Université de Lille

Master 1 Mathématiques Appliquées, Statistiques

Travail Encadré de Recherche

Matrices de Hadamard et Applications.

Paul Maire

Professeur Encadrant :
Thomas Simon

12 mai 2018

Table des matières

Remerciements

Pour la réalisation et la rédaction de ce mémoire, je tiens avant tout à remercier mon professeur, Mr. Thomas Simon, pour avoir été à l'écoute et répondu à mes questions.

Introduction

Il est bien connu que ce qui fait une partie de la beauté des mathématiques, est son incroyable unité et sa capacité d'intéraction entre des domaines qui, a priori, ne semblaient pas nécessairement liés, mais qui se trouvent l'être bien plus que ce que l'on pensait. C'est ici une illustration de ce fait qui sera mise en évidence. Dans ce mémoire seront abordées les matrices d'Hadamard et ses applications. Tout d'abord, nous nous attarderons sur les plans d'expérience en blocs équilibrés incomplets, qui se trouvent être à l'origine des matrices d'Hadamard, et nous verrons dans quelle mesure ces deux notions sont liées. Subséquemment, nous nous intéresserons à quelques résultats mathématiques simples liés à l'existence de matrices d'Hadamard d'ordre donné et établirons un état des lieux sur le sujet. Pour finir, notre regard se tournera sur une des applications des travaux d'Hadamard que sont les codes, et nous permettrons quelques digressions sur le sujet.

Chapitre 1

Plan d'expérience en blocks équilibrés incomplets

Nous allons aborder dans ce chapitre la notion de plan d'expérience en blocs équilibrés incomplets, en nous intéressant à certaines familles singulières de tels plans, tels que les plans complémentaires ou les plans projectifs finis (PPF). On abordera également dans ce chapitre les matrices d'incidence et les implications qu'apportent leurs propriétés, ainsi que les système triple de steiner (STS). Tout ceci est une base nécessaire pour nous diriger ensuite vers l'étude des matrices et plans d'Hadamard, et leur utilisation dans la construction de codes binaires et correcteurs d'erreurs.

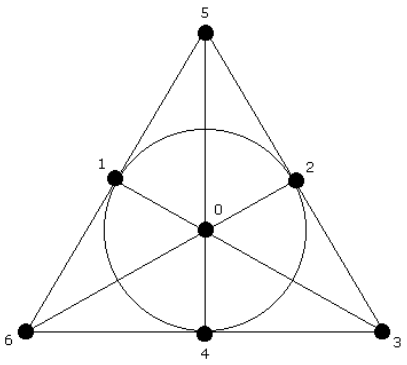
1.1 Définition et exemples

Démarrons par un exemple, afin d'avoir une vision un peu plus claire des choses : Sept golfeurs passent une semaine de vacances en bord de mer, dans une ville où se trouvent deux parcours de golf. Ils décident que chacun devrait faire une partie de golf chaque jour. Ils décident aussi que chaque jour, ils devraient se séparer en deux groupes, un groupe de 3 qui jouerait sur un parcours, et un autre de 4 qui jouerait sur l'autre. La question est la suivante : les groupes peuvent-ils être arrangés de telle sorte que chaque paire de golfeurs joue ensemble dans le groupe de 3 le même nombre de fois, et le même nombre de fois également dans le groupe de 4 ? (Pas nécessairement le même nombre de fois ET dans le groupe de 3 ET dans le groupe de 4)

Voici une solution :

$$
\begin{array}{ll}
\text{Jour 1} & \{1,2,4\}\,\{3,5,6,7\} \\
\text{Jour 2} & \{2,3,5\}\,\{4,6,7,1\} \\
\text{Jour 3} & \{3,4,6\}\,\{5,7,1,2\} \\
\text{Jour 4} & \{4,5,7\}\,\{6,1,2,3\} \\
\text{Jour 5} & \{5,6,1\}\,\{7,2,3,4\} \\
\text{Jour 6} & \{6,7,2\}\,\{1,3,4,5\} \\
\text{Jour 7} & \{7,1,3\}\,\{2,4,5,6\}
\end{array}
$$

On vérifie facilement que chaque paire de golfeurs joue ensemble 1 fois dans le groupe de 3, et 2 fois dans le groupe de 4. Ce qui a été utilisé ici est la configuration dîte du Plan à 7 points, illustré par la figure suivante :



On constate dans cette figure qu'il y a 7 points et 7 lignes, chaque ligne contenant 3 points, et chaque paire de points étant dans exactement une ligne. Les groupes de taille 4 sont les complémentaires des lignes de cette configuration.
Donnons donc maintenant une définition formelle de ce qu'on appelle un plan d'expérience en blocs équilibrés incomplets (Balanced Incomplete Block Design, BIBD) :

Définition : Un plan (v, k, λ) est une collection de sous-ensembles à k-éléments (appelés blocs) d'un ensemble S à v éléments, avec $k < v$, telle que chaque paire d'éléments de S se retrouvent ensemble dans exactement λ blocs. Par cette définition, on se rend donc compte que le plan à 7 points est donc enfait un plan $(7, 3, 1)$. Le plan à 7 points rentre enfait dans une catégorie plus large que l'on va développer dans la section suivante, les Systèmes Triple de Steiner (STS), tout comme les plans affines d'ordre 3, qui sont enfait des plans $(9, 3, 1)$.

1.2 STS : Système Triple de Steiner

Définition : Un plan $(v, 3, 1)$ est appelé un Système Triple de Steiner d'ordre v, on le note $STS(v)$, et ces systèmes n'existent que pour certaines valeurs de v. En effet, regardons d'abord quelques résultats généraux :

Théorème 1.2.1 : On suppose que le plan (v, k, λ) possède b blocs. Alors, chaque élément se trouve dans précisément r blocs, avec :

$$\lambda(v-1) = r(k-1) \text{ et } bk = vr$$

Preuve : On prend n'importe quel élément x, et l'on suppose qu'il se trouve dans r blocs. Dans chacun de ces r blocs, il forme une paire avec $k-1$ autres éléments . On va donc trouver finalement $r(k-1)$ paires dans les blocs où se trouvent x. Mais x forme également une paire avec chacun des $v-1$ autres éléments λ fois, donc le nombre de paires où se trouvent x est également égal à $\lambda(v-1)$. D'où $\lambda(v-1) = r(k-1)$.Il est démontré que r ne dépend pas du choix de x, puisqu'uniquement déterminé par v,, k, et λ.

Pour montrer que $bk = vr$, notons d'abord que chaque bloc a k éléments, et donc les b blocs contiennent bk éléments au total (en comptant les répétitions). Mais chaque élément x se trouve r fois dans les blocs, ce qui implique par nécessité $bk = vr$.

De ce théorème vient donc le résultat suivant :

Théorème 1.2.2 : Un STS(v) n'existe que si v $\equiv 1$ *ou* 3 (mod 6).

Preuve : On suppose qu'un plan $(v, 3, 1)$ existe. Alors, $v - 1 = 2r$ et $3b = vr$, ce qui amène $v = 2r + 1$ et $b = \frac{1}{6}v(v-1)$. Si $v = 6u + 5$ alors $b = \frac{1}{6}(6u+5)(6u+4)$ n'est pas un entier, alors il faut v $\equiv 1$ *ou* 3 (mod 6).

Ces systèmes prennent leur appellation de Steiner, qui les a abordé dans un papier en 1953, mais l'équivalence de ce résultat, qui est donc un résultat plus fort, avait déjà été démontrée en 1847, par Kirkman. Le $STS(7)$ mentionné auparavant est finalement construit en partant du bloc $\{1, 2, 4\}$, auquel est rajouté 1 à chaque composante, en travaillant modulo 7. Le pourquoi de cette construction sera expliqué ultérieurement.
Les progrès effectués dans le domaine de ces plans et modèles a grandement été aidé par leur représentation matricielle. Ce qui nous amène à notre paragraphe suivant !

1.3 Matrice d'incidence et implications

La matrice d'incidence d'un plan (v, k, λ) est la matrice $\mathcal{A}$=(a_{ij}) de taille $b \times v$ définie telle que :

$$a_{ij} = \begin{cases} 1 & \text{si le i-ème bloc contient le j-ème élément,} \\ 0 & \text{sinon.} \end{cases}$$

Illustrons cette définition par un exemple. La matrice d'incidence du plan à 7 points, obtenu avec les blocs $\{1, 2, 4\}, \{2, 3, 5\}, ..., \{7, 1, 3\}$:

$$\mathcal{B} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{R}^{7\times 7}$$

En effet, la $1^{ère}$ ligne comporte des 1 aux positions 1, 2, et 4, le premier bloc étant $\{1, 2, 4\}$, et ainsi de suite. Les lignes correspondent aux blocs, et les colonnes aux éléments. Enfin, on remarque que la matrice $\mathcal{A}$ dépend finalement de l'ordre dans lequel les blocs et les éléments sont pris, même si on verra que l'ordre n'influe pas sur les propriétés de A, auxquelles nous allons désormais nous intéresser.

Théorème 1.3.1 : $\mathcal{A}$ matrice d'incidence d'un plan (v, k, λ), alors :

$$\mathcal{A}^T\mathcal{A} = (r - \lambda)\mathcal{I} + \lambda\mathcal{J}$$

, avec $\mathcal{J}$ la matrice de taille $v \times v$ uniquement composée de 1, et le r précédemment évoqué.

Preuve : La (i, j)-ème entrée de la matrice $\mathcal{A}^T\mathcal{A}$ est le produit scalaire entre la ième ligne de $\mathcal{A}^T$ et la jème colonne de $\mathcal{A}$, autrement dit entre la ième et la jème colonne de $\mathcal{A}$. Ainsi, la (i, i)-ème coordonnée, sur la diagonale, est le produit scalaire entre la ième colonne et elle-même, tout comme le nombre de 1 dans la ième colonne. Mais cela représente également le nombre de blocs contenant le ième élément, soit r.

Si $i \neq j$, le produit scalaire de la ième et jème colonne est le nombre d'endroits où ces deux colonnes possèdent un 1. Cela correspond au nombre de blocs contenant à la fois le ième et le jème, qui est λ. Donc tous termes diagonaux de la matrice $\mathcal{A}^T\mathcal{A}$ sont égaux à r, et tous les termes non-diagonaux sont égaux à λ. .

La matrice d'incidence est aussi utilisée pour démontrer le résultat suivant (dont on admettra la preuve) :

Théorème 1.3.2 : Dans chaque plan (v, k, λ), on a $v \leq b$.

De plus, un plan (v, k, λ) est dit symétrique lorsque $b = v$, avec toujours b le nombre de blocs. Des résultats précédents, si $b = v$, alors $r = k$ et ainsi $\lambda(v - 1) = k(k - 1)$ et $\mathcal{A}^T\mathcal{A} = (k - \lambda)\mathcal{I} + \lambda\mathcal{J}$. Le caractère "symétrique" vient des propriétés suivantes, qui elles-mêmes viennent du fait que $r = k$:
-Chaque bloc contient k éléments ; chaque élément est dans k blocs.
-Chaque paire d'éléments se trouve dans λ blocs.
-Chaque paire de blocs s'intersectent en λ éléments, *ie* le nombre d'éléments qu'ils partagent (la preuve de cette dernière assertion se trouvera en annexe).

Nous vient donc le théorème suivant :

Théorème 1.3.3 : Si $\mathcal{A}$ est la matrice d'incidence d'un plan symétrique, alors $\mathcal{A}^T\mathcal{A} = \mathcal{A}\mathcal{A}^T$.

Preuve : Comme $\mathcal{A}\mathcal{J} = k\mathcal{J}$ et $\mathcal{J}\mathcal{A} = r\mathcal{J}$, il vient, du fait que $r = k$, que $\mathcal{J}\mathcal{A} = \mathcal{A}\mathcal{J}$, soit $\mathcal{A}$ qui commute avec $\mathcal{J}$. Ce qui amène que $\mathcal{A}$ commute avec $(k - \lambda)\mathcal{I} + \lambda\mathcal{J} = \mathcal{A}^T\mathcal{A}$. Ainsi, $\mathcal{A}\mathcal{A}^T = \mathcal{A}\{(k - \lambda)\mathcal{I} + \lambda\mathcal{J}\}\mathcal{A}^{-1} = \{(k - \lambda)\mathcal{I} + \lambda\mathcal{J}\}\mathcal{A}\mathcal{A}^{-1} = (k - \lambda)\mathcal{I} + \lambda\mathcal{J} = \mathcal{A}^T\mathcal{A}$. .

On remarque enfin que, dans le cas d'un plan symétrique, si on prend $\mathcal{A}$ la matrice d'incidence de ce dît plan, alors $\mathcal{A}^T$ est également matrice d'incidence d'un plan symétrique, appelé le plan **dual**. Par exemple, en revenant à l'exemple du plan à 7 points évoqué plus haut, $\mathcal{A}^T$ est la matrice d'incidence du plan à 7 points composé des blocs $\{1, 5, 7\}, \{1, 2, 6\}, \{2, 3, 7\}, \{1, 3, 4\}, \{2, 4, 5\}, \{3, 5, 6\}, \{4, 6, 7\}$ (*onremarqu* $7{,}2 \to 6{,}...{,}7 \to 1$, on en revient au plan à 7 points initial).

1.4 Plans complémentaires

Définition : Soit $\mathcal{D}$ un modèle (v, k, λ). On appelle modèle complémentaire $\overline{\mathcal{D}}$ un plan dont les blocs sont les complémentaires des blocs de $\mathcal{D}$. Dans l'exemple du problème des golfeurs, les blocs de taille 4 forment les blocs complémentaires de ceux du plan à 7 points, et l'ensemble forme donc le plan complémentaire au plan à 7 points.

Théorème 1.4.1 : Soit $\mathcal{D}$ un modèle (v, k, λ) sur l'ensemble $\mathcal{S}$, constitué des blocs $B_1,...,B_d$. Alors les ensembles $\overline{B_i} = \mathcal{S}\backslash\{B_i\}$ forment un plan $(v, v - k, \lambda')$, avec $\lambda' = b - 2r + \lambda$, λ' positif.

Preuve : Comme $|B_i| = k$ pour tout i, il est clair que $|\overline{B_i}| = v - k$ pour tout i. On doit montrer

que toutes paires d'éléments de $\mathcal{S}$ se trouve en exactement λ' des blocs $\overline{B_i}$. Maintenant, si $x, y \in \mathcal{S}$, alors $x, y \in \overline{B_i}$ précisément lorsque ni x ni y n'appartiennent à B_i. Mais par le principe d'inclusion-exclusion, le nombre de blocs B_i ne contenant ni x ni y vaut : $b -$ (nombre de blocs contenant x) $-$ (nombre de blocs contenant y) + (nombre de blocs contenant à la fois x et y) $= b - 2r + \lambda$.

Théorème 1.4.2 : Le complémentaire d'un plan symétrique est lui aussi symétrique, selon la définition de symétrie donnée précédemment.

Preuve : Si $\mathcal{D}$ est symétrique, alors $b = v$, et donc $\overline{\mathcal{D}}$ a également $b = v$ blocs.

1.5 plan solvables et Plans Projectifs Finis (PPF)

Définition : Un modèle (v, k, λ) sur l'ensemble $\mathcal{S}$ est **solvable** si les blocs peuvent être arrangés en r groupes de telle sorte que chaque groupe forme une partition de $\mathcal{S}$. Les groupes sont ensuite appelés classes parallèles ou de résolution.

Remarques : Un plan solvable ne peut exister que si k divise v. De plus, il faut qu'il y ait précisemment r groupes car : chaque élément se trouve dans r blocs, et doit se trouver dans exactement un bloc de chaque groupe.

Théorème 1.5.1 : Tout modèle $(n^2, n, 1)$ est solvable.

Preuve : Admise.

Après avoir vu ce qu'était que la notion de plan solvable, regardons celle de Plan Projectif Fini (PPF).

Définition : Pour $n \neq 2$, un plan projectif fini (PPF) d'ordre n est un plan $(n^2 + n + 1, n + 1, 1)$. On fera référence dans la suite aux plans projectifs finis par l'appellation PPF.

Il vient donc que dans un PPF, on a le même nombre de blocs et d'éléments. Ils copient finalement les lignes et les points d'une géométrie. En effet, quelque soient deux blocs (lignes), ils s'intersectent en un élément (point), et chaque paire de points se trouve sur une unique ligne. Le plan à 7 points est enfait un PPF d'ordre 2.

Regardons ensuite deux résultats intéressants sur ces plans projectifs finis :

Théorème 1.5.2 : Il existe un plan projectif fini d'ordre $n \Leftrightarrow$ Il existe un plan affine d'ordre n.

Preuve : Admis.

Théorème 1.5.3 : Les PPFs d'ordre n, avec n puissance positive d'un nombre premier, existent.

Preuve : Admis.

Il a été conjecturé que si n n'est pas puissance positive d'un nombre premier, alors il n'existe pas de PPF d'ordre n. Le résultat a été confirmé pour $n = 6$ et $n = 10$, mais est toujours sujet à la reflexion concernant $n = 12$.

Chapitre 2

Matrices et plans d'Hadamard

Au vu de tous les résultats évoqués dans le premier chapitre, nous avons désormais les outils nécessaires pour nous pencher sur les plans et matrices d'Hadamard, que nous allons donc étudier dans ce second chapitre.

2.1 Définition d'une matrice d'Hadamard et propriétés

Définition : Une matrice $\mathcal{H}$ $(+1, -1)$ est une matrice dont toutes les composantes sont $+1$ ou -1. Une matrice $(+1, -1)$ de taille $n \times n$ est une matrice d'Hadamard d'ordre n si $\mathcal{H}^T\mathcal{H} = \mathcal{H}\mathcal{H}^T = n\mathcal{I}$ (ce qui implique que $\mathcal{H}$ est inversible, d'inverse $\mathcal{H}^{-1} = \frac{1}{n}\mathcal{H}^T$).

De plus, $\mathcal{H}^T\mathcal{H} = n\mathcal{I}$ implique que n'importe quelles deux lignes de $\mathcal{H}$ sont orthogonales. L'égalité $\mathcal{H}\mathcal{H}^T = n\mathcal{I}$ implique elle l'orthogonalité de n'importe quelles deux colonnes de $\mathcal{H}$.

Les matrices d'Hadamard sont ainsi nommées suite aux travaux de Jacques Hadamard. En effet, en 1893, Hadamard a montré que n'importe quelle matrice $\mathcal{H}=(h_{ij})$ de taille $n \times n$ telle que $|(h_{ij})| \leq 1$ a un déterminant qui vaut au plus $n^{n/2}$, avec égalité seulement si $\mathcal{H}\mathcal{H}^T = n\mathcal{I}$. Depuis, comme on le verra dans le chapitre 3, les matrices d'Hadamard ont été utilisé dans de nombreux domaines des combinatoires, et ont été par exemple à l'origine de l'envoi de photographies encodées envoyées depuis Mars en direction de la Terre.

Intéressons-nous maintenant à la construction d'une telle matrice. Peut-on en faire de tout ordre ? Comment conserver la propriété exprimée ci-dessus ?

Pour construire des matrices d'Hadamard d'ordre 2^m, on a la méthode de construction par récurrence suivante :

On pose $\mathcal{H}_0$ la matrice de taille 1×1 avec donc comme seule composante 1, et $\mathcal{H}_1$ la matrice $\mathcal{H}_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Ainsi, pour tout $m \geq 1$, on définit $\mathcal{H}_m = \begin{pmatrix} \mathcal{H}_{m-1} & \mathcal{H}_{m-1} \\ \mathcal{H}_{m-1} & -\mathcal{H}_{m-1} \end{pmatrix}$.

On peut légitimement se demander s'il existe des matrices d'Hadamard d'ordre n, avec n quelconque. Ce qui nous amène au théorème suivant :

Théorème 2.1.1 : Pour $n > 2$, n doit être multiple de 4.

Preuve : Supposons que $\mathcal{H}$ a été normalisée, de telle sorte que la premère ligne ne comporte que des 1. Puisque les lignes sont orthogonales, la deuxième ligne doit forcément comporter le même nombre de 1 et de -1 ; soit $\frac{n}{2}$ 1 et $\frac{n}{2}$ -1, ce qui implique que n est nécessairement paire. En réarrangeant l'ordre des colonnes, on peut supposer que la première ligne ne comporte que des 1 et la deuxième des 1 sur les $\frac{n}{2}$ premières entrées, et -1 sur les $\frac{n}{2}$ dernières. Si $n > 2$, considérons la troisième ligne de $\mathcal{H}$. Supposons que h de ses $\frac{n}{2}$ premières composantes sont des 1, et k de ses $\frac{n}{2}$ dernières composantes sont des 1. Alors, $\frac{n}{2} - h$ de ses $\frac{n}{2}$ premières composantes sont des -1, et $\frac{n}{2} - k$ de ses $\frac{n}{2}$ composantes sont des -1.

Comme la première et la troisième lignes sont orthogonales, on a :

$$h - (\frac{n}{2} - h) + k - (\frac{n}{2} - k) = 0,$$

ce qui nous donne $h + k = \frac{n}{2}$. Par l'orthogonalité des deuxièmes et troisièmes lignes, on obtient de la même manière $h = k$. Ainsi, on arrive à $h = k = \frac{n}{2}$, et n doit ainsi être multiple de 4.

On notera que si l'on multiplie n'importe quelle ligne ou colonne par -1, on obtient encore une matrice d'Hadamard, l'orthogonalité des lignes et des colonnes étant préservée. On peut ainsi toutes les normaliser, autrement dit faire que toutes les composantes de la 1^{re} ligne et de la 1^{re} colonne soient égales à 1. Ce qui nous amène au corollaire suivant :

Corollaire 2.1.1 : Dans toute matrice d'Hadamard d'ordre 4^m, n'importe quelles 2 colonnes autres que la 1^{re} ont des 1 aux mêmes emplacements à exactement m reprises.

Preuve : On réutilise l'argument utilisé sur les lignes dans le théorème précédent, mais cette fois sur les colonnes.

2.2 Définition d'un modèle d'Hadamard et exemple

Des matrices d'Hadamard découlent des plans d'Hadamard, qui seront enfait des plans (v, k, λ). En effet, l'idée derrière tout cela est la suivante : on prend une matrice normalisée, on en enlève sa première ligne ainsi que sa première colonne, on remplace les -1 par des 0, et on prend ensuite cette matrice résultante comme matrice d'incidence du plan considéré. Ce qui nous donne le théorème suivant :

Théorème 2.2.1 : S'il existe $\mathcal{H}$ matrice d'Hadamard d'ordre $4m$, alors il existe un plan $(4m - 1, 2m - 1, m - 1)$.

Preuve : Soit $\mathcal{H}$ une matrice d'Hadamard d'ordre $4m$ normalisée. Chaque ligne et chaque colonne, hormi la 1^{re} ligne ainsi que la 1^{re} colonne, compte $2m$ "1" et $2m$ "-1". On enlève ces premières ligne et colonne et on y remplace tous les -1 par des 0. On se retrouve donc avec une matrice $\mathcal{A}$ $(4m - 1) \times (4m - 1)$ remplie de 0 et de 1. Plus précisément, chaque colonne et chaque ligne possède $2m$ "0" et $2m - 1$ "1".

On interprète $\mathcal{A}$ comme une matrice d'incidence d'un modèle nécessairement symétrique. Ce modèle possède $4m-1$ blocs et $4m-1$ éléments ; chaque bloc possède $2m-1$ éléments et chaque élément se trouve dans $2m - 1$ blocs. On considère maintenant n'importe quels 2 éléments. Les colonnes de $\mathcal{A}$ qui correspondent à ces 2 éléments ont $m - 1$ "1" ensemble (cf *Corollaire* 2.1.1), c'est-à-dire que ces 2 éléments se trouvent ensemble dans exactement $m - 1$ blocs. Donc le plan est bien équilibré avec $\lambda = m - 1$.

Ces résultats nous mènent donc vers une définition précise d'un plan d'Hadamard :

Définition : Un plan $(4m - 1, 2m - 1, m - 1)$ est appelé plan d'Hadamard.

On peut même aller un petit peu plus loin que le résultat mis en évidence avec le théorème 2.2.1, puisque ce résultat est en fait une équivalence. En s'intéressant de plus près à la preuve du résultat, on remarque qu'en effectuant la démarche inverse, on obtient la preuve de l'équivalence. Ce résultat nous permet donc de construire des matrices d'Hadamard d'ordre $4m$ dès que l'on peut construire le plan correspondant.

Regardons une méthode de construction de plan d'Hadamard, la plus simple :
Soit p un nombre premier de la forme $p = 4m - 1$, et prenons les carrés de $1, 2, ..., \frac{1}{2}(p - 1)$ $(mod\ p)$. En général, l'ensemble des carrés de $1, 2, ..., \frac{1}{2}(p - 1)$ $(mod\ p)$ joue le rôle de bloc de départ pour un plan d'Hadamard cyclique $(4m-1, 2m-1, m-1)$. Voyons un exemple pour y voir un peu plus clair :

Prenons p=11. Les carrés de $1, 2, ..., 5$ $(mod\ 11)$ sont $1, 4, 9, 5, 3$. On prend donc l'ensemble

$1, 3, 4, 5, 9$ comme bloc de départ, et on obtient les autres blocs en ajoutant successivement 1 (mod 11) à chaque composante du bloc. Le plan $(11, 5, 2)$ qui en résulte a la matrice d'incidence suivante :

$$\mathcal{B} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{R}^{11\times 11}$$

On obtient donc de cette matrice d'incidence la matrice d'Hadamard d'ordre 12 suivante :

$$\mathcal{B} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix} \in \mathbb{R}^{12\times 12}$$

Il est conjecturé qu'une matrice d'Hadamard d'ordre $4n$ existe pour tout entier n positif, mais c'est encore loin d'être prouvé. C'est ce sur quoi notre attention va se porter dans les deux sections suivantes.

2.3 Propriétés et résultats mathématiques intéressants

Dans cette section, nous allons nous intéresser sur les résultats qui ont été démontrés (et dont nous admettrons la majeure partie des résultats) afin de répondre à la question suivante :

Pour quels entiers n a-t-on une matrice d'Hadamard d'ordre n (de taille $n \times n$) ?

Hadamard tout d'abord démontré le résultat suivant :

S'il existe $\mathcal{H}$ matrice d'Hadamard d'ordre n, alors $n = 1$, $n = 2$, ou n multiple de 4.

Hadamard a ensuite émis la conjecture suivante en 1893 :
Pour tout entier naturel n multiple de 4, il existe une matrice de Hadamard d'ordre n. Malgré plus d'un siècle d'efforts, cette conjecture n'a toujours pas été démontrée mais voici une suite de résultats, démontrés au fil des années, qui nous permettent d'affiner les valeurs de n pour lesquelles les matrices d'Hadamard sont possibles. On appellera dans la suite nombre d'Hadamard tout entier n tel que $\mathcal{H}$ d'ordre n existe.

En 1863, soit 26 ans avant l'article de Jacques Hadamard, James Joseph Sylvester aborda en premier le problème de ces matrices (qu'il appellera échiquier anallagmatiques). Dans cet article, il en construit de taille $n \times n$, avec n une puissance de 2, c'est-à-dire $n = 2^r$. L'idée derrière cette construction réside dans le théorème suivant :

Théorème 2.3.1 : Si on a une matrice $\mathcal{H}$ d'Hadamard d'ordre n, alors on en construit une nouvelle d'ordre $2n$ facilement.

Preuve : On note $\mathcal{H}'$ le négatif de $\mathcal{H}$ (*ie* la matrice obtenue en intervertissant les 1 et les -1). $\mathcal{H}'$ est évidemment une matrice d'Hadamard d'ordre n également. La matrice $\mathcal{G} = \begin{pmatrix} \mathcal{H} & \mathcal{H} \\ \mathcal{H} & \mathcal{H}' \end{pmatrix}$ est également une matrice d'Hadamard, mais celle-ci d'ordre $2n$. La vérification se fait simplement pour les cas $n = 2$, $n = 4$, voire $n = 8$, mais devient vite compliquée à l'oeil nu, et extrêmement fastidieuse.

Jacques Hadamard montrera également l'existence de matrices d'ordre $n = 12$ ainsi que $n = 20$, d'une manière qui aura sûrement aidé les progrès faits dans le domaine ultérieurement.

Parmi ceux-ci, on trouve dès 1898 trace d'un résultat significatif démontré par Scarpis :

Théorème 2.3.2 : Soit n multiple de 4 tel que $n-1$ premier. S'il existe une matrice de Hadamard d'ordre n, alors il en existe une plus grande d'ordre $(n-1).n$

Preuve : Admise, mais la preuve est en réalité constructive, et consiste à combiner les lignes de la matrice d'origine pour en construire une nouvelle, de plus grande taille

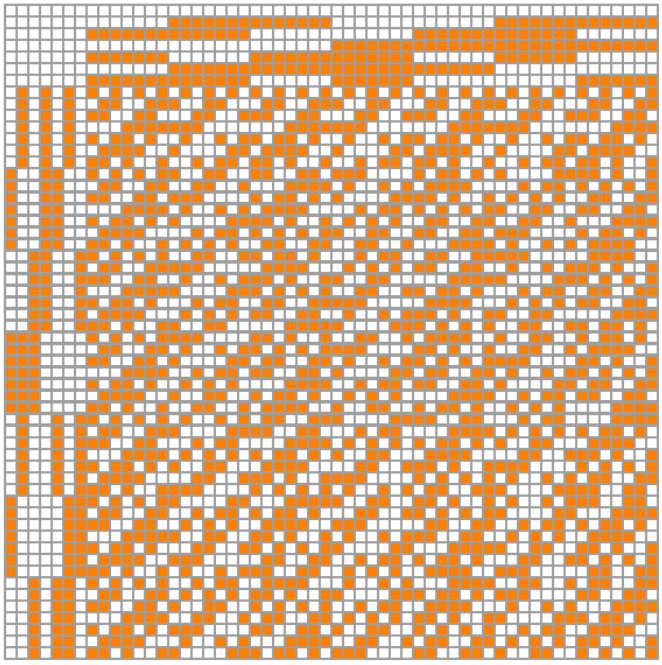
Ce dernier résultat nous amène à une digression naturelle : les **nombres de Mersenne**. On appelle nombre de Mersenne les nombres de la forme $2^r - 1$, avec r premier. En effet, on peut se poser la question suivante : quand $2^r - 1$ est-il premier ? Une première prérogative est que r soit premier (d'où notre intérêt porté sur les nombres de Mersenne). En effet, si d divise r alors 2^d - 1 divise 2^r - 1. Cela découle par exemple de l'identité remarquable a^n- $b^n = (a\text{-}b)\ (a^{n\text{-}1} + a^{n\text{-}2}b + \cdots + ab^{n\text{-}2} + b^{n\text{-}1})$, en posant $a = 2^d$, $b = 1^d = 1$ et $n = \frac{r}{d}$. Mais la question de la primalité des nombres de Mersenne reste un problème aux multiples mystère depuis longtemps. Actuellement, nous connaissons 47 premiers de Mersenne, mais on ne sait toujours pas s'il en existe une infinité ou non. Par exemple, les quatre plus petits premiers de Mersenne sont les suivants :

$$2^2 - 1 = 3, \quad 2^3 - 1 = 7, \quad 2^5 - 1 = 31, \quad 2^7 - 1 = 127$$

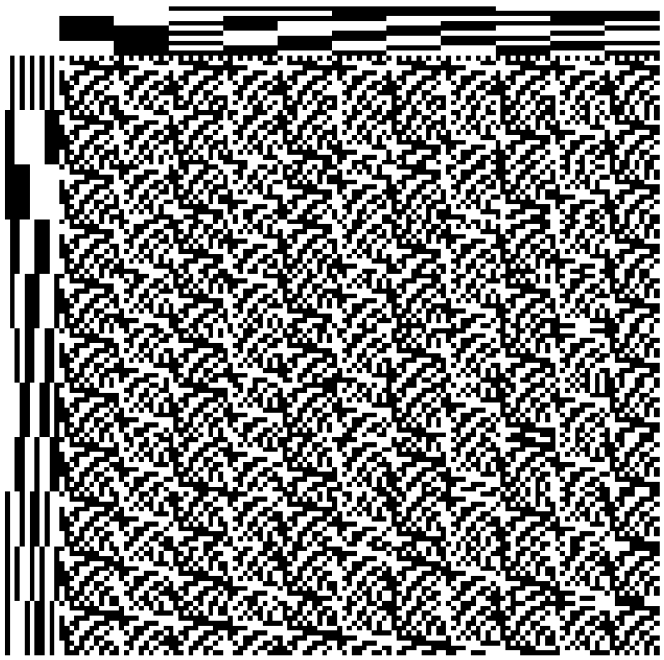
Enfin, il est également intéressant de noter que le plus grand nombre premier (13 millions de chiffres, découvert en 2008) connu est un premier de Mersenne :

$$2^{43112609} - 1$$

Scarpis a donc établi un lien intéressant entre les nombres de Mersenne et les matrices d'Hadamard. Voici donc, en couleurs (cases blanches et oranges correspondant aux 1 et aux 0), la matrice d'Hadamard d'ordre 56, qui découle donc du nombre de Mersenne 7 ($n = 8 = 2^3$) :



De plus, cette construction de Scarpis, dans certains cas, peut être répétée. Par exemple, en partant de $n = 4$, on obtient une matrice d'Hadamard d'ordre 12. 11 étant premier, on peut réappliquer la méthode à celle-ci et ainsi obtenir une matrice d'Hadamard d'ordre 132, que voici (en noir et blanc, et sans lignes et colonnes) :



On notera une similarité assez évidente entre cette matrice et les QR Code et autres flashcodes que nous voyons régulièrement autour de nous. Ce lien sera étudié dans le $3^{ème}$ chapitre. La vérification, à l'oeil nu, du caractère égalitaire, propriété caractéristique des matrices d'Hadamard, de cette construction est impossible. Mais la preuve de Scarpis et sa méthode de construction permet d'en avoir l'assurance.

Suite à ce résultat, la première avancée notable qui a suivi fut l'oeuvre de Ray Edwin Gilman en 1930. En effet, il a démontré que l'une des hypothèses du théorème de Scarpis est automatiquement satisfaite. Le voici :

Théorème 2.3.3 : Soit n un multiple de 4 tel que n-1 soit un nombre premier. Alors il existe

une matrice de Hadamard d'ordre n.

Preuve : On note $\mathcal{H}_n$ l'ensemble des matrices d'Hadamard. Cette preuve s'effectuera en 4 temps. On va tout d'abord décrire $\mathcal{H}_1$ et $\mathcal{H}_2$, et montrer que pour $n > 2$ non-divisible par 4, $\mathcal{H}_n = \emptyset$. Ensuite, en prenant p premier de la forme $p = 4m - 1$, nous montrerons qu'il existe exactement $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$ * et que si $l^2 \neq 0$, alors $-l^2$ n'est pas un carré. Puis nous en déduirons que $|\{i, j \in \mathbb{Z}/p\mathbb{Z}/r = i^2 - j^2\}| = \frac{p-3}{4}$ pour tout $r \in \mathbb{Z}/p\mathbb{Z}$ *. Enfin nous terminerons par aboutir au résultat de Gillman.

Démarrons. $\mathcal{H}_1 = \{1, -1\}$ et

$$\mathcal{H}_2 = \left\{ \begin{array}{c} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \end{array} \right\}$$

Les 6 dernières matrices sont obtenues en multipliant les lignes ou colonnes de la première par -1. On remarque que si $\mathcal{H}_n \neq \emptyset$, alors par multiplication des colonnes par -1 et permutations des colonnes, $\mathcal{H}_n$ contient une matrice dont la première ligne est remplie de 1, et la seconde remplie de 1 puis de -1, avec autant de 1 que de -1 (on aura donc n pair pour $n \geq 2$). Supposons maintenant $n \geq 3$ et regardons la troisième ligne en notant k le nombre d'indice ($\leq \frac{n}{2}$) et h le nombre d'indice ($> \frac{n}{2}$).

Comme $\langle L_1, L_3 \rangle = 0$, on a $k - (\frac{n}{2} - k) + h - (\frac{n}{2} - h) = 0$.

Comme $\langle L_2, L_3 \rangle = 0$, on a $k - (\frac{n}{2} - k) - h + (\frac{n}{2} - h) = 0$.

On obtient donc $h = k$ et $4h = n$, qui est un multiple de 4.

Passons à la deuxième étape. On écrit $p = 2k + 1$ et on regarde $1^2, \cdots, k^2 \in \mathbb{Z}/p\mathbb{Z}$ *. Si $i^2 = j^2$ dans cette liste, alors $(i - j)(i + j) = 0$ et donc $i = j$ car $i \neq j$ $(mod\ p)$ puisque $1 \leq i, j \leq k$. Comme $(-i^2) = i^2$ et que $\mathbb{Z}/p\mathbb{Z}$ * $= \{-k, \cdots, -1, 1, \cdots, k\}$, on a bien $k = \frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$ *. De plus, si $l^2 \neq 0$ est un carré, et $-l^2$ aussi, alors $-l^2 \times (l^{-1})^2 = -1$ est aussi un carré. Posons alors $-1 = x^2$. Par Fermat, $(-1)^k = x^{p-1} = 1$ et donc k est pair, ce qui est exclu puisque $2k + 1 = 4m - 1$ et donc $k = 2m - 1$.

Passons à la troisième étape de notre preuve. Si $l^2 = i^2 - j^2$, alors $-l^2 = j^2 - i^2$ et il suffit, par notre second point, de montrer la proposition pour $r = l^2$ avec $l \in \{1, \cdots, k\}$. Mais on remarque :

$$1 = i^2 - j^2 \ \ (1) \Leftrightarrow l^2 = (li)^2 - (lj)^2 \ \ (2)$$

. Ainsi, $|\{i, j \text{vérifiant } (1)\}| = |\{i, j \text{vérifiant } (2)\}|$. Finalement, $|\{i, j \in \mathbb{Z}/p\mathbb{Z}/r = i^2 - j^2\}|$ ne dépend pas de $r \in \mathbb{Z}/p\mathbb{Z}$ *. On note ce nombre n, que l'on calcule comme il suit :

$$n \times |\{\mathbb{Z}/p\mathbb{Z} *\}| = |\{(i, j),\ 1 \leq i \neq j \leq k\}| = k(k - 1).$$

On obtient donc $n(p - 1) = (\frac{p-1}{2}) \times (\frac{p-3}{2})$, et donc $n = \frac{p-3}{4}$.

Nous voila avec les outils nécessaires pour arriver au résultat de Gilman. Soit $\widetilde{\mathbf{M}} \in \mathcal{M}_{4m-1}(\mathbb{R})$ la matrice circulante construite à partir de la première ligne :

$$\widetilde{\mathbf{M}}_{ij} = 1 \text{ si j est un carré dans } \mathbb{Z}/p\mathbb{Z} *, 0 \text{ sinon.}$$

On définit la matrice réelle $\mathbf{M} \in \mathcal{M}_{4m}$ qui est enfait la matrice $\widetilde{\mathbf{M}}$ à laquelle on a rajouté une première ligne et colonne entièrement remplie de 1. Par définition, il faut montrer que $\mathbf{M}$ est orthogonale. Notons $L_1, \cdots, L_{4m}$ ses lignes. Chaque ligne L_j, pour $j \geq 2$, ayant $1 + \frac{p-1}{2} = \frac{p+1}{2} = 2m$ coefficients égaux à 1 et $2m$ coefficients égaux à -1, on a $\langle L_1, L_j \rangle = 0$ pour $j \geq 2$.

Pour conclure, il suffit de montrer $\langle \widetilde{L_i}, \widetilde{L_j} \rangle = -1$ pour tout $i \neq j$, avec $\widetilde{L_1}, \cdots, \widetilde{L_p}$ sont les lignes de $\widetilde{\mathbf{M}}$.

Posons $r = j - i \in \{1, \cdots, p - 1\} = \mathbb{Z}/p\mathbb{Z} *$. Par le troisième point de notre preuve, et par définition de $\widetilde{\mathbf{M}}, \widetilde{L_i},$ et $\widetilde{L_j}$ ont $\frac{p-3}{4}$ "1" en commun.

On a donc

$$\langle \widetilde{L_i}, \widetilde{L_j} \rangle = (\frac{p-3}{4})(1 \times 1) + (\frac{p+1}{4})((-1) \times 1) + (\frac{p+1}{4})((-1) \times (-1)) = -1$$

en utilisant le fait que $\widetilde{L_i}$ et $\widetilde{L_j}$ comptent chacune $\frac{p-1}{2}$ "1" et $\frac{p+1}{2}$ "-1".

On en conclut donc que $|\{p = 4m-1 \text{ premier}\}| = +\infty$ et donc $|(\bigcup_{n\geq 2} \mathcal{H}_n)| = +\infty$.

Peu de temps après, Raymond Paley a généralisé le résultat de Gilman dans le théorème suivant :

Théorème 2.3.4 : Soit n un multiple de 4 tel que $n-1$ ou $\frac{n}{2}-1$ soit une puissance de nombre premier. Alors il existe une matrice de Hadamard d'ordre n.

Preuve : Admise, mais se base sur les mêmes principes que celle de Gilman, à ceci près qu'elle utilisé la répartition des carrés parfaits dans une structure de corps fini (les entiers *modulo* **p**). On notera que cette preuve est une parfaite illustration de l'unité des mathématiques, où des notions algébriques abstraites telles que les corps finis, aident à la construction d'objets mathématiques parfaitement concrets, comme les matrices d'Hadamard.

Grâce à tous ces résultats, récapitulons et regardons ce qu'ils nous permettent d'affirmer. Premièrement, voici les nombres qui, à l'aide du théorème de Gilman, sont des nombres d'Hadamard parmi les multiples de 4 bornés par 100 (car on remarque bien que chaque entier $n-1$ est premier pour chacun des n qui suit) :

$$4, 8, 12, 20, 24, 32, 44, 48, 60, 68, 72, 80 \text{ et } 84.$$

. Ensuite, par le théorème de Paley, on peut rajouter à cette liste les cinq nombres suivants :

$$28, 36, 52, 76 \text{ et } 100.$$

En effet, on a :

$$28-1 = 27 = 3^3,\ \frac{36}{2}-1 = 17,\ \frac{52}{2}-1 = 5^2,\ \frac{76}{2}-1 = 37 \text{ et } \frac{100}{2}-1 = 72.$$

Dans chaque cas, on obtient bien un premier ou une puissance de premier, ce qui permet l'application du théorème de Paley. A ceux-ci, on pourra ajouter les nombres suivants :

$$16, 40, 56, 64, 88 \text{ et } 96.$$

Ceux-ci s'obtiennent en appliquant le résultat de Sylvester permettant de passer de n à $2n$ aux nombres des deux listes précédemment énoncées. Enfin, pour les entiers multiples de 4 bornés par 100, on y ajoutera 92, qui ne rentre pas dans les critères de Paley, Gilman, ou Sylvester, mais qui est bien un nombre d'Hadamard (prouvé par un gros calcul sur ordinateur en 1962, grâce à une construction plus générale présentée par Williamson en 1944).

2.4 Les défis et enjeux restants encore à démontrer

A l'aide de la section précédente, nous avons pû établir un état des lieux des connaissances et avancées faîtes sur les travaux d'Hadamard. Mais nous sommes encore loin d'avoir répondu à la problématique de départ et démontré la conjecture d'Hadamard.

Du côté positif, des chercheurs ont montré, à l'aide de calculs sur ordinateur, que tous les multiples de 4 bornés par 1000 sont bien des nombres d'Hadamard, à l'exception des trois nombres 668, 716, et 892, qui restent encore aujourd'hui en suspens.

Pour les multiples de 4 entre 1000 et 2000, on dénombre pas moins de 9 cas en suspens :

$$1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948 \text{ et } 1964.$$

Enfin, pour les très grands multiples de 4, on ne sait finalement rien de particulier qui nous permette de dire que tel multiple de 4 serait un nombre d'Hadamard. Nous sommes donc dans une

situation où l'on sait énormémement de choses, puis extrêmement peu !

Il est intéressant de noter également que d'autres approches, que nous n'aborderons pas en profondeur ici, ont été considérées pour obtenir des résultats concernant les nombres d'Hadamard. En effet, par exemple, en 1976, Jennifer Seberry Wallis apporta son écot avec le théorème suivant (dont la preuve sera admise) :

Théorème 2.4.1 : Soit q un nombre impair. Alors pour tout exposant t suffisamment grand, le nombre $2^t q$ est un nombre de Hadamard.

Il reste encore à affiner ce résultat, afin de remplacer le "t suffisamment grand". Il y a également des intérêts portés sur les matrices circulantes, ou bien encore les quadruplés de Turyn, mais qui ne permettent pas d'obtenir plus de résultats significatifs pour le moment.

Chapitre 3

Des matrices d'Hadamard aux Codes

Après s'être attardé sur les plans d'expérience finis, qui nous ont amené à nous intéresser aux matrices et plans d'Hadamard, portons désormais notre regard sur les codes binaires, et correcteur d'erreurs, qui nous le verrons, sont intimement liés aux travaux d'Hadamard.

3.1 Définition d'un code (binaire)

Définition : Un code binaire de longueur n est un ensemble $\mathcal{C}$ de séquences binaires à n chiffres. La (Hamming) distance $d(x, y)$ entre deux mots de code x et y est le nombre d'emplacement où ils diffèrent. Si $d(x, y) \geq 2t + 1$ pour tout x, tout y, avec $x \neq y$, le code $\mathcal{C}$ est dit t-erreur correcteur.

Derrière cette définition un peu formelle, le raisonnement est le suivant :
Un code binaire est une collection de séquences binaires à n chiffres, appelés mots de code. Si ces mots de code sont transmis, alors des erreurs peuvent émerger à cause d'interférences, et les mots de code reçus peuvent différer à certains endroits des mots de code envoyés. L'idée de départ derrière les codes correcteurs d'erreurs est de choisir les mots de code suffisamment différents les uns des autres pour que même si des erreurs arrivent pendant la transmission, chaque moi reçu est "plus proche" (au sens de la distance de Hamming) que n'importe quelle autre. On a ici le concept de "distance" entre deux mots de code qui est introduite, à savoir le nombre d'endroits dans lesquels ils diffèrent. Si tous les mots de code sont choisis tels que chacun diffère en au moins $2t + 1$ endroits, alors, même si t erreurs sont faites pendant la transmission du mot de code, la séquence binaire reçue sera toujours plus proche de l'original que n'importe quel autre, et ainsi peut être correctement décodé comme le mot de code le plus proche.

Exemple : On s'intéresse aux quatre séquences binaires suivantes :

Séquence 1 (0, 0, 0, 0, 0, 0, 0)
Séquence 2 (1, 1, 1, 1, 1, 1, 1)
Séquence 3 (1, 0, 1, 0, 1, 0, 1)
Séquence 4 (0, 1, 0, 1, 0, 1, 0)

Ces quatre séquences diffèrent en au moins trois endroits et forment donc une code correcteur d'une erreur (1-error correcting code). Donc, si par exemple, $(1, 0, 1, 0, 1, 0, 1)$ est envoyé et $(1, 1, 1, 0, 1, 0, 1)$ est reçu (à cause d'interférences), la séquence $(1, 1, 1, 0, 1, 0, 1)$ est plus proche de $(1, 0, 1, 0, 1, 0, 1)$ que de n'importe quel autre mot de code et peut donc être décodé correctement.

Cependant on trouve dans un code deux aspects conflictuels : avec n donné, on voudrait avoir la distance minimum entre deux mots de code aussi grande que possible (pour améliorer la correction d'erreur), mais on voudrait aussi avoir le plus de mots de code possibles. Il y a donc un conflit : on ne peut pas avoir trop de mots de code qui sont à une large distance les uns des autres.

Cela nous amène à un problème fondamental : étant donnés n et k, combien de séquences binaires de longueur n peut-on trouver tel que chaque paire de séquences binaires diffère en au moins k endroits ?

On va considérer un cas particulier : quand $k = \lceil \frac{n}{2} \rceil$, et avec n impaire :

Lemme 3.1.1 : On suppose qu'il existe N séquences binaires de longueur $n = m - 1$, dont n'importe quelles deux diffèrent en au moins m endroits. Alors, $N \leq n + 1$.

Preuve : Admise.

Intéressons nous encore ici à un exemple, pour illustrer ce lemme : combien de mots de code de longueur 11 peut-on trouver tels que chaque paire diffère en au moins 6 endroits ?

Par le lemme énoncé précédemment, on ne peut en trouver plus de 12. Mais en utilisant le plan d'Hadamard $(11, 5, 2)$ (et la matrice d'Hadamard d'ordre 12 correspondant). La matrice d'incidence correspondant est telle qu'il suit : chaque ligne possède 5 "1", mais chaque paire de lignes ne partage que 2 "1", donc deux lignes diffèrent en $2 \times (5 - 2) = 6$ endroits. Donc, si on prend ces lignes comme mots de code, plus la ligne de 1 (qui diffère en 6 endroits des 11 autres), on obtient 12 mots de code.

Enfin, voyons un dernier résultat :

Théorème 3.2.1 : Si $\mathcal{C}$ est un code binaire t-erreur-correcteur, alors $|\mathcal{C}|.\left\{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}\right\} \leq 2^n$. En cas d'égalité (qui s'obtient lorsque la somme des $\binom{n}{k}$ est égale à une puissance de 2), $\mathcal{C}$ est dit parfait. Pour un tel code $\mathcal{C}$, toute séquence binaire est correctible en un mot de code $\mathbb{C}$, c'est-à-dire que chaque séquence est à distance au plus t d'un unique mot de code.

Preuve : Voir en annexe.

3.2 Utilisation des travaux d'Hadamard dans l'univers des codes

Les notions développées dans la section précédente nous amènent à aborder le lien qui se trouve entre les travaux de Jacques Hadamard et les codes binaires. Cela par le biais du corollaire suivant :

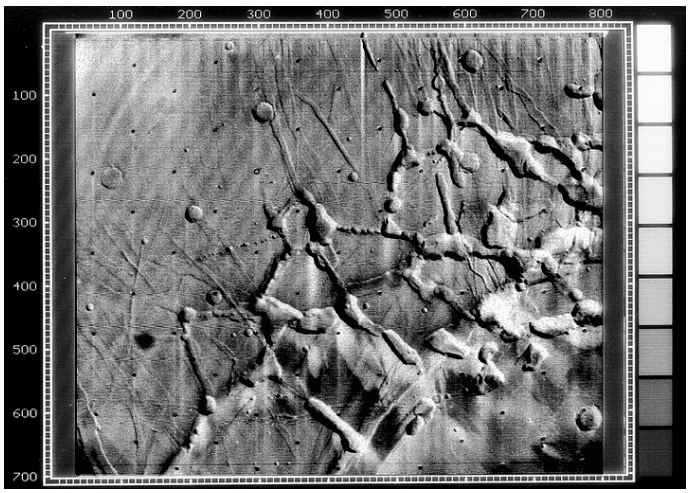
Corollaire 3.2.1 : Soit $\mathcal{C}$ code de longueur $n = 2m$, contenant N mots de code, dont chaque paire diffère en au moins m endroits.
Alors, $N \leq 2n$. De plus, si une matrice d'Hadamard d'ordre n existe, alors il existe un tel code mais avec $2n$ mots de code.

Preuve : Voir en annexe.

Encore une fois, le lien avec les travaux d'Hadamard sera plus éloquent au travers d'un exemple :

Prenons la matrice d'Hadamard $\mathcal{H}_5$, qui possède 32 lignes et colonnes. On note $\mathcal{A}$ la matrice obtenue en remplaçant tous les -1 par des 0, et $\overline{\mathcal{A}}$ la matrice obtenue en intervertissant les 1 et les 0 de $\mathcal{A}$. Ainsi, les lignes de $\mathcal{A}$ et $\overline{\mathcal{A}}$ forment un code de 64 mots de code de longueur 32, chacun différant en au moins 16 endroits. On a donc un code 7-erreurs-correcteur.

Un tel code a été utilisé en 1972, pendant l'exploration spatiale Mars Mariner, afin de renvoyer des photos à la Terre. En effet, chaque photo consistait en un ensemble de points de différentes nuances de gris (64 nuances nécessitant des séquences binaires à 6 chiffres puisque $2^6 = 64$) et la séquence de nuances codées était encodée/cryptée en utilisant le code 7-erreur-correcteur que l'on vient de décrire. Les photos résultantes se sont avérées remarquablement bonnes ! En voici une :



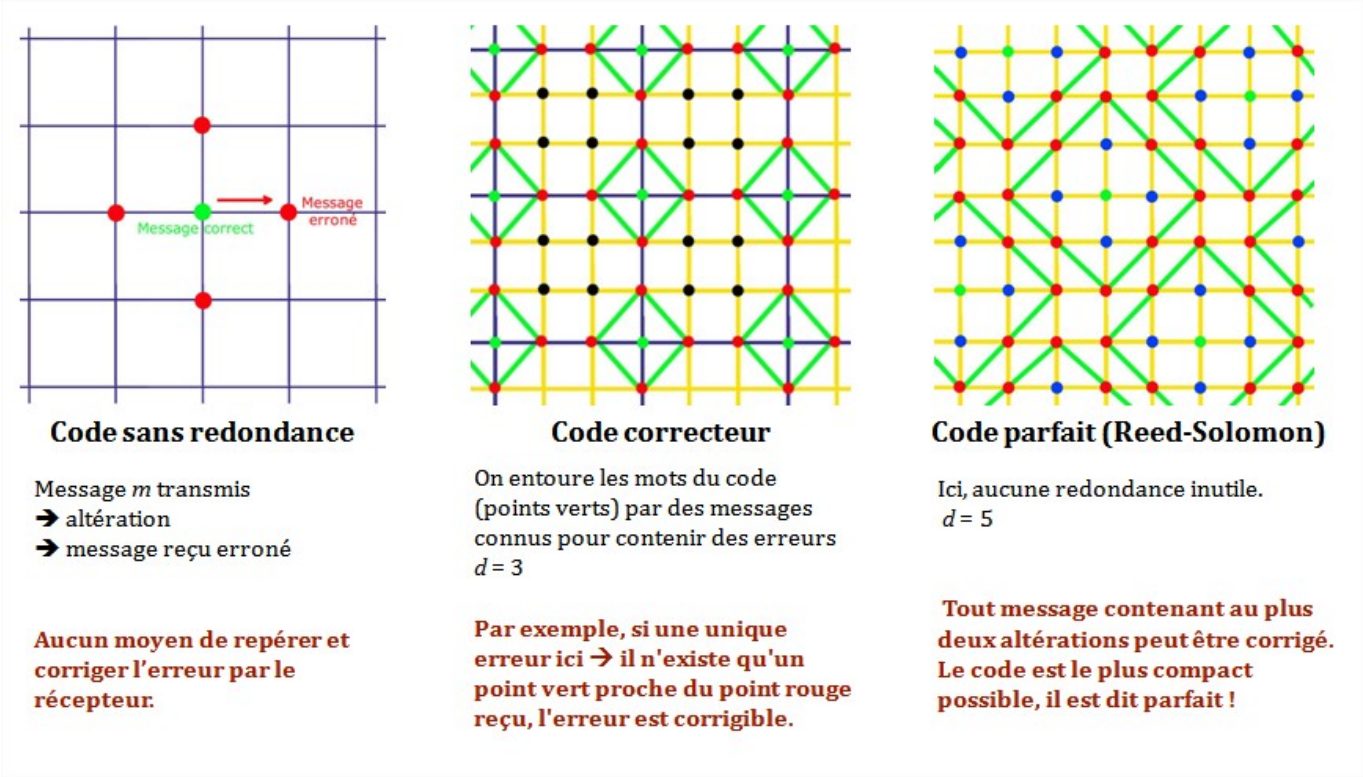
Les expéditions plus récentes ont utilisés des codes plus sophistiqués, comme des CD.

3.3 Digression : Les Quick Response Code, leurs particularités, le code correcteur de Reed-Salomon

Dans le monde avec lequel on intéragit quotidiennement, il se trouve que les structures de codes abordées dans le chapitre précédent sont enfait à chaque coin de rue, ou presque. En effet, les Quick Response codes, autrement dit QR codes, fleurissent et sont utilisés très régulièrement. La particularité du QR code repose enfait sur son code correcteur. En effet, ce code correcteur particulier va créer de la redondance, afin d'accroître la fiabilité de l'information transmise, prévenir à toute altération du motif, et fournir au lecteur l'information codée de départ sans souci. Ce code correcteur particulier qu'il contient est **le code de Reed-Solomon**. Ce code de Reed-Salomon, inventé par les mathématiciens Irving S.Reed et Gustave Solomon, est dit parfait. C'est un code correcteur très utilisé, permettant la correction d'erreurs dûes à une transmission déficiente d'un message.

Le code de Reed-Solomon prend racine sur un principe mathématique ayant pour objectif de construire un polynôme à partir des symboles à transmettre (source) et de le **suréchantillonner**, c'est-à-dire de lui apporter plus d'informations. On envoie ensuite ce résultat en lieu et place des symboles originaux. C'est grâce à la redondance de ce suréchantillonnage que le récepteur du message encodé peut reconstruire le polynôme de départ, et ce même quand des erreurs ont lieu pendant la transmission.

Pour illustrer le propos, voici des illustrations de code non correcteur, de code correcteur (type code de Hamming) et de code parfait (type code de Reed-Solomon) :



Il convient d'expliquer un petit peu les illustrations précédentes. De manière générale, tous les codes correcteurs subissent une contrainte du même ordre. Si, dans le message réçu, une information est altérée, alors une information supplémentaire sera nécessaire pour détecter et à fortiori corriger l'erreur. Le mot de code est ensuite envoyé dans un espace plus vaste, comme il est mis en évidence dans l'illustration du milieu. Celle de gauche met en évidence un code sans redondance aucune.

Chaque point du code (en vert sur la figure) va différer des autres points du code par au moins d coordonnées. Enfin, la modification d'une coordonnée est ici modélisée par un segment du quadrillage.

Si un point du code est altéré à la transmission, alors un nouveau message (rouge sur la figure) est envoyé. Nous ne savons, à ce moment, rien d'une quelconque erreur. Le but sera donc d'entourer les messages sans erreurs (qui correspondent aux intersections du quadrillage) avec des messages contenant des erreurs, et de réaliser seulement ensuite l'envoi du message. Ces redondances sont mises en évidence sur l'illustration du milieu par les intersections oranges. Si une erreur unique a lieu, le message transmis correspond à un point rouge. Enfin, si la redondance a été correctement construite, on ne va trouver qu'un seul point licite (vert) à proximité du celui illicite (rouge) reçu.

Pour revenir à notre illustration centrale, on remarque que les points du code diffère par au moins $d = 3$ coordonnées. Si la déficience se trouve sur une unique coordonnée, la transmission va donc correspondre à un point rouge du schéma. Le récepteur va donc pouvoir corriger l'erreur, car on ne trouve qu'un seul point vert à une distance $d = 1$ du message reçu.

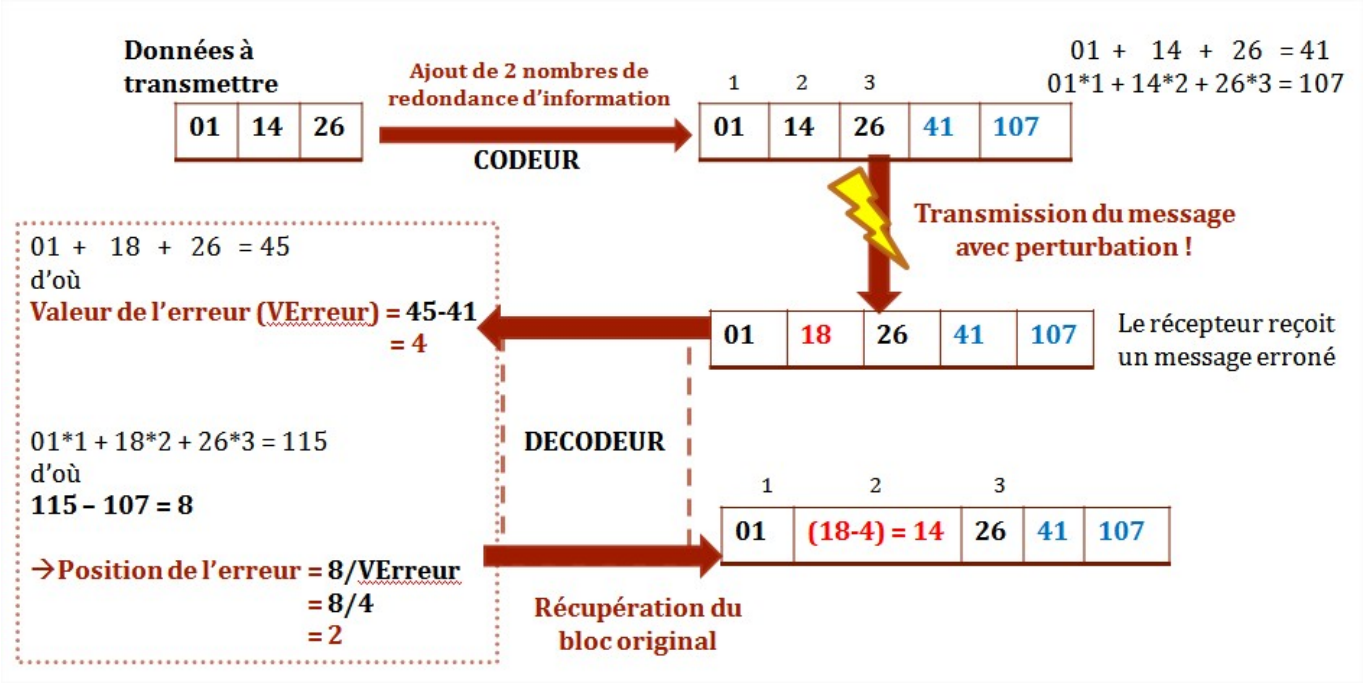
ps : La distance de Hamming correspond ici au plus petit nombre de segments du quadrillage à traverser pour joindre deux points, soit $d = 3$.

Comme vu précédemment en section 3.1, le principe d'un code correcteur est de proposer une géométrie ou les messages valides sont le plus possible éloignés les uns des autres. Sur nos schémas, ce sont les boules centrées sur les codes licites, si elles ne s'intersectent pas, qui permettent de retrouver le message initial. Une perturbation sera corrigible si elle ne fait pas sortir le code de sa boule. Sur la figure centrale, on remarque que les points noirs ne sont d'aucune utilité. De plus, on doit parcourir au moins 2 segments du quadrillage afin de relier un point noir et un point vert. Vient donc une

ambiguïté : chaque point rouge se trouve à 2 segments de 2 points verts. Ainsi, on ne réussira pas, en général, à corriger une double erreur. Enfin, pour revenir à ces points noirs, ils représentent une redondance inutile et prennent de la place. Ils se trouvent à une distance de 2 des points du code, distance pas traitable ici.

Attardons nous sur la figure de droite. Sur celle-ci, les points verts sont espacés d'une distance égale à 5 entre eux. Si la transmissions ne produit pas plus de 2 erreurs, alors elles seront toutes corrigibles. De plus, on ne trouve pas de points en dehors des boules fermées de rayon 2 dont le centre correspond aux points du code, *ie* on ne trouve pas de redondance inutile (point noir). Sont en bleus les points se situant à une distance égale à 1 du code, en rouge ceux à une distance de 2. On se rend finalement compte que tout l'espace est rempli par les boules fermées de centre correspondant aux points du code et de rayon 2, et qu'il n'y a aucune intersection entre elles.

Illustrons donc notre propos par un exemple du fonctionnement d'un code correcteur :



Dans cet exemple, le codeur va rajouter à notre information des nombres, ici 2, qui serviront de redondance d'information. Comme on peut le voir, le 1^{er} nombre de redondance représente la somme des 3 nombres, le 2^{nd} représente quant à lui la somme pondérée des 3, chacun étant multiplié par son rang.

S'il y a altération du message, le décodeur va détecter l'erreur, puis la corriger. Pour se faire, il utilisera les nombres de redondance ajoutés précédemment. Le recalcul de cette somme de nombres permettra de retrouver le même premier nombre de redondance d'information. Dans l'exemple, le décodeur obtient 45 à la place de 41, et sait donc détecter qu'il y a eu erreur à la transmission du message. Il va donc prendre note de la différence entre le nouveau nombre et celui stocké. Cette différence va donc correspondre à la valeur de l'erreur. Afin de la corriger, il va devoir la situer parmi les informations reçues.

Concernant le deuxième nombre de redondances, le décodeur obtient une différence, qui sera divisée par la valeur de l'erreur. Cette valeur nous indiquera la position de l'erreur. On va donc retirer 4 au nombre du deuxième rang.

Finalement, le décodeur a pu détecter l'erreur, la corriger de manière simple, et la délivrer et ce malgré l'altération du message initial. On remarque également que si le message n'est pas altéré à la transmission, les différences des sommes simples et pondérées obtenues sont nulles.

3.4 Pour aller plus loin : Les Quadratic Residue Code

Par un heureux hasard, au gré des recherches effectuées pour comprendre l'origine et le fonctionnement des Quick Response Codes et leur lien avec les matrices et plans d'Hadamard, je suis tout d'abord tombé sur un autre type de QR Code, plus intimement lié aux travaux d'Hadamard que les Quick Response Codes, mais qui utilisent des notions bien plus complexes. Ce sont les Quadratic Residue Codes.

Les Quadratic Residue Codes concernent une famille particulière de matrices d'Hadamard, appelés matrices de Skew Hadamard, auxquelles seront liés les plans de Skew Hadamard.

Définition : Une matrice d'Hadamard $\mathcal{H}$ est dîte matrice de Skew Hadamard s'il existe $\mathcal{S}$ telle que $\mathcal{H} = \mathcal{I} + \mathcal{S}$, avec $\mathcal{S}$ matrice antisymétrique ne contenant que des 0 sur la diagonale.

La matrice d'incidence d'un plan de Skew Hadamard aura également quelques particularités, que voici :

Comme nous restons dans un cas d'Hadamard, on a :

$$\mathcal{A}^T\mathcal{A} = n\mathcal{I} + (n-1)\mathcal{J} \text{ et } \mathcal{A}\mathcal{J} = \mathcal{J}\mathcal{A} = (2n-1)\mathcal{J}.$$

Le côté Skew implique :

$$\mathcal{A} + \mathcal{A}^T + \mathcal{I} = \mathcal{J}.$$

Les codes $\mathcal{C}$ ainsi obtenus ont la particularité, dans le cas Skew Hadamard, en plus d'être self orthogonal d'être également self dual ($ie\ \mathcal{C} = \mathcal{C}^\perp$).

Sans rentrer dans les détails de la construction et des caractéristiques des Quadratic Residue Codes, dans lesquels un lecteur intéressé pourra se plonger, il est intéressant de noter qu'ils font appel à des notions d'arithmétique modulaire poussées, d'algèbre, et évidemment la notion de résidue quadratique d'où ces codes tirent leur nom.

Enfin, afin d'attirer et attiser l'intérêt du lecteur, terminons en donnant la définition formelle d'un Quadratic Residue Code de longueur l, avec l premier, sur $\mathbb{Z}/p\mathbb{Z}$, avec p premier et résidu quadratique modulo l :

Définition : Soit $\mathcal{Q}$ l'ensemble des résidus quadratiques modulo l, et $\mathcal{N}$ l'ensemble des non-résidus modulo l. L'ensemble $\mathcal{Q}$ est fermé sous la multiplication par p, p appartenant à $\mathcal{Q}$. Soit α la racine l-ième de l'unité dans une certaine extension de $\mathbb{Z}/p\mathbb{Z}$. Soit $q(x) = \prod_{r\in\mathcal{Q}} (x - \alpha^r)$.

On définit le Quadratic Residue Code $\mathcal{Q}$ comme étant le code cyclique de longueur l sur $\mathbb{Z}/p\mathbb{Z}$ avec $q(x)$ comme polynôme générateur.

Conclusion

A la lecture de ce mémoire, on peut se rendre compte de l'étendue des mathématiques. En effet, après avoir établi différents liens entre différents domaines, les plans d'expérience avec les matrices et plans d'Hadamard, les matrices et plans d'Hadamard avec les codes, des domaines qui n'amènent pas particulièrement à penser de prime abord qu'ils soient fortement liés, on prend conscience de l'immensité des mathématiques, et du travail qu'il faut y consacrer. Concernant les matrices d'Hadamard, malgré des travaux débutés depuis plus de 150 ans, elles restent nimbées d'interrogations qui sont pour le moment sans réponse ! Et ce malgré les progrès technologiques effectués au fil des ans, permettant à des ordinateurs de faire un nombre monstrueux d'opérations, facilitant les calculs et vérifications. Enfin, on a tous entendu, ou même parfois prononcé, le non-sens voulant faire penser que les mathématiques n'étaient pas si utiles que ce que l'enseignement laisse à penser, qu'on ne l'applique pas tant que ca dans notre vie de tous les jours. Les codes, et QR Codes, représentent une preuve de plus, s'il en fallait, que l'univers des mathématiques qui nous entoure est un facteur prépondérant à nos avancées.

Bibliographie

[1], I. Anderson. *A first course in discrete mathematics*. Springer-Verlag, Heidelberg, 2000.

[2], S. Eliahou. La conjecture de Hadamard I et II. Dans : *Image des mathématiques*, CNRS, 2012.

[3], A. Hedayat et W. D. Wallis. Hadamard matrices and their applications. *Ann. Stat.* **6** (6), 1184-1238, 1978.

[4], M. de Almeida. QR Code. Dans *Le code-barres version 2D*, Institut d'électronique et d'informatique Gaspard-Monge.