_0^k}\end{pmatrix}=\begin{pmatrix}1\\ \vdots\\ 1\\ \hline 0\\ \vdots\\ 0\end{pmatrix}$ d'où un type $\left(2^k, 2\right)$

2. Liberté de $\left(V_0^{k+1}, V_1^{k+1}, V_2^{k+1}, \cdots, V_{2^k}^{k+1}\right)$

$$\sum_{j\in\left\{0, 2^0, 2^1, \cdots, 2^{k-1}, 2^k\right\}} \alpha_j V_j^{k+1}=0 \Leftrightarrow \sum_{j\in\left\{0, 2^0, 2^1, \cdots, 2^{k-1}\right\}} \alpha_j \begin{pmatrix}V_j^k\\ \hline V_j^k\end{pmatrix}+\alpha_{2^k}\begin{pmatrix}1\\ \vdots\\ 1\\ \hline 0\\ \vdots\\ 0\end{pmatrix}=0$$

$$\Rightarrow \sum_{j\in\left\{0, 2^0, 2^1, \cdots, 2^{k-1}\right\}} \alpha_j V_j^k=0$$

Selon l'hypothèse de récurrence, liberté de $\left(V_0^k, V_1^k, V_2^k, \cdots, V_{2^{k-1}}^k\right)$, tous les α_j pour $j \in \left\{0, 2^0, 2^1, \cdots, 2^k - 1\right\}$ sont nuls. Il reste alors $\alpha_{2^k}\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix} = 0$. D'où la nullité de α_{2^k}.

3. Poids des vecteurs de $C = Vec\left(V_0^{k+1}, V_1^{k+1}, V_2^{k+1}, \cdots, V_{2^{k-1}}^{k+1}, V_{2^k}^{k+1}\right)$. Pour $X \in C$ on distinguera 2 cas :

   a) $X \in Vec\left(V_0^{k+1}, V_1^{k+1}, V_2^{k+1}, \cdots, V_{2^{k-1}}^{k+1}\right)$. Alors :

   $$X = \sum_{j \in \left\{0,\, 2^0,\, 2^1,\, \cdots,\, 2^{k-1},\, 2^k\right\}} \alpha_j V_j^{k+1} = \sum_{j \in \left\{0,\, 2^0,\, 2^1,\, \cdots,\, 2^{k-1},\, 2^k\right\}} \alpha_j \begin{pmatrix} V_j^k \\ V_j^k \end{pmatrix} = \begin{pmatrix} X' \\ X' \end{pmatrix} \text{ où } X' \in Vec\left(V_0^k, V_1^k, V_2^k, \cdots, V_{2^{k-1}}^k\right).$$

   Selon l'hypothèse de récurrence le poids $w(X') \geq 2^{k-1}$ et donc $w(X) \geq 2^k$.

   b) $X = Y + V_{2^k}^{k+1}$, $Y \in Vec\left(V_0^{k+1}, V_1^{k+1}, V_2^{k+1}, \cdots, V_{2^{k-1}}^{k+1}\right)$.

   Selon le a) $Y = \begin{pmatrix} Y' \\ Y' \end{pmatrix}$. En posant $w(Y') = d$, et en additionnant $\begin{pmatrix} Y' \\ Y' \end{pmatrix} + \begin{pmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, on obtiendra

   $2^k - d$ « 1 » au « nord » et d « 1 » au « sud » donc $w(Y) = 2^k$.

Avec les notations de la proposition précédente on peut alors affirmer :

42. Corollaire

Le code linéaire défini par la matrice génératrice :

$$G = \left(V_0^k \mid V_1^k \mid V_2^k \mid \cdots \mid V_{2^{k-1}}^k\right) \in \mathcal{M}_{2^k \times (k+1)}(F_2)$$

a pour paramètres : $\left(k+1, 2^k, 2^{k-1}\right)$.

REMARQUE :

Si l'on considère la matrice $H \in \mathcal{M}_{\left(2^k - k - 1\right) \times 2^k}(F_2)$ transposée de la matrice obtenue à partir de R_k en excluant les colonnes appartenant à G, alors $H \times G = 0$. En effet, ce produit matriciel utilise des colonnes distinctes C et C' de R_k et l'on sait (Cf. démonstration proposition 34) qu'entre ces deux colonnes, on a $2^{k-2}\begin{pmatrix}0\\0\end{pmatrix}, 2^{k-2}\begin{pmatrix}1\\0\end{pmatrix}, 2^{k-2}\begin{pmatrix}0\\1\end{pmatrix}, 2^{k-2}\begin{pmatrix}1\\1\end{pmatrix}$. De sorte que $C^t C' = 2^{k-2} = 0$ dans F_2.

Par conséquent $Im(G) \subseteq Ker(H)$. Il reste à prouver l'égalité pour avoir une matrice de contrôle, mais je n'y suis parvenu… pour l'instant.

À suivre…

Notations

Notations générales

$\lvert E\rvert$	Nombre d'éléments d'un ensemble fini E.
$m\cdots n$	ensemble des entiers i $m\leq i\leq n$
$\lfloor x\rfloor$	Partie entière d'un réel x.

Algèbre

$A[X]$	Anneau (et espace vectoriel) des polynômes sur l'anneau A.
$A_n[X]$	Sous-espace vectoriel des polynômes de degré $\leq n$
$\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n$	Anneau (corps si n premier) des entiers modulo n.
F_q	Corps fini de $q=p^r$ éléments, p premier.
A/I	Quotient de l'anneau A par l'idéal I.
aA, (a)	Idéal principal de l'anneau A engendré par a.

Algèbre linéaire

$Vec(A)$	Le sous-espace engendré par une partie A d'un espace vectoriel E.
$Vec(e_{1,}\cdots e_n)$	Le sous-espace engendré par $\{e_{1,}\cdots e_n\}$.
$Dim(E)$	La dimension d'un espace vectoriel de dimension finie.
$X_{\boldsymbol{b}}$ $C_{\boldsymbol{b}}(x)$	Les coordonnées d'un vecteur x d'un espace vectoriel E muni d'une base $\boldsymbol{b}$.
$\mathcal{L}(E,F)$	L'espace vectoriel des applications linéaires de E vers F.
$\mathcal{L}(E)$	L'espace vectoriel (et anneau) des endomorphismes de E.
$\mathcal{M}_{n,p}(K)$	L'espace des matrices de n lignes et p colonnes
$\mathcal{M}_n(K)$	L'espace des matrices carrées de n lignes et n colonnes
$\mathrm{GL}(E)$, $\mathrm{GL}_n(K)$	Groupe linéaire général
$\left(a_{i,j}\right)_{\substack{i=1\cdots n\\ j=1\cdots p}}$	Matrice de taille $n\times p$ ayant pour terme $a_{i,j}$ en ligne i, colonne j.
$a_{i,j}$ $A_{i,j}$	Le terme de la matrice A situé en ligne i, colonne j
$A_{i,\bullet}$	La ligne i de la matrice A.
$A_{\bullet,j}$	La colonne j de la matrice A.
$Im(f)$, $Im(A)$	L'image d'une application linéaire f, d'une matrice A.
$Ker(f)$, $Ker(A)$	Le noyau d'une application linéaire f, d'une matrice A.
$Rg(f)$, $Rg(A)$	Le rang d'une application linéaire f, d'une matrice A.
$M_{\boldsymbol{c},\boldsymbol{b}}(f)$	La matrice de l'application linéaire f dans la base $\boldsymbol{b}$ de départ et $\boldsymbol{c}$ d'arrivée.

$M_{\boldsymbol{b}}(f)$	La matrice de l'endomorphisme f dans la base $\boldsymbol{b}$.
E_i	Le vecteur de la base canonique de K^n dont tous les termes sont nuls sauf le $i^{ème}$.
I ou I_n	La matrice identité de $\mathcal{M}_n(K)$.
U ou U_n	Le vecteur de K^n dont toutes les coordonnées sont égales à 1.
J ou J_n	$J_n = U_n U_n^t$ matrice de $\mathcal{M}_n(K)$ dont tous les termes valent 1.
id ou id_n	L'endomorphisme identité d'un espace de dimension n.
$Tr(A), Tr(f)$	La trace d'une matrice carrée A, d'un endomorphisme f.
$F+G$	Somme des sous-espaces F et G.
$F \oplus G$	Somme directe des sous-espaces (ou espaces) F et G.
$f \oplus g$, $A \oplus B$	Somme directe des applications linéaires f et g, des matrices A et B.
A^t	La matrice transposée de la matrice A.
f^t	La transposée de l'application linéaire f.
$Diag(d_1, \cdots d_n)$	Matrice diagonale.
$E*$	L'espace dual de E.
$\langle \varphi ; x \rangle$	La valeur d'une forme linéaire $\varphi \in E*$ sur un vecteur $x \in E$.
$Det_{\boldsymbol{b}}(x_1, \cdots, x_n)$	Déterminant d'une liste de vecteurs dans une base $\boldsymbol{b}$.
$Det(A)$, $\lvert A \rvert$	Déterminant de la matrice carrée A.
$Det(f)$, $\lvert f \rvert$	Déterminant de l'endomorphisme f.
$x \perp y$, $G \perp H$	Orthogonalité de vecteurs, de sous-espaces.
$F^{\perp}$	Le supplémentaire orthogonal du sous-espace F
$\langle x ; y \rangle$	Produit scalaire des vecteurs x et y.
$\lVert x \rVert_2$	Norme euclidienne du vecteur x.
$O(E), O(n)$	Groupe orthogonal alias groupe des isométries de E ($K = \mathbb{R}$).
$A*$	Matrice ajointe de A ($= \overline{A}^t$).
$U(E), U(n)$	Groupe unitaire alias groupe des isométries de E ($K = \mathbb{C}$).
$Spec(f), Spec(A)$	Ensemble des valeurs propres d'un endomorphisme f, d'une matrice A.
$C_f(X), C_A(X)$	Polynôme caractéristique d'un endomorphisme f, d'une matrice A.
E_λ	Sous-espace propre associé à une valeur propre λ
$P(f)$	Polynôme P appliqué à l'endomorphisme f.
$K[f]$	L'algèbre (commutative) des polynômes de l'endomorphisme f.
$f*$	Application adjointe de f.

Bibliographie sommaire

1 Bachoc C., *Cours de codes,* Université de Bordeaux I (UE Codes/Signal).
http://www.ufr-mi.u-bordeaux.fr/CSI/Cours/code.pdf

2 Cellier J., *Algèbre linéaire*, PUR 2008.

3 Coste L., Paugam A., Quarez R., *Codes Correcteurs*, Université de Rennes I.
http://dyna.maths.free.fr/docs/lecons/developpement_algebre_370.pdf

4 Eliahou S., *La conjecture de Hadamard (I) et (II),* Image des Mathématiques.
https://images.math.cnrs.fr/La-conjecture-de-Hadamard-I.html

5 Escoffier JP. *Théorie de Galois*, Masson 1997

6 Goethals J.M.,. Seidel J.J, *Orthogonal matrices with zero diagonal.ii,* Can.J.Math., Vol.XXIII, No.5, 1971, pp.816-832.
http://mathscinet.ru/files/OneZeroDiagonalII.pdf

7 Masahiko Miyamoto, *A construction of Hadamard matrices*, Journal of Combinatorial Theory, Series A Volume57, Issue1, May 1991, Pages 86-108.
https://www.sciencedirect.com/science/article/pii/0097316591900085/pdf?md5=8080b4c9e7ba8cee8b206a69267a7d6b&pid=1-s2.0-0097316591900085-main.pdf

8 Mathon R. , *Symmetric conference matrices of order* pq^2+1*,* Can. J. Math., Vol. XXX, No. 2, 1978, pp. 321-331.
http://mathscinet.ru/files/MathonR.pdf

9 Mercier DJ. , *L'algèbre dans la correction des erreurs.*
https://hal.univ-antilles.fr/hal-00764247/

10 Parvathy S., *Theory Of Block Designs*, Indian Institute of Science Education and Research, Mohali.
https://www.isibang.ac.in/~sury/parvathy.pdf

11 Seberry, J.R.,Wysocki, B.J.,Wysocki, T.A., *On some applications of Hadamard matrices*, University of Wollongong
https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1603&context=infopapers

12 Suk Joon, Michael Hwang, *Application of Balanced Incomplete Block Designs in Error Detection and Correction.*
https://www.researchgate.net/publication/319621339_Application_of_Balanced_Incomplete_Block_Designs_in_Error_Detection_and_Correction
Steepleton Jacob, *Constructions of Hadamard Matrices,* April 27,2019.

13 Zemor G., *Arithmétique 1: corps finis et applications.*
http://www.math.u-bordeaux.fr/~zemor/arit06.pdf

14 Zemor Gilles, *Master CSI, Arithmétique 1: corps finis et applications*, 11 décembre 2006.
http://www.math.u-bordeaux.fr/~zemor/arit06.pdf