Soyons des designers!

Jean-Philippe Labbé

Projet présenté aux professeurs
Javad Mashreghi
Bernard R. Hodgson

Projet de fin d'études
MAT-19517

23 avril 2008

Soyons des designers!

Jean-Philippe Labbé

23 avril 2008

Table des matières

Table des matières ii

Table des figures iii

Introduction 1

1 Théorie des hypergraphes 2
- 1.1 Définitions . . . 2
  - 1.1.1 Hypergraphes . . . 3
  - 1.1.2 Représentation d'un hypergraphe . . . 4
  - 1.1.3 Nomenclature des hypergraphes . . . 5
  - 1.1.4 Isomorphisme, matrice d'incidence et dual . . . 6
  - 1.1.5 Théorème général . . . 9
- 1.2 Exemples d'hypergraphes . . . 10

2 Théorie des designs 13
- 2.1 Structures d'incidence . . . 13
- 2.2 Les designs et les géométries projectives et affines . . . 16
  - 2.2.1 Géométrie projective . . . 16
  - 2.2.2 Géométrie affine . . . 18
  - 2.2.3 Designs . . . 20
- 2.3 t-designs et systèmes de Steiner . . . 23
- 2.4 Partition et résolubilité d'un design . . . 25
- 2.5 Design divisible et design transversal . . . 27

3 Résolubilité de designs 28
- 3.1 Historique des systèmes de Steiner . . . 28
- 3.2 Résultats préalables . . . 29
- 3.3 Constructions . . . 31
- 3.4 Résolubilité de $S(2, 4; v)$ . . . 32

Conclusion 34

Appendice 35

Bibliographie 37

Table des figures

1.1 Graphe simple 3
1.2 Représentation classique d'un hypergraphe simple 4
1.3 Plan projectif fini d'ordre 2 5
1.4 Deux hypergraphes isomorphes 6
1.5 La matrice d'incidence de PG(2,2) 7
1.6 L'hypergraphe K_4 et son dual 9
1.7 Le plan affin d'ordre 3 11
1.8 Un hypergraphe quelconque 12

2.1 La solution du problème des écolières 26

Introduction

À la lecture du livre *The man who loved only numbers* de Paul Hoffman [Hoffman], j'ai décidé d'étudier à Budapest durant l'automne 2006 pour profiter du savoir des mathématiciens hongrois. Le programme d'études *Budapest Semesters in Mathematics* a été créé par Paul Erdős, László Lovász et Vera T. Sós, d'éminents chercheurs en analyse combinatoire et en théorie des nombres. Là-bas, j'ai profité du savoir hongrois : j'ai suivi, entre autres, un cours de théorie analytique des nombres avec Antal Balog et un cours avancé en combinatoire offert par Ervin Győri. Lors de ce dernier, j'ai étudié la théorie des hypergraphes, la théorie de Ramsey et diverses méthodes combinatoires. Quelques semaines après mon séjour en Hongrie, j'ai utilisé mes notions en combinatoire pour résoudre le problème des écolières de Kirkman dans le cadre du cours *Résolution de problèmes mathématiques*. J'ai tout de suite voulu généraliser ce problème.

D'abord, je me suis posé deux questions : pouvons-nous résoudre ce problème avec davantage d'écolières ? Pouvons-nous résoudre le même problème mais posé d'une manière plus générale ? Lors du présent document, nous répondrons à ces questions. Nous allons aborder la théorie des designs qui transpose efficacement ce genre de problèmes.

Afin de se préparer, nous donnerons des définitions et des exemples essentiels à la compréhension du texte en commençant par la théorie des hypergraphes. Par la suite, nous donnerons tout le bagage nécessaire en théorie des designs en s'attaquant à la nomenclature, aux exemples et en terminant par les designs utiles à la résolution des questions. Finalement, nous examinerons comment les mathématiciens Haim Hanani, Dwijendra K. Ray-Chaudhuri et Richard M. Wilson ont généralisé leur propre solution du problème de Kirkman.

Chapitre 1

Théorie des hypergraphes

Les étudiants en mathématiques découvrent habituellement la théorie des graphes lors d'un premier cours en analyse combinatoire ou en mathématiques discrètes. Par contre, il est rare que les hypergraphes fassent partie du cursus universitaire. Partant de cela, nous développerons la théorie des hypergraphes afin d'introduire de façon claire la théorie des designs. Nous verrons en premier lieu les définitions pertinentes et ensuite quelques exemples qui seront utilisés plus tard. D'abord, les hypergraphes sont en fait une généralisation des graphes. L'aspect plus général de cette théorie provient de la suppression de la restriction sur le nombre de sommets d'une arête. En effet, un hypergraphe contient des arêtes ayant un nombre arbitraire de sommets. Cela permet d'élargir les possibilités de la théorie des graphes. Par conséquent, certaines notions deviennent d'autant plus importantes qu'elles sont plus simples à manier, c'est le cas de la dualité. Les définitions sont puisées dans les notes imprimées du cours *Combinatorics 2* [Gyarfas] offert dans le programme *Budapest Semesters in Mathematics* et dans le livre de Claude Berge [Berge].

1.1 Définitions

En premier lieu, rappelons qu'intuitivement un graphe est un schéma constitué d'un ensemble de points et de segments (orientés ou non) reliant chacun deux points. Les points sont appelés les *sommets* du graphe, et les segments, les *arêtes* du graphe. On

peut voir un premier exemple de graphe G à la figure 1.1, où

$$G = (\{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}, \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_7\}, \{p_1, p_4\}, \{p_1, p_6\}, \{p_2, p_4\}, \{p_2, p_5\}, \{p_4, p_5\}, \{p_5, p_6\}, \{p_6, p_7\}, \{p_5, p_7\}\}).$$

Plusieurs questions intéressantes touchant les graphes se généralisent aux hypergraphes.

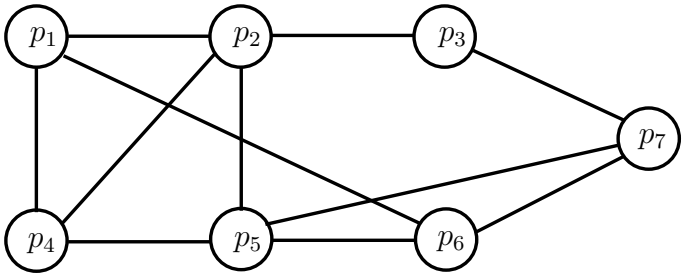

FIG. 1.1 – Un premier exemple de graphe simple ayant 7 sommets

Que ce soit à propos du nombre chromatique, des cycles ou des plongements, elles ont toutes été abordées par les théoriciens des graphes durant les dernières décennies. Cependant, notre étude porte sur un ensemble très restreint d'hypergraphes formé par les designs. Nous explorerons donc les hypergraphes pour devenir à l'aise avec ceux-ci avant d'arriver à formuler de façon claire les questions qui nous intéressent.

1.1.1 Hypergraphes

Nous commençons par la définition d'un hypergraphe.

Définition 1.1 Soient $V := \{p_1, p_2, ..., p_v\}$ un ensemble fini non vide et $\mathbf{B} := \{B_i\}_{i \in I}$, avec I un ensemble d'indices non vide, une famille de parties de V. Le couple $\mathcal{H} := (V, \mathbf{B})$ est appelé un *hypergraphe* d'*ordre* $v = |V|$ s'il satisfait aux conditions

$$\begin{aligned} B_i &\neq \varnothing \qquad (\forall i \in I), \\ \bigcup_{i \in I} B_i &= V. \end{aligned} \tag{1.1}$$

Les éléments de V sont appelés les *sommets* et ceux de $\mathbf{B}$, les *arêtes* de l'hypergraphe.

Les conditions (1.1) ne sont pas absolument nécessaires pour obtenir un hypergraphe : il est possible qu'un hypergraphe possède des sommets isolés ou des arêtes vides. Cependant, nous exigerons qu'un hypergraphe remplisse ces conditions. Une des premières questions qui survient après une telle définition porte sur la représentation des hypergraphes.

1.1.2 Représentation d'un hypergraphe

Les hypergraphes sont plus difficiles à représenter sur papier qu'un graphe. Par contre, on peut s'y prendre ainsi : on représente B_i par un trait plein entourant ses éléments si $|B_i| > 2$; par un trait continue joignant ses deux éléments si $|B_i| = 2$, tout comme l'arête d'un graphe ; finalement, si B_i est un *singleton* (c'est-à-dire que $|B_i| = 1$), on le représente par un trait plein entourant l'unique sommet contenu par l'arête. À la figure 1.2, nous voyons une représentation d'hypergraphe classique. L'hypergraphe est donné explicitement par

$$H := (\{p_i\}_{1 \leq i \leq 7}, \{\{p_1, p_2, p_3\}, \{p_3, p_5, p_6\}, \{p_2, p_3\}, \{p_6, p_7\}, \{p_4\}\})$$

.

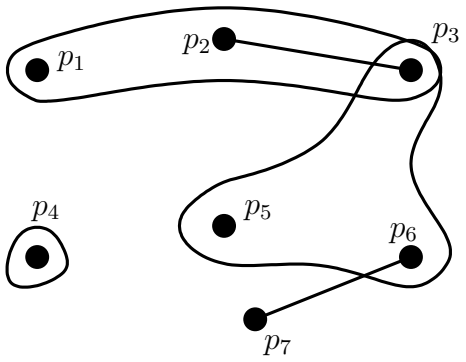

FIG. 1.2 – Représentation classique d'un hypergraphe simple

Cependant, il est possible de déroger à cette convention lorsque le contexte est clair. Voici un exemple fort important qui en témoigne.

Exemple 1.2 Prenons comme ensemble de sommets $V := \{0, 1, 2, 3, 4, 5, 6\}$ et comme ensemble d'arêtes $\mathbf{B} := \{\{0, 1, 3\}, \{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}\}$.

Nous représentons cet hypergraphe $PG(2,2) := (V, \mathbf{B})$ à la figure 1.3, en utilisant des segments de droite (les arêtes), contenant chacun trois points et un cercle contenant lui aussi trois points.

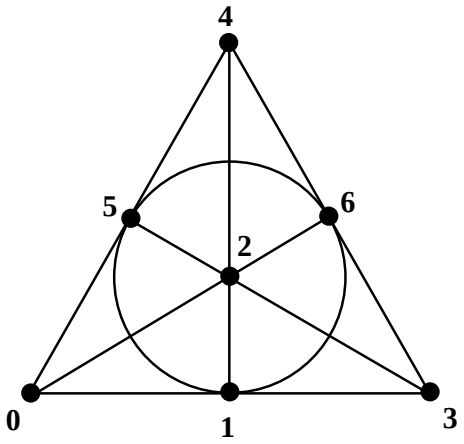

FIG. 1.3 – Une autre représentation d'hypergraphe : il s'agit du plan projectif fini d'ordre 2. On le note $PG(2,2)$.

Plus généralement, nous utilisons n'importe quelles courbes dans le plan pour illustrer la relation entre les sommets et les arêtes.

1.1.3 Nomenclature des hypergraphes

Si les B_i sont tous différents, on dira que l'hypergraphe $\mathcal{H}$ est *simple* (et B est un sous-ensemble de l'ensemble puissance de V). Dans le cas contraire, l'hypergraphe est dit *multiple*. Si $|B_i| = 2$ pour tout i, un hypergraphe simple devient un graphe simple (sans sommets isolés par les conditions (1.1)). Dans un hypergraphe, deux sommets p et q sont dits *adjacents* s'il existe une arête B_i qui les contient tous les deux ; deux arêtes B_i et B_j sont dites *adjacentes* si leur intersection est non vide. Nous dirons qu'un sommet p est *incident* à une arête B si l'arête contient le sommet p et inversement, une arête B est *incidente* à un sommet p si le sommet p est contenu dans l'arête B.

Voici maintenant quelques définitions fondamentales qui sont à la base de la théorie des designs. Elles permettent de caractériser les hypergraphes ayant des propriétés plus intéressantes.

En premier lieu, on définit le *degré* $d(p_i)$ d'un sommet $p_i \in V$ par le nombre d'arêtes qui contiennent le sommet p_i. Un hypergraphe $\mathcal{H}$ sera dit *régulier*, si $d(p_i) = d(p_j)$ pour tous les $p_i, p_j \in V$. Dans le même esprit, $\mathcal{H}$ sera dit *r-régulier*, si $\mathcal{H}$ est régulier avec un degré commun r. Ensuite, un hypergraphe $\mathcal{H}$ sera *uniforme*, si $|B_i| = |B_j|$ pour toutes les $B_i, B_j \in \mathbf{B}$. Finalement, $\mathcal{H}$ sera *k-uniforme*, si $\mathcal{H}$ est uniforme avec des arêtes contenant k sommets.

À l'aide de ces définitions, il est possible de redéfinir les graphes à l'aide des hypergraphes. Un graphe G est un hypergraphe 2-uniforme et un graphe simple est un hypergraphe simple 2-uniforme.

1.1.4 Isomorphisme, matrice d'incidence et dual

La notion d'isomorphisme se définit comme en théorie des graphes.

Définition 1.3 Deux hypergraphes $\mathcal{H}$ et $\mathcal{K}$ sont dits *isomorphes* (nous noterons $\mathcal{H} \cong \mathcal{K}$) s'il existe une bijection entre leurs ensembles de sommets qui préserve les arêtes.

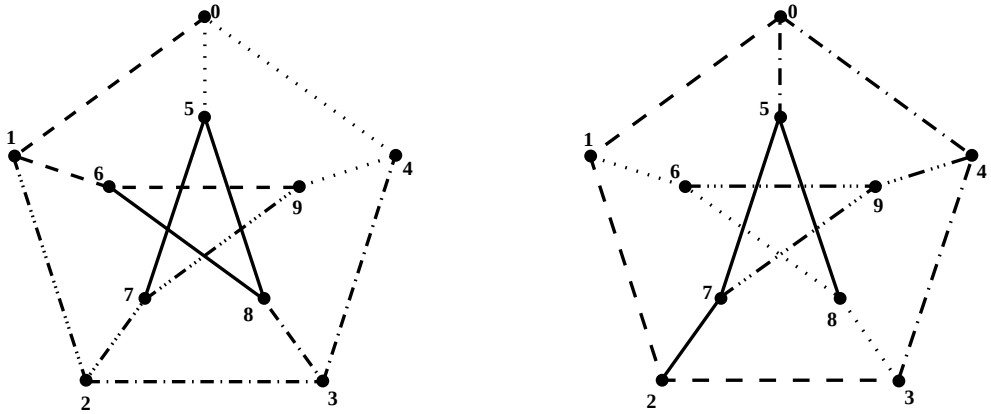

FIG. 1.4 – Les hypergraphes $H1$ et $H2$ sont isomorphes. Notons que les arêtes sont données par les différents styles de segments.

La figure 1.4 illustre deux hypergraphes isomorphes $H1$ et $H2$. La bijection entre les sommets de $H1$ et ceux de $H2$ est donné par la permutation suivante (sous représentation cyclique).

$$\begin{aligned} \Phi : V_{H1} &\rightarrow V_{H2} \\ \Phi &:= (0)(1)(26)(39)(4)(5)(78) \end{aligned}$$

Remarque 1.4 Pour que l'isomorphisme soit bien défini, il doit être indépendant du choix des arêtes. En quelque sorte, on doit pouvoir renommer les arêtes à notre guise.

La prochaine notion nous permettra d'éclaicir cette idée.

Définition 1.5 À chaque hypergraphe $\mathcal{H}$, on peut associer une *matrice d'incidence* $M_{\mathcal{H}}(\mathbf{Z}_2)$[1] avec $b := |I|$ vecteurs-colonnes représentant les arêtes, v vecteurs-lignes représentant les sommets et ayant les coefficients :

$$m_{ij} := \begin{cases} 1 & \text{si } v_i \in B_j\,; \\ 0 & \text{si } v_i \notin B_j. \end{cases}$$

De plus, il est clair que toute matrice binaire est la matrice d'incidence d'un hypergraphe : pour respecter les conditions (1.1) la matrice ne doit pas contenir de vecteur-colonne nul ni de vecteur-ligne nul. En exemple, la figure 1.5 montre la matrice d'in-

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \left(\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right) \end{array}$$

FIG. 1.5 – La matrice d'incidence de PG(2,2)

cidence de $PG(2,2)$ présenté à l'exemple 1.2. La notion d'isomorphisme peut être interprétée par rapport aux matrices d'incidences. Avant d'établir la relation, voici une définition utile pour arriver au résultat.

Définition 1.6 Une *matrice de permutation* est une matrice binaire carrée de dimension n ayant exactement une entrée non-nulle dans chaque colonne et chaque ligne.

[1]Une section explorant les notions fondamentales des corps finis est présente en appendice

Chacune de ces matrices représente une certaine permutation de n éléments. En multipliant un matrice donnée par une matrice de permutation, on permute les colonnes ou les lignes de la matrice donnée.

Nous notons par P_n l'ensemble des matrices de permutation. Il est clair que les matrices de permutation forment un groupe $(P_n, \cdot)$ (non commutatif pour $n > 2$) isomorphe au groupe de symétrie sur n éléments, S_n.

En examinant la définition 1.3, nous voyons clairement que deux hypergraphes $\mathcal{H}$ et $\mathcal{K}$ d'ordre v ayant b arêtes, sont isomorphes si et seulement s'il existe deux matrices de permutation $L \in P_v$ et $C \in P_b$ telles que $L \cdot M_{\mathcal{H}} \cdot C = M_{\mathcal{K}}$. Nous définissons donc une relation d'équivalence sur l'ensemble des hypergraphes qui nous permet de simplifier l'étude des hypergraphes.

Proposition 1.7 Le concept d'isomorphisme induit une relation d'équivalence $\sim$ sur l'ensemble des hypergraphes. La relation est définie comme suit :

$$\mathcal{H} \sim \mathcal{K} \quad \Leftrightarrow \quad \exists L_{v\times v} \in P_v, C_{b\times b} \in P_b \text{ telles que } L \cdot M_{\mathcal{H}} \cdot C = M_{\mathcal{K}}$$

Démonstration. La reflexivité, la transitivité et la symétrie de $\sim$ se déduisent des propriétés de groupe de P_v et P_b.

■

Ensuite, à tout hypergraphe $\mathcal{H} = (V, \{B_1, B_2, \ldots, B_b\})$, correspond un hypergraphe $\mathcal{H}^* := (\mathbf{B}, \{V_1, V_2, \ldots, V_v\})$, dont les sommets sont des points $b_1, b_2, \ldots, b_b$ (représentant respectivement $B_1, B_2, \ldots, B_b$), et les arêtes des ensembles $V_1, V_2, \ldots, V_v$ (représentant respectivement $v_1, v_2, \ldots, v_v$), où :

$$V_j \quad := \quad \{b_i : v_j \in B_i\}_{i \leq b} \qquad (j = 1, 2, \ldots, v).$$

Les conditions (1.1) sont satisfaites puisque $V_j \neq \varnothing$ et $\bigcup_j V_j = \mathbf{B}$. L'hypergraphe $\mathcal{H}^*$ est appelé l'*hypergraphe dual* de $\mathcal{H}$. Il est clair que la matrice d'incidence de $\mathcal{H}^*$ est la transposée de $M_{\mathcal{H}}$. Donc, en particulier $(\mathcal{H}^*)^* \cong \mathcal{H}$. Il y a une bijection f entre les sommets de $\mathcal{H}$ et les arêtes de $\mathcal{H}^*$ et une bijection g entre les arêtes de $\mathcal{H}$ et les sommets de $\mathcal{H}^*$. Enfin, la définition nous donne clairement que $\mathcal{H}^*$ est unique à un isomorphisme

près. Il est possible de traduire les concepts concernant un hypergraphe aux concepts concernant son dual. Voici quelques exemples :

$\mathcal{H}$	$\mathcal{H}^*$
$p \in B$	$f(p) \ni g(B)$
$d(p)$	$\|f(p)\|$
$\|B\|$	$d(g(B))$
r-régulier	r-uniforme
k-uniforme	k-régulier

TAB. 1.1 – *Traduction entre les concepts d'hypergraphe et son dual*

Nous montrons immédiatement un exemple de dualité à la figure 1.6. Nous reviendrons sur la dualité un peu plus loin dans ce chapitre avec un autre exemple.

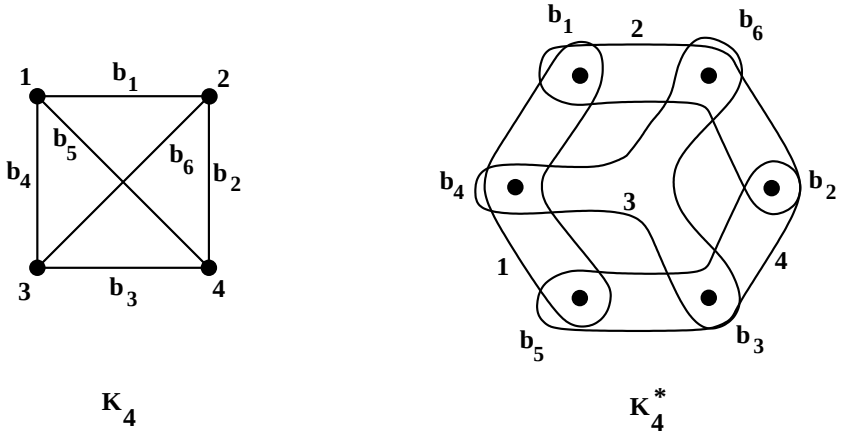

FIG. 1.6 – L'hypergraphe K_4 possède un dual ${K_4}^*$ représenté ici de façon classique.

1.1.5 Théorème général

Comme nous l'avons constaté, les hypergraphes ouvrent la porte à une multitude de possibilités. Malgré ce fait, un théorème s'applique à tout hypergraphe.

Théorème 1.8 Pour tout hypergraphe $\mathcal{H} = (V, \mathbf{B})$, nous avons

$$\sum_{p \in V} d(p) \quad = \quad \sum_{B \in \mathbf{B}} |B|. \tag{1.2}$$

Démonstration. Considérons la matrice d'incidence $M_{\mathcal{H}}$ de $\mathcal{H}$. Nous allons procéder à une double énumération. D'abord, pour chaque ligne de $M_{\mathcal{H}}$, $d(p)$ représente la somme de la ligne représentant le sommet p. En sommant chaque ligne, nous obtenons la somme des cellules de $M_{\mathcal{H}}$. Ensuite, pour chaque colonne de $M_{\mathcal{H}}$, $|B|$ représente la somme de la colonne qui représente B. Finalement, en sommant toutes les colonnes, nous arrivons à la même somme.

■

Voici un corollaire immédiat du théorème.

Corollaire 1.9 Soit $\mathcal{H} = (V, \mathbf{B})$ un hypergraphe d'ordre v ayant b arêtes qui est r-régulier et k-uniforme. Alors

$$vr = bk. \quad \blacksquare \tag{1.3}$$

Malgré sa simplicité, le principe de la double énumération se révèle parfois comme un outil extrêmement puissant pour déduire des égalités plus complexes. Le cas $b = 2$ montre qu'il s'agit en fait d'une généralisation du *Lemme des poignées de main* de la théorie des graphes.

Avant de procéder aux exemples d'hypergraphes illustrant les notions introduites, on complète avec une remarque à propos des hypergraphes en général. Les hypergraphes peuvent être facilement représentés à l'aide des graphes. En effet, les hypergraphes ne sont rien d'autres que des graphes biparties. Il suffit de représenter les sommets de $\mathcal{H}$ d'un côté et les arêtes de l'autre et ensuite, de relier chacune des arêtes avec chacun des sommets qui la composent. Cette forme sera celle privilégiée lors de la définition des designs. Il s'agit là d'un aspect parfois utile lors de démonstrations et il est important d'en saisir toute la portée.

1.2 Exemples d'hypergraphes

L'objectif de ce chapitre est de se familiariser avec les hypergraphes et de s'habituer aux principes qu'ils engendrent. Afin de devenir à l'aise avec cette théorie, on trouve dans cette section des exemples importants qui font appel aux notions développées. Parmi ces exemples se cachent déjà des designs, que nous identifierons plus tard. Pour

l'instant, il est important de bien comprendre les idées ainsi que la nomenclature, car les designs requièrent beaucoup de vocabulaire pour être bien définis.

Exemple 1.10 Soient $r, n \in \mathbb{N}$ tels que $1 \leq r \leq n$. Un exemple relativement simple est l'*hypergraphe uniforme complet* K_n^r d'ordre n. Les arêtes de cet hypergraphe sont tous les sous-ensembles de r sommets parmi les n. Ainsi, K_n^r possède $\binom{n}{r}$ arêtes et il est aussi $\binom{n-1}{r-1}$-régulier. Si $r = 2$, alors K_n^2 devient K_n le graphe complet sur n sommets.

Poursuivons avec des exemples plus complexes d'hypergraphes. Nous donnons ici leurs définitions et leurs caractéristiques remarquables.

Exemple 1.11 (Plan affin d'ordre 3) Soit

$$AG(2,3) \quad := \quad \left(\mathbf{Z}_9, \left\{ \begin{array}{l} \{3n, 3n+1, 3n+2\} \bmod 9, \{3n+2, 3n+3, 3n-2\} \bmod 9, \\ \{3n-1, 3n+1, 3n+3\} \bmod 9, \{n, n+3, n+6\} \bmod 9 \end{array} \right\} \right).$$

Nous justifierons la notation $AG(2,3)$ dans le prochain chapitre. Cet hypergraphe est 3-uniforme, 4-régulier et simple.

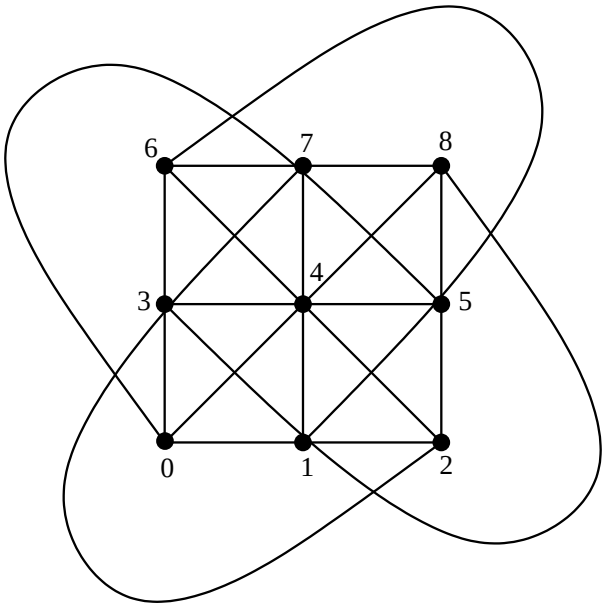

FIG. 1.7 – Une représentation de $AG(2,3)$

Exemple 1.12 Soit $\mathcal{H} := (\mathbf{Z}_6, \{\{0,3\}, \{0,3\}, \{1,4\}, \{2,5\}, \{0,1,2\}, \{3,4,5\}, \{1,2,4,5\}\})$. Cet hypergraphe est 3-régulier et multiple. Remarquons qu'il n'est pas uniforme par la présence d'arêtes incidentes à des nombres différents de sommets.

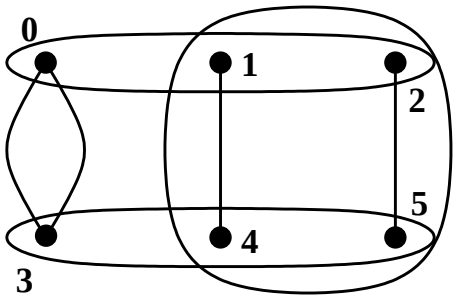

FIG. 1.8 – Un hypergraphe 3-régulier multiple d'ordre 6

Nous constatons tout l'éventail de possibilités que nous offrent les hypergraphes. Par contre, puisque toute théorie est née d'un questionnement ou d'un besoin, les hypergraphes que nous traiterons possèderont plusieurs propriétés d'incidences qui reflètent des situations données par un problème.

Ainsi, revenons sur l'hypergraphe $PG(2,2)$ illustré à la figure 1.3. Cet hypergraphe est 3-uniforme et 3-régulier. De plus, on peut remarquer que chaque paire d'arêtes sont incidentes en un et un seul sommet. De plus, toujours dans $PG(2,2)$ chaque paire de sommets est contenue dans une unique arête. Cette dernière propriété se retrouve aussi dans l'exemple 1.11. Ces propriétés seront étudiées en abordant les premiers exemples de design que sont les *plans projectifs finis* et les *plans affins finis*. Constatons finalement que $PG(2,2)$ est *autodual*, c'est-à-dire que $PG(2,2)^* \cong PG(2,2)$. Également, cela veut dire que la matrice d'incidence de $PG(2,2)$ est une matrice symétrique. À la figure 1.5, nous voyons la symétrie par rapport à l'axe secondaire de la matrice, il suffit de renverser l'ordre des colonnes (à l'aide des matrices de permutations) et nous obtenons la matrice symétrique.

Maintenant que nous avons introduit comme il se doit les hypergraphes, nous passons à l'objet principal de notre étude qu'est la théorie des designs.

Chapitre 2

Théorie des designs

Au chapitre précédent, nous avons vu quelques exemples de designs. Nous avons découvert de nouvelles propriétés en les examinant. Les deux propriétés portent sur l'incidence des sommets et des arêtes entre eux. En effet, dans les exemples 1.2 et 1.11, deux sommets distincts sont incidents en une unique arête. De plus, pour le plan projectif, il en est de même pour son dual. Autrement dit, deux arêtes distinctes sont incidentes en un unique sommet. Nous verrons comment ces propriétés mènent à définir les designs en examinant les structures d'incidence. Finalement, nous verrons quelques notions théoriques importantes.

2.1 Structures d'incidence

Un exemple très simple de géométrie finie est la structure d'incidence. En géométrie, on parle souvent de points, lieux de points, de leurs intersections, etc. Une structure d'incidence permet de caractériser les diverses possibilités d'incidence entre deux classes d'objets.

Définition 2.1 Une *structure d'incidence* est un triplet $\mathbf{D} = (V, \mathbf{B}, I)$, où V et $\mathbf{B}$ sont deux ensembles quelconques disjoints et I est une relation binaire entre V et $\mathbf{B}$, c'est-à-dire que $I \subseteq V \times \mathbf{B}$. Les structures d'incidence sont similaires aux hypergraphes. Par contre, les éléments de V seront appelés des *points*, ceux de $\mathbf{B}$ des *blocs* et ceux de I des *étiquettes*. L'*ordre* d'une structure est le nombre $v = |V|$. Au lieu d'écrire $(p, V) \in I$, nous écrirons plutôt pIB et nous dirons que le point p *appartient* au bloc B, B *passe*

par p, p et B sont *incidents*. Finalement si $(p, V) \notin I$, nous écrirons $p \not I B$.

Nous justifions maintenant la notation adoptée lors du premier chapitre. Pour éviter la confusion, les points seront toujours notés par des lettres minuscules $p, q, r, ...$ et les blocs par des lettres majuscules $B, C, \ldots$. Tout le long du présent texte, la plupart des paramètres seront représentés par les conventions adoptées par les théoriciens des designs.Les conventions sont celles présentes dans le livre de Thomas Beth, Dieter Jungnickel et Hanfried Lenz [Beth]. Selon nos définitions, toute relation entre deux ensembles nous donne un exemple de structure d'incidence. Naturellement, les structures d'incidences sont beaucoup trop générales pour avoir un intérêt en elles-mêmes. Appuyés par les exemples du précédent chapitre, nous verrons quelles sont les structures qui nous intéressent. Auparavant, voici encore quelques conventions d'écriture. Si p est un point quelconque, (p) représentera l'ensemble des blocs qui lui sont incidents, c'est-à-dire

$$(p) \quad := \quad \{B \in \mathbf{B} : pIB\}, \tag{2.1}$$

et plus généralement pour tout sous-ensemble $Q \subset \mathbf{V}$,

$$(Q) \quad := \quad \{B \in \mathbf{B} : pIB \quad \forall p \in Q\}. \tag{2.2}$$

Lorsque le contexte sera clair, nous écrirons simplement $(p_1, \ldots, p_m)$ au lieu de $(\{p_1, \ldots, p_m\})$. De plus, nous écrirons aussi

$$(\mathbf{C}) \quad := \quad \{p \in V : pIB \quad \forall B \in \mathbf{C}\}, \tag{2.3}$$

pour tout sous-ensemble $\mathbf{C} \subset \mathbf{B}$. Remarquons que le degré d'un point est aussi donné par $|(p)|$. De plus, nous dirons que D est *simple* si $(B) \neq (C)$ pour toute paire de blocs distincts. Finalement, nous appellerons la *grandeur*[1] d'un bloc B le nombre $|(B)|$ (voir la définition en (2.3)). Dans la suite, nous simplifierons la notation en omettant la relation d'incidence I. Ainsi, nous écrirons plus souvent $\mathbf{D} = (V, \mathbf{B})$ au lieu de $\mathbf{D} = (V, \mathbf{B}, I)$ même si $\mathbf{D}$ n'est pas simple.

Nous terminons cette section par un premier résultat non trivial. Nous allons maintenant établir l'existence de structures d'incidence simples r-régulières et k-uniformes. Nous voyons la démonstration de David Billington formulée en 1982. En premier lieu nous avons besoin d'un lemme.

[1] *block-size* en anglais.

Lemme 2.2 Supposons qu'il existe une structure d'incidence simple $\mathbf{D}$ k-uniforme d'ordre v ayant b blocs et des degrés $r_1, \ldots, r_v$. Si $r_i > r_j$ pour un certain couple (i, j) avec $i > j$, alors il existe une structure d'incidence simple $\mathbf{D}'$ k-uniforme de degré v ayant b blocs et des degrés $r_1, \ldots, r_i - 1, r_{i+1}, \ldots, r_{j-1}, r_j + 1, \ldots, r_v$.

Démonstration. L'hypothèse $r_i > r_j$ implique que $\mathbf{D}$ possède plus de blocs contenant le point p_i mais pas p_j que de blocs contenant p_j mais pas p_i. Ainsi, nous sommes garantis d'avoir un bloc B de $\mathbf{D}$ qui contient p_i mais pas p_j et tel que $B' := (B \backslash \{p_i\}) \cup \{p_j\}$ n'est pas un bloc de $\mathbf{D}$. Maintenant, nous remplaçons le bloc B par B' et nous obtenons la structure $\mathbf{D}'$.

■

Théorème 2.3 Une structure d'incidence simple, r-régulière, k-uniforme, d'ordre v et ayant b blocs existe si et seulement si

$$vr = bk \quad \text{et} \quad b \leq \binom{v}{k}. \tag{2.4}$$

Démonstration. Par le corollaire 1.9 et puisque nous voulons que la structure soit simple, les conditions (2.4) sont clairement nécessaires à l'existence d'une telle structure. Maintenant, supposons que nous avons les conditions (2.4), pour certains entiers k, r, v, b. Nous définissons une structure $\mathbf{D}_0$ en choisissant un ensemble quelconque de b sous-ensembles contenant k éléments $\{B_1, \ldots, B_b\}$ à partir de l'ensemble $V = \{p_1, \ldots, p_v\}$. Nous les choisissons aussi deux à deux disjoints. Notons les degrés des points de V par $r_1, \ldots, r_v$; clairement nous avons

$$vr = bk \quad = \quad r_1 + \cdots + r_v. \tag{2.5}$$

Si tous les points sont de degré r, nous avons terminé. Sinon, nous appliquons le lemme 2.2 pour réduire de 1 un degré plus grand que r tout en augmentant de 1 le degré d'un autre point plus petit que r. En appliquant ce processus récursivement, nous obtenons la structure simple désirée $\mathbf{D}$.

■

2.2 Les designs et les géométries projectives et affines

Maintenant, nous finalisons l'étude des exemples de la section 1.2 laquelle nous menera vers les concepts fondamentaux de la théorie des designs. Nous examinerons attentivement les géométries affines et projectives en démontrant certaines propriétés.

2.2.1 Géométrie projective

D'abord, voici la définition d'un plan projectif.

Définition 2.4 Une structure d'incidence $\mathbf{D} = (V, \mathbf{B}, I)$ est appelée un *plan projectif* si et seulement si elle satisfait les axiomes suivants[2] :

- Toute paire de points distincts sont rejoints par exactement une ligne. (2.6)
- Toute paire de lignes distinctes se croisent en un unique point. (2.7)
- Il existe un *quadrangle*, c'est-à-dire quatre points tels qu'il n'y a pas trois points de ceux-ci qui sont colinéaires. (2.8)

Nous avons déjà rencontré un exemple de plan projectif au dernier chapitre. C'était l'hypergraphe $PG(2, 2)$ (nous justifions maintenant la notation PG qui vient de l'anglais *projective geometry*, les variables seront justifiées plus tard au cours de cette section) avec 7 points et 7 lignes représenté à la figure 1.3. Il est facile de se convaincre qu'il est le plus petit plan projectif fini possible. Comme nous l'avions remarqué précédemment, cette structure d'incidence est 3-régulière et 3-uniforme. Nous voyons maintenant pourquoi il en est ainsi.

Proposition 2.5 Soit $\mathbf{D} = (V, \mathbf{B}, I)$ un plan projectif fini. Alors il existe un nombre naturel n, appelé *l'ordre* de $\mathbf{D}$, qui satisfait :

$$|(p)| = |(G)| = n + 1 \qquad \text{pour tout } p \in V \text{ et } G \in \mathbf{B}; \tag{2.9}$$

$$|V| = |\mathbf{B}| = n^2 + n + 1. \tag{2.10}$$

[2]En géométrie, on parle habituellement de *ligne* au lieu de *bloc*. Nous utiliserons les deux termes selon le contexte.

Démonstration. Considérons un point quelconque p et une ligne G avec $p \not I G$. Par (2.6) et (2.7), l'application $\pi : (G) \to (p)$ avec $\pi(q) := pq$ pour tout qIG est une bijection (ici, pq représente l'unique ligne passant par p et q). Ainsi, $|(p)| = |(G)|$ lorsque $p \not I G$. Par conséquent, l'axiome (2.6) sera satisfait si nous pouvons montrer que pour toute paire de lignes distinctes G, H il y a un point tel que $p \not I G, H$. En effet, en prenant un point p incident à une ligne G et un point q tel que $q \not I G$, alors en considérant pq et G, il existe un point qui leur est non incident, ainsi $|(pq)| = |(G)|$. De plus, en prenant $r \neq p$ tel que rIG, on trouve aussi que $|(pq)| = |(rq)|$. Ainsi, puisque $|(p)| = |(qr)|$, nous avons l'égalité $|(p)| = |(G)|$, comme voulu. Démontrons donc que pour toute paire de lignes distinctes, il existe un point qui ne leur est pas incident. Par (2.8), il existe un quadrangle s, t, u, v. Si chaque point est incident à G ou H, nous pouvons supposer que s, tIG et u, vIH. Alors nous pouvons choisir p comme le point à l'intersection de su et tv. Pour vérifier (2.10), nous utilisons la double énumération. Nous choisissons un point p et nous comptons les étiquettes (q, G) avec pIG et $p \neq q$. Par (2.6), nous obtenons $|V| - 1$ tels étiquettes ; et par (2.9) nous avons $(n+1)n$ tels étiquettes. Ainsi, $|V| = n^2 + n + 1$. L'égalité pour $|\mathbf{B}|$ suit de façon similaire (ou en utilisant (2.9), la valeur de $|V|$ et (1.3)).

■

Voici une proposition montrant l'existence d'une classe infinie de plans projectifs finis. Étant donnée une structure d'incidence $\mathbf{D} = (V, \mathbf{B})$, nous dirons qu'un sous-ensemble U de V est un *sous-espace* si chaque bloc de $\mathbf{D}$ est soit contenue complètement dans U ou bien incidente à U en un et un seul point.

Proposition 2.6 Soit $q = p^f$, où p est un nombre premier et f un entier positif. Alors, il existe un plan projectif d'ordre q.

Démonstration. Considérons le corps fini $F = GF(q)$ et W l'espace vectoriel de dimension 3 sur F. Choisissons tous les sous-espaces de W de dimension 1 pour représenter les points et tous les sous-espaces de W de dimension 2 pour les lignes. En utilisant la formule de dimension de l'algèbre linéaire, nous voyons que les axiomes (2.6) et (2.7) sont satisfaits. Pour le dernier axiome, nous choisissons e_1F, e_2F, e_3F et $(e_1+e_2+e_3)F$ où e_1, e_2, e_3 est une base de W.

■

En fait, cet argument fonctionne pour tout espace vectoriel de dimension 3. Le fait que F soit un corps est nécessaire seulement pour montrer que le plan projectif est d'ordre q :

le nombre de sous-espaces de dimension 1 de W est donc $(q^3-1)/(q-1) = q^2+q+1$. Le plan projectif fini qui vient d'être construit sera noté $PG(2,q)$.

2.2.2 Géométrie affine

Voyons maintenant les géométries affines.

Définition 2.7 Une structure d'incidence $\mathbf{D} = (V, \mathbf{B}, I)$ est un *plan affin* si et seulement si elle satisfait les axiomes suivants :

- Toute paire de points distincts sont rejoints par exactement une ligne (2.11)
- Étant donné un point p et une ligne G tel que $p \not I\, G$, il y a exactement une ligne H tel que pIH qui n'est pas adjacente à G (2.12)
- La structure possède un *triangle*, c'est-à-dire trois points non colinéaires. (2.13)

Dans la suite, nous dirons que deux lignes G et H sont *parallèles* si $G = H$ ou $|(G,H)| = 0$, et nous écrivons $G \parallel H$. Ainsi, la condition (2.12) est l'axiome d'Euclide concernant les parallèles. Voyons donc comment on caractérise les plans affins.

Proposition 2.8 Soit $\mathbf{D} = (V, \mathbf{B}, I)$ un plan affin. Alors le parallélisme est une relation d'équivalence sur $\mathbf{B}$. Si $\mathbf{D}$ est fini, il existe un nombre naturel n (appelé l'ordre de $\mathbf{D}$) qui satisfait :

$$|(p)| = n+1 \qquad \text{pour tout point } p; \tag{2.14}$$

$$|(G)| = n \qquad \text{pour toute ligne } G; \tag{2.15}$$

$$|V| = n^2, \qquad |\mathbf{B}| = n^2+n. \tag{2.16}$$

Démonstration. Il reste seulement à vérifier la transitivité de $\parallel$ (les autres conditions découlent de la définition). Ainsi, supposons que $G \parallel H$ et $H \parallel K$. Sans perte de généralité, nous supposons que G, H et K sont mutuellement distinctes. Si $G \not\parallel K$, il y aurait un point p incident à G et K ; mais alors G et K seraient deux parallèles de H passant par p, ce qui contredit (2.12). Le reste de la démonstration est similaire à la démonstration de la proposition 2.5 et se déduit facilement. ■

Nous pouvons aussi trouver une famille infinie de plans affins en montrant qu'ils sont similaires aux plans projectifs. Avant de procéder à la démonstration nous avons besoin d'une définition.

Définition 2.9 Soient $\mathbf{D} = (V, \mathbf{B}, I)$ une structure d'incidence, $Q \subseteq V$ et $\mathbf{C} \subseteq \mathbf{B}$. Alors, la structure d'incidence *induite* par $\mathbf{D}$ sur Q et $\mathbf{C}$ est $D' = (Q, \mathbf{C}, I|Q \times \mathbf{C})$, et $\mathbf{D}'$ est appelée sous-structure induite de $\mathbf{D}$. Au lieu de $I|Q \times \mathbf{C}$, nous écrirons encore I.

Proposition 2.10 Soient $\mathbf{D} = (V, \mathbf{B})$ un plan projectif et G une ligne de $\mathbf{D}$. Alors la sous-structure $\mathbf{D}_G = (V \setminus (G), \mathbf{B} \setminus \{G\}, I)$ est un plan affin. Inversement, tout plan affin peut être obtenu de cette façon à partir d'un plan projectif. Dans le cas fini, les ordres des plans (et non l'ordre des structures) $\mathbf{D}$ et $\mathbf{D}_G$ sont égaux.

Démonstration. Fixons un plan projectif $\mathbf{D}$ et enlevons une ligne U de même que tous ces points. Alors $\mathbf{D}_U$ satisfait (2.11), puisque $\mathbf{D}$ satisfait (2.6). Maintenant, soient p un point et G une ligne de $\mathbf{D}_U$ tels que $p \not I\, G$. Si q est le point d'intersection de G et U dans $\mathbf{D}$, alors la ligne pq est la parallèle de G recherchée passant par p. Elle est certainement unique. Ensuite, la condition (2.13) suit par (2.8) et du fait qu'il existe un point qui n'est pas incident à deux lignes données (voir la démonstration de la proposition 2.5).

Inversement, étant donné un plan affin, nous obtenons un plan projectif. Nous ajoutons un point pour chaque classe de lignes parallèles. Ensuite, nous ajoutons une ligne (« la ligne à l'infini ») qui passe par chacun des points ajoutés. De plus, chaque point ajouté sera incident à chaque ligne contenue dans la classe de parallèles qu'il représente. Nous pouvons voir cette construction en décrétant que chaque ligne parallèle se rencontre en un certain point à l'infini. Il est clair par la construction que le résultat est bien un plan projectif et que nous retrouvons le plan affin en supprimant la ligne à l'infini.

■

Nous remarquons que le plan projectif créé à partir du plan affin est en fait unique à un isomorphisme près contrairement aux plans affins obtenus à partir d'un plan projectif donné ; deux plans affins non isomorphes peuvent être construits, selon la ligne qui est supprimée. Voici un corollaire immédiat des propositions 2.6 et 2.10.

Corollaire 2.11 Pour chaque puissance première q, il existe un plan affin d'ordre q.

■

Les plans affins peuvent aussi être construits de façon similaire à la démonstration de la proposition 2.6. On utilise alors un espace vectoriel de dimension 2 sur le corps F et on pose les points comme étant les vecteurs et les lignes comme les classes de sous-espaces de dimension 1.

2.2.3 Designs

Nous passons maintenant à la généralisation des propriétés (en remplaçant « exactement une » par « exactement λ » dans (2.11) et (2.6)) des plans affins et projectifs en arrivant à la définition d'un design.

Définition 2.12 Une structure d'incidence $\mathbf{D} = (V, \mathbf{B})$ finie est appelée un *design* avec paramètres v, k, λ ($v, k, \lambda \in \mathbb{N}$) si elle satisfait les conditions suivantes :

- $|V| = v$; (2.17)
- $|(p, q)| = \lambda$ pour tout $p, q \in V, p \neq q$, c'est-à-dire que toute paire de points sont joints par exactement λ blocs ; (2.18)
- $|(B)| = k$ pour tout bloc B. (2.19)

Pour des raisons historiques que nous verrons plus loin, nous appellerons souvent $\mathbf{D}$ un $S_\lambda(2, k; v)$ ou dans le cas $\lambda = 1$ simplement $S(2, k; v)$. Ainsi dans cette notation, les plans projectifs d'ordre n sont des exemples de $S(2, n+1, n^2+n+1)$ et les plans affins sont des $S(2, n, n^2)$. En fait, ils sont les seuls exemples avec ces paramètres. Nous avons trouvé des exemples de plans projectifs pour des ordres $q = p^f$, où p est un nombre premier et f un entier positif. À ce jour, nous ne savons pas s'il existe des plans projectifs d'ordre quelconque. Par contre, nous savons qu'il n'existe pas de plan projectif d'ordre 6 et 10.[3] En voyant la définition d'un design, on constate qu'il n'y a aucune condition regardant le degré constant de chaque point, pourtant les exemples montraient cette constance. En fait, elle est une conséquence de la définition.

[3]Le plan projectif d'ordre 6 n'existe pas par le puissant théorème de Bruck-Ryser-Chowla. Aussi, Clement W.H. Lam de l'Université Concordia a montré en 1989 qu'il n'existe pas de plan projectif d'ordre 10 à l'aide de lourds calculs informatiques.

Théorème 2.13 Soit $\mathbf{D}$ un $S_\lambda(2,k;v)$. Alors nous avons

$$|(p)| = \lambda(v-1)/(k-1) =: r \qquad \text{pour tout point } p; \tag{2.20}$$

$$|\mathbf{B}| = \lambda v(v-1)/k(k-1) =: b. \tag{2.21}$$

Démonstration. Fixons p un point de $\mathbf{D}$. Nous y allons d'une double énumération. Comptons les étiquettes (q,G) avec pIG et $q \neq p$ de deux façons. Nous obtenons $\lambda(v-1) = |(p)|(k-1)$ par (2.17), (2.18) et (2.19). Nous avons donc (2.20), de plus (2.21) suit de (1.3) en utilisant (2.20).

■

Puisque r et b doivent être des entiers positifs, nous avons

Corollaire 2.14 Soient $v,k,\lambda \in \mathbb{N}$. Alors les conditions suivantes sont nécessaires pour l'existence d'un $S_\lambda(2,k;v)$

$$\lambda(v-1) \equiv 0 \pmod{k-1}; \tag{2.22}$$

$$\lambda v(v-1) \equiv 0 \pmod{k(k-1)}. \tag{2.23}$$

La recherche de conditions suffisantes pour l'existence des designs prend une place prépondérante en théorie des designs. En fait, il a été démontré par Haim Hanani au cours des années 1960 que les conditions (2.22) et (2.23) sont suffisantes pour $k = 3, 4$ et 5 avec une seule exception pour $k = 5$. De plus, Richard Wilson en 1975 a montré que ces conditions sont asymptotiquement suffisantes, c'est-à-dire qu'elles sont suffisantes pour tout v suffisamment grand, étant donnés les entiers positifs k et λ.

Les espaces affins et projectifs fournissent encore plus d'exemples de designs en généralisant leurs constructions. Nous verrons comment on les construit, mais l'argumentation permettant de montrer qu'ils sont des designs sera laissée de côté puisqu'elle ne présente pas d'élément essentiel.

Définition 2.15 Soient F un corps et W un espace vectoriel de dimension n sur F. Alors l'ensemble de toutes les classes de sous-espaces de W est appelé l'*espace affin de dimension n* sur F. Si F est un corps fini à q éléments, l'espace s'écrira comme $AG(n,q)$. (AG provient de l'anglais *affine geometry*) Les classes de sous-espaces de dimension zéro sont appelées les *points*, celles de dimension un, les *lignes*, celles de dimension deux, les

plans, celles de dimension $n-1$, les *hyperplans* et finalement les classes de sous-espaces de dimension i sont appelées *plans à dimension i* ou *i-plans*. En prenant les points de $AG(n,q)$ complétés des d-plans de $AG(n,q)$ on forme une structure d'incidence notée $AG_d(n,q)$ avec la relation donnée par l'inclusion des points dans les d-plans. Par abus de notation, on note souvent $AG(n,q)$ au lieu de $AG_1(n,q)$.

Proposition 2.16 La structure d'incidence $AG_d(n,q)$ est un design avec paramètres $v = q^n, k = q^d, r = \begin{bmatrix} n \\ d \end{bmatrix}_q, \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$ et $b = q^{n-d}\begin{bmatrix} n \\ d \end{bmatrix}_q$, où $\begin{bmatrix} n \\ i \end{bmatrix}_q$ désigne le nombre de sous-espaces de dimension i d'un espace vectoriel de dimension n sur $GF(q)$, souvent appelés coefficients gaussiens.

■

Les coefficients gaussiens sont calculés par la formule suivante. La formule découle d'un dénombrement des sous-espaces possibles. Soient q une puissance d'un nombre premier et n et d des entiers positifs tels que $d \leq n$. Alors,

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-d+1}-1)}{(q^d-1)(q^{d-1}-1)\cdots(q-1)}.$$

Ensuite, voici comment construire les espaces projectifs.

Définition 2.17 Soient F un corps et W un espace vectoriel de dimension $n+1$ sur F. Alors l'ensemble de tous les sous-espaces de W est appelé l'*espace projectif de dimension n* sur F. Si F est $GF(q)$, l'espace s'écrira comme $PG(n,q)$. Les sous-espaces de dimension 1 (respectivement dimension 2, dimension 3, dimension n) de W sont appelés les *points* (respectivement les *lignes*, les *plans*, les *hyperplans*) et de façon générale, les sous-espaces de dimension $i+1$ sont appelés *i-plans*. En prenant les points de $PG(n,q)$ complétés des $(d-1)$-plans de $PG(n,q)$ on forme une structure d'incidence notée $PG_d(n,q)$ avec la relation donnée par l'inclusion des points dans les $(d-1)$-plans. Par abus de notation, on note souvent $PG(n,q)$ au lieu de $PG_1(n,q)$.

Proposition 2.18 La structure d'incidence $PG_d(n,q)$ est un design avec paramètres $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q = (q^{n+1}-1)/(q-1), k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q = (q^{d+1}-1)/(q-1), r = \begin{bmatrix} n \\ d \end{bmatrix}_q, \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$ et $b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$.

■

Nous terminons cette section par quelques autres définitions et notations. Les designs sont définis de façon restrictive, il sera utile d'alléger les conditions (2.18) et (2.19) comme suit :

Définition 2.19 Soient λ un nombre naturel et $K \subseteq \mathbb{N}$. Une structure d'incidence $\mathbf{D} = (V, \mathbf{B})$ est appelée *design avec paires équilibrées* (DPE) possédant des blocs avec des degrés contenus dans K si et seulement si la structure satisfait aux conditions

$$|(p,q)| = \lambda \quad \text{pour toutes paires de points } p, q, p \neq q, \tag{2.24}$$

$$|(B)| \in K \quad \text{pour tout bloc } B. \tag{2.25}$$

Si $\mathbf{D}$ est d'ordre v, on le note $S_\lambda(2, K; v)$. Pour $\lambda = 1$, nous utilisons la notation plus simple $S(2, K; v)$ et on le nomme parfois *espace linéaire*. Notons qu'il n'est pas nécessaire d'avoir chaque entier de K comme degré d'un bloc. De plus, il peut arriver que K soit un ensemble infini. Dans le cas où $K = k$, nous revenons à la définition d'un design.

Finalement, voici des notations utilisées au prochain chapitre. Étant donnés un nombre naturel λ et $K \subseteq \mathbb{N}$, l'ensemble des $v \in \mathbb{N}$ pour lesquels un $S_\lambda(2, K; v)$ existe sera noté par $B(K, \lambda)$. Lorsque $\lambda = 1$, nous le notons par $B(K)$. Si $K = k$, nous le noterons simplement par $B(k)$. Nous pouvons considérer B comme un opérateur sur $2^{\mathbb{N}}$ agissant sur K en l'envoyant sur $B(K)$. Cette idée d'opérateur reviendra lorsque nous démontrerons l'existence de designs résolubles. Pour l'instant, continuons l'étude des designs.

2.3 t-designs et systèmes de Steiner

Revenons aux structures de la proposition 2.16, nous avons observé que la structure $AG_2(n, 2)$ (c'est-à-dire la structure d'incidence formée par les points et les lignes dans l'espace affin de dimension n sur $GF(2)$) est un $S_\lambda(2, 4; 2^n)$ avec $\lambda = 2^{n-1} - 1$. En particulier, deux points sont traversés par $2^{n-1} - 1$ plans. En allant encore plus loin, nous remarquons que chaque triplet détermine un unique plan. (Pour trouver cela, nous avons utilisé le fait que trois points distincts ne peuvent être colinéaires dans $GF(2)$)

Motivés par cet exemple, nous voyons maintenant la généralisation des designs.

Définition 2.20 Soient t et λ deux entiers positifs et $\mathbf{D} = (V, \mathbf{B})$ une structure d'incidence finie. Alors, $\mathbf{D}$ est appelée t-équilibrée avec paramètre λ si et seulement si

$$|(Q)| \quad = \quad \lambda \text{ pour tout t-uplet } Q \subseteq V. \tag{2.26}$$

Si $\mathbf{D}$ est d'ordre v et $|(B)| \in K$ pour tout $B \in \mathbf{B}$, alors $\mathbf{D}$ est appelé un $S_\lambda(t, K; v)$. Dans le cas où $K = k$, $\mathbf{D}$ est alors appelé un *t-design* de paramètre k et λ. Un t-design d'ordre v est noté $S_\lambda(t, k; v)$. Lorsque $\lambda = 1$, nous l'appelons « système de Steiner » $S(t, k; v)$, ce qui justifie le choix de notre notation.

Ainsi, les géométries affines et projectives sont des systèmes de Steiner. Les DPE sont des structures 2-équilibrées et les designs définis à la section précédente sont des 2-designs. Les designs $AG_2(n, 2)$ sont des exemples de 1-, 2- et 3-designs. Notons que les 1-designs sont des structures d'incidences régulières. Nous concluons cette section par une courte digression.

Nous avons vu deux représentations d'espace linéaire, $S(2, K; v)$, aux exemples 1.2 et 1.11. Pour les représenter, nous avons utilisé des lignes courbes. La proposition suivante nous affirme qu'il est nécessaire de les utiliser pour représenter les espaces linéaires.

Proposition 2.21 (Problème de Sylvester) Un système de Steiner $S(2, K; n)$ avec au moins trois points sur chaque ligne ne peut être représenté dans l'espace euclidien en utilisant seulement des segments de droites à moins que tous les points ne soient sur une même ligne.

Démonstration. Supposons le contraire et choisissons une ligne L et un point $p \notin L$ tels que la distance euclidienne de p à L soit minimal, disons d. Puisque L possède au moins trois points, il y a un triangle $\{p, a, b\}$ avec $a, b \in L$ tel que l'angle en a est au moins $\pi/2$. Ainsi, la distance de a au segment pb est plus petite que d, puisque le triangle possède un angle obtus en a. Nous avons donc trouver un point a et une ligne pb possèdant une distance euclidienne plus petite que d, ce qui constitue une contradiction, nous donnant le résultat.

■

2.4 Partition et résolubilité d'un design

Lorsque nous avons construit les plans projectifs à partir des plans affins, nous avons utilisé le parallélisme. Le parallélisme étant une relation d'équivalence, les blocs du plan affin étaient partitionnés de façon évidente. Voyons d'abord la définition d'une partition d'une structure d'incidence.

Définition 2.22 Soient $\mathbf{D} = (V, \mathbf{B})$ une structure d'incidence et $\mathbf{B} = \mathbf{B}_1 \cup \cdots \cup \mathbf{B}_m$ une partition de l'ensemble des blocs. Nous dirons que les sous-structures induites par $\mathbf{D}$ sur $\mathbf{B}_1$, $\mathbf{D}_i = (V, \mathbf{B}_i, I)$ (avec $i = 1, \ldots, m$), forment une *partition* de $\mathbf{D}$. Nous dirons aussi que $\{\mathbf{B}_1, \ldots, \mathbf{B}_m\}$ est une partition de $\mathbf{D}$. Les $\mathbf{D}_i$ (ou bien $\mathbf{B}_i$) sont appelés les *parties* de $\mathbf{D}$.

Les partitions qui nous intéressent possèdent une autre propriété que voici :

Définition 2.23 Soit $\mathbf{D}$ une structure d'incidence d'ordre v. Si une partie de $\mathbf{D}$ est un $S(1, K; v)$, elle est appelée *classe de parallèles* de $\mathbf{D}$. Si chaque partie d'une partition $\mathbf{B}_1 \cup \cdots \cup \mathbf{B}_m$ de $\mathbf{D}$ est une classe de parallèles, alors la partition est appelée une *1-factorisation*[4] et $\mathbf{D}$ est dite *résoluble*. Une 1-factorisation est aussi appelée un *parallélisme* ou une *résolution*.

Subséquemment, lorsqu'un design est résoluble cela signifie qu'il est représentable par une union disjointe de partitions de ces points. Nous terminons cette section avec encore quelques notations avant de voir quelques exemples de designs résolubles.

Un design $S(t, K; v)$ résoluble sera noté $RS(t, K; v)$. L'ensemble des $v \in \mathbb{N}$ tels qu'un $RS(t, K; v)$ existe sera noté $RB(K)$. Nous définissons similairement $RB(k)$.

Exemple 2.24 Soit u un entier positif. Considérons le graphe complet $K_{2u} = S(2, 2; 2u)$ avec les sommets $a, b_1, \ldots, b_{2u-1}$. Alors les classes de parallèles $\mathbf{B}_1, \ldots, \mathbf{B}_{2u-1}$ définies par

$$\mathbf{B}_i \;:=\; \{\{a, b_i\}\} \cup \{\{b_j, b_k\} : j + k \equiv 2i \pmod{2u-1}\}$$

forment une résolution de K_{2u}. En effet, chaque arête de K_{2u} est contenue dans une unique partie $\mathbf{B}_i$ et pour une partie fixe, deux arêtes distinctes sont parallèles.

[4] Il est aussi possible de définir une r-factorisation lorsque les parties sont des $S_r(1, K; v)$.

L'exemple suivant est certainement le problème le plus célèbre de la théorie des designs.

Exemple 2.25 (Le problème des écolières de Kirkman) Quinze écolières marchent en rang de trois quotidiennement pour sept jours. On doit les disposer afin que deux jeunes filles marchent dans un même rang une et une seule fois durant les sept jours.

Ce problème est équivalent à trouver une résolution d'un système de Steiner avec paramètre $v = 15$ et $k = 3$ (et donc $r = 7$ et $b = 35$).

Il est possible de trouver sept résolutions non isomorphes à ce problème. À la figure 2.1, nous montrons les rangs quotidiens qui nous donne les sept différentes parties de la résolution. Nous utilisons l'arithmétique des résidus pour trouver ces rangs. Nous notons par p^*, p_i, q_i les points du design, où i est un résidu $\pmod 7$.

$$\text{Jour } (i+1) : \begin{cases} \text{rangée } 1 : & p^* & p_i & q_i \\ \text{rangée } 2 : & p_{i+1} & p_{i+2} & p_{i+4} \\ \text{rangée } 3 : & p_{i+3} & q_{i+2} & q_{i+5} \\ \text{rangée } 4 : & p_{i+5} & q_{i+1} & q_{i+6} \\ \text{rangée } 5 : & p_{i+6} & q_{i+3} & q_{i+4} \end{cases}$$

FIG. 2.1 – Les rangs quotidiens (Jour 1 à 7) qui résolvent le problème des écolières.

Ces deux exemples démontrent que $2u \in RB(2)$ et $15 \in RB(3)$. Remarquons que 2 divise $2u$ et 3 divise 15. En examinant les conditions pour obtenir une résolution, nous obtenons

Proposition 2.26 La condition suivante est nécessaire pour l'existence d'un design résoluble $RS(2, k; v)$,

$$v \equiv k \pmod{k(k-1)}. \tag{2.27}$$

Démonstration. Par la définition 2.23, deux blocs distincts d'une classe de parallèles ne sont pas adjacents. Ainsi $v \equiv 0 \pmod k$. En combinant cette condition avec la condition 2.22 du corollaire 2.14 nous avons le résultat. ■

Au dernier chapitre, nous examinerons l'ensemble $RB(4)$. Afin de caractériser $RB(4)$ nous devons connaître encore quelques designs présentés dans la prochaine section.

2.5 Design divisible et design transversal

Un design *divisible* est un design avec paires équilibrées possédant une classe de parallèles particulière et finalement un design *transversal* est un design divisible possédant quelques propriétés de plus. Voyons la définition plus précise d'un design divisible.

Définition 2.27 Soient $K, M \subseteq \mathbb{N}$. Un *design divisible* $GD[K, M; v]$[5] est un triplet (X, G, A), où X est un ensemble de v points, $G := \{G_j\}_{j \in J}$ est une classe de parallèles (les éléments G_j sont appelés *groupes*) de X qui satisfait $\{|G_j| : G_j \in G\} \subset M$, $A := \{A_i\}_{i \in I}$ est un ensemble de blocs de X satisfaisant $\{|A_i| : A_i \in A\} \subset K$ et où chaque paire $\{p, q\} \subset X$ est contenu dans un et un seul groupe ou dans un et un seul bloc, mais pas les deux.

L'ensemble des entiers positifs v tels qu'un design divisible $GD[K, M; v]$ existe sera noté par $GD(K, M)$. Similairement, lorsque $K = \{k\}$ et $M = \{m\}$ on notera le design divisible par $GD[k, m; v]$ et on dira que le design est *uniforme* et l'ensemble de ces designs par $GD(k, m)$.

Définition 2.28 Un *design tranversal* $TD[s; t]$ est un design divisible uniforme $GD[s, t; st]$ où la grandeur des blocs s est égale au nombre de groupes. Conséquemment, chaque bloc est adjacent à chaque groupe en un et un seul point. Un design transversal $TD[s; t]$ possède exactement t^2 blocs. Un design transversal *résoluble* $RTD[s; t]$ est un design transversal $TD[s; t]$ où les blocs peuvent être partitionnés en t classes de parallèles (qui contiennent exactement t blocs). L'ensemble des entiers positifs t pour lesquels un $TD[s; t]$ (respectivement un $RTD[s; t]$) existe sera noté $TD(s)$ (respectivement $RTD(s)$).

Finalement, à l'aide de la panoplie de définitions touchant les designs nous aborderons un problème type de la théorie. Au prochain chapitre, nous établirons un critère nécessaire et suffisant pour qu'un système de Steiner $S(2, 4; v)$ soit résoluble.

[5]La notation GD provient de l'anglais « Group Divisible ».

Chapitre 3

Résolubilité de designs

3.1 Historique des systèmes de Steiner

La théorie des designs serait née il y a plus de 150 ans en Inde. Il est difficile de savoir à quand remonte la première définition d'un système de Steiner. En 1835, Julius Plücker [Plücker] a construit un exemple de $S(2,3;9)$ en se fiant sur les neuf points d'inflection d'une courbe cubique sans point singulier dans le plan complexe. Wesley Woolhouse [Woolhouse] a étudié certains problèmes concernant l'existence de systèmes de Steiner en 1844. Quelques années plus tard, Thomas Kirkman [Kirkman] a émis le problème portant sur l'existence des systèmes de Steiner $S(2,3;v)$. Tout ça bien avant le travail de Steiner [Steiner] en 1853.

À ce jour, bien des problèmes restent à résoudre, en particulier au sujet de l'existence des t-designs, $S_\lambda(t,k;v)$. Un théorème semblable au théorème 2.13 concernant les t-designs nous donne des conditions nécessaires, par contre ces conditions ne sont pas suffisantes en général. Bien sûr, un t-design avec paramètres $k = t$ ou $k = v$ existe toujours, ces exemples sont appelé *designs triviaux*. Malgré beaucoup de recherche, aucun système de Steiner non trivial $S(t,k;v)$ avec $t \geq 6$ n'a encore été trouvé.

Lors de l'exemple 2.25, nous avons donné une des sept résolutions possibles d'un système de Steiner $S(2,3,15)$. Afin de généraliser, le problème de Kirkman peut se poser pour un nombre quelconque de jeunes filles. Avec la condition nécessaire (2.27), nous obtenons que $v \equiv 3 \pmod 6$. La question qui se pose maintenant est de savoir si cette

condition est suffisante. La question a été répondu positivement en 1971 dans un article de Ray-Chaudhuri et Richard Wilson [Ray-Chaudhuri]. Maintenant, nous reprenons le problème de Kirkman en changeant les rangs de trois par des rangs de quatre. Les mêmes questions sont posées à savoir s'il existe un système de Steiner $S(2,4,v)$ résoluble pour un v donnée et si les conditions nécessaires sur v sont suffisantes. Ces questions ont été répondu en 1972 dans un article écrit par Hanani, Ray-Chaudhuri et Wilson (voir [Hanani]). Nous verrons ici comment ils sont arrivés aux résultats.

3.2 Résultats préalables

Nous commençons par des faits sur les ensembles $B(K), GD(K,M), TD(s)$ que nous avons définis au chapitre précédent. Rappelons leurs définitions :

$$\begin{aligned} B(K) &:= \{v \in \mathbb{N} : S(2,K;v) \text{ existe}\}; \\ GD(K,M) &:= \{v \in \mathbb{N} : GD[K,M;v] \text{ existe}\}; \\ TD(s) &:= \{t \in \mathbb{N} : TD[s;t] \text{ existe}\}. \end{aligned}$$

Soient $k, m \in \mathbb{N}$, en observant la définition d'un design divisible nous obtenons

$$GD(k,m) \subset B(\{k,m\}). \tag{3.1}$$

De plus, en ajoutant un point à chaque groupe d'un design divisible, nous obtenons

$$GD(k,m)+1 \subset B(\{k,m+1\}), \tag{3.2}$$

où $H+1 := \{h_i+1 : h_i \in H\}$, si H est un ensemble d'entiers. Dans le cas $m = k-1$ nous avons un résultat plus puissant

$$GD(k,k-1)+1 = B(k). \tag{3.3}$$

Ensuite, à propos des designs transversaux nous avons

$$s \leq s' \Rightarrow TD(s) \supset TD(s'), \tag{3.4}$$

$$RTD(s) = TD(s+1). \tag{3.5}$$

Ensuite, à la lumière de la proposition 2.6 et du corollaire 2.11, si $q = p^f$ est une puissance d'un nombre premier nous avons

$$q^2 + q + 1 \in B(q+1), \tag{3.6}$$
$$q^2 \in B(q). \tag{3.7}$$

À partir de (3.6), il suit que

$$q^2 + q \in GD(q+1, q), \tag{3.8}$$

en utilisant (3.3). De plus, la propriété (3.8) est équivalente à

$$q \in TD(q+1) = RTD(q), \tag{3.9}$$

en utilisant (3.5). Poursuivons avec le lemme suivant, donné sans démonstration.

Lemme 3.1 Soit $R^*(k) := \{r \in \mathbb{N} : (k-1)r + 1 \in RB(k)\}$, c'est-à-dire que $R^*(k)$ est l'ensemble des degrés r pour lesquels un design résoluble avec des blocs de grandeur k existe. Alors

$$R^*(k) = B(R^*(k)). \tag{3.10}$$

■

Nous terminons cette section avec deux théorèmes présents dans l'article [Hanani]. Nous omettons volontairement les démonstations, puisqu'elles possèdent de trop longs développements.

Théorème 3.2 Soient $U(k) := \{u \in \mathbb{N} : k(k-1)u + k \in RB(k)\}$ et $h, t \in \mathbb{N}$ tels que $0 \leq h \leq t$. Fixons $k = 3$ ou 4. Si $\{t, h\} \subset U(k)$ et $t \in TD(k+2)$, alors $(k+1)t+h \in U(k)$.

■

Théorème 3.3 Soit $m, n \in \mathbb{N}$. Si $4m \in RB(4)$ et $4n \in RB(4)$, alors $4mn \in RB(4)$.

■

3.3 Constructions

Pour arriver à démontrer que la condition (2.27) est suffisante, nous devons construire quelques résolutions. D'abord, l'ensemble des points V sera un produit cartésien d'ensembles de résidus modulo des entiers ($\mathbf{Z}_n$) avec certains corps finis. Les points seront donnés entre parenthèses ( ) et les lettres x, y représenteront des générateurs des corps finis. Les blocs seront donnés entre accolades { } et lorsqu'ils seront repris de façon cyclique, nous ajouterons $\pmod q$ après le bloc. Finalement, les classes de parallèles seront données entre crochets [ ].

Lemme 3.4 Si $q = 4t+1$ est une puissance d'un nombre premier, alors $3q+1 \in RB(4)$.

Démonstration. Soit $V = \mathbf{Z}_3 \times GF(q) \cup (\infty)$ Les blocs sont

$$\left[\begin{array}{l} \{(0,0),(1,0),(2,0),(\infty)\}, \\ \{(0,x^{\alpha}),(0,x^{\alpha+2t}),(1,x^{\alpha+t}),(1,x^{\alpha+3t})\} \pmod{3,-}, \alpha = 0,1,\ldots,t-1. \end{array} \right] \pmod{(-,q)}.$$

■

Lemme 3.5 $100 \in RB(4)$.

Démonstration. Soient $V = \mathbf{Z}_4 \times GF(25)$ et $x^2 = 2x + 2$. Les blocs sont

$$\left[\begin{array}{l} \{(0,0),(1,0),(2,0),(3,0)\}, \\ \{(\alpha,x^{6\alpha+6\beta}),(\alpha,x^{6\alpha+6\beta+2}),(\alpha,x^{6\alpha+6\beta+5}),(\alpha,x^{6\alpha+6\beta+19})\}, \\ \alpha = 0,1,2,3, \beta = 0,1, \\ \{(0,x^{\nu}),(1,x^{\nu+6}),(2,x^{\nu+12}),(3,x^{\nu+18})\}, \nu = 3,4,7,9,10,12-18,20-23. \end{array} \right] \pmod{(-,25)},$$

$$[\{(0,x^{\mu}),(1,x^{\mu+6}),(2,x^{\mu+12}),(3,x^{\mu+18}),\} \pmod{(-,25)}], \mu = 0,1,2,5,6,8,11,19.$$

■

Les trois prochains lemmes utilisent des constructions similaires pour arriver au résultat.

Lemme 3.6 $172 \in RB(4)$. ■

Lemme 3.7 $232 \in RB(4)$. ■

Lemme 3.8 $388 \in RB(4)$. ■

Nous avons maintenant vu tous les résultats préliminaires pour arriver au résultat souhaité. La prochaine section termine notre étude sur la résolubilité du système de Steiner $S(2,4;v)$.

3.4 Résolubilité de $S(2,4;v)$

Voici donc le théorème qui répond aux questions établies au début de ce chapitre.

Théorème 3.9 Soit $v \in \mathbb{N}$. Alors

$$RS(2,4,v) \text{ existe} \quad \Leftrightarrow \quad v \equiv 4 \pmod{12}. \tag{3.11}$$

C'est-à-dire que la condition (2.27) est suffisante si $k = 4$.

Démonstration. Nous avons ($\Rightarrow$) par (2.27). Pour démontrer ($\Leftarrow$), nous montrons que pour tout entier positif u, $u \in U(4)$ (voir la définition du théorème 3.2). Nous avons trivialement que $u \in U(4)$ pour $u = 0$. Pour $u =$1, 2, 3, 4, 6, 7, 9, 10, 12, 13, 15, 18, 20, 22, 24, 31, 34, 79 nous avons que $12u + 4 \in RB(4)$ par le lemme 3.4 et donc, $u \in U(4)$. Pour $u = 8$, $12u+4 = 100 \in B(4)$ par le lemme 3.5. Pour $u = 11$, nous avons $r = 4u + 1 = 45$. Par (3.9) et (3.4), $9 \in TD(5)$ et par (3.1), nous avons $45 \in B(\{5,9\})$. De plus, $\{5,9\} \subset R^*(4)$ puisque $\{1,2\} \subset U(4)$ et donc par (3.10), $45 \in R^*(4)$ (ce qui veut dire que $11 \in U(4)$). Pour $u = 14$, $12u + 4 = 172 \in RB(4)$ par le lemme 3.6, pour $u = 19$, $12u+4 = 232 \in RB(4)$ par le lemme 3.7 et pour $u = 32$, $12u+4 = 388 \in RB(4)$ par le lemme 3.8. Pour $u = 5, 16, 17, 21, 23, 33$ nous avons respectivement $v = 64(= 4\cdot 4\cdot 4), 196(= 4\cdot 7\cdot 7), 208(= 4\cdot 4\cdot 13), 256(= 4\cdot 4\cdot 16), 280(= 4\cdot 7\cdot 10), 400(= 4\cdot 10\cdot 10)$ et $u \in U(4)$ est obtenu par le théorème 3.3. Pour les autres valeurs de u, nous montrons que $u \in U(4)$ par induction en utilisant le théorème 3.2. ■

La démonstration du théorème peut paraître abstraite et les constructions provenir de nulle part. Par contre, la démarche inductive est très bien construite. Il aura fallu plus de 120 ans pour réussir à résoudre le problème des écolières entièrement et son analogue pour des rangs de quatre. Pour terminer, nous présentons la construction d'une résolution à partir du lemme 3.4 avec $t = 1$ et donc avec $v = 16$ écolières. Nommons les écolières Alice, Béatrice, Catherine, Dominique, Élise et ainsi de suite jusqu'à Pascale.

Nous constatons que Dominique est la préférée du professeur puisqu'elle reste à l'avant à chaque jour ; les autres changent selon trois cycles de cinq écolières.

$$\overbrace{\begin{bmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{bmatrix}}^{Lundi}, \overbrace{\begin{bmatrix} E & I & M & D \\ O & A & H & J \\ G & B & L & N \\ K & C & P & F \end{bmatrix}}^{Mardi}, \overbrace{\begin{bmatrix} O & G & K & D \\ P & E & J & B \\ H & I & N & C \\ L & M & F & A \end{bmatrix}}^{Mercredi},$$

$$\overbrace{\begin{bmatrix} P & H & L & D \\ F & O & B & I \\ J & G & C & M \\ N & K & A & E \end{bmatrix}}^{Jeudi}, \overbrace{\begin{bmatrix} F & J & N & D \\ A & P & I & G \\ B & H & M & K \\ C & L & E & O \end{bmatrix}}^{Vendredi}.$$

Les cycles sont représentés dans l'arrangement ci-dessous. Les cycles sont $(\alpha\ \beta\ \gamma\ \delta\ \epsilon)$, $(1\ 2\ 3\ 4\ 5)$ et $(a\ b\ c\ d\ e)$.

$$\begin{bmatrix} \alpha & 1 & a & D \\ \epsilon & \beta & 4 & 3 \\ 5 & 2 & d & c \\ e & b & \delta & \gamma \end{bmatrix}$$

Avec un tel arrangement, le professeur peut produire $((4! \cdot 4!) \cdot 5) \cdot 5! = 345600$ semaines différentes en permutant les rangées et les colonnes de chaque jour et ensuite en permutant les jours.

Conclusion

Au tout début, j'ai dû résoudre le problème de Kirkman. Pour ce faire, j'ai utilisé une méthode très spécifique au problème et je ne pouvais pas l'appliquer à un nombre plus élevé d'étudiantes. De plus, la chance y était pour quelque chose : après avoir créé mon système de Steiner, je ne savais pas s'il était résoluble. Par contre, je voulais savoir comment il était possible de construire un tel système résoluble et ensuite démontrer qu'il existe pour des entiers déterminés. Ainsi, j'ai revu la théorie des hypergraphes et étudié beaucoup la théorie des designs. En fait, les structures d'incidences sont très polyvalentes et peuvent être utilisées afin de modéliser plusieurs problèmes différents. Il s'agit de bien faire la transition entre le problème posé et la théorie des designs. Nous pouvons ensuite appliquer des théorèmes purement théoriques qui servent à résoudre notre problème. Dans notre cas, nous étions intéressé au problème de Kirkman avec des rangs de 4. Nous voulions savoir si le critère nécessaire sur le nombre d'écolières était suffisant. À l'aide d'un théorème de Hanani, Ray-Chaudhuri et Wilson nous avons vu qu'il était suffisant.

Le théorème abordé date de 1972, depuis ce temps, beaucoup de questions sur les résolutions de designs ont été répondues. Par contre, des questions sont toujours sans réponses... Par exemple, on ne sait pas si un des 831 designs non isomorphes $S_4(2, 5, 15)$ est résoluble, il existe encore 23 valeurs de v pour lesquelles l'existence d'une résolution de $S(3, 4; v)$ est indéterminée.

Beaucoup d'énergie est investie dans les questions qui portent sur l'existence des designs. Ainsi, il serait intéressant de chercher un algorithme qui permettrait de déterminer si un design est résoluble ou non à l'aide de sa matrice d'incidence. Dans l'éventualité où un tel algorithme n'existe pas, je crois qu'il serait bien d'y consacrer du temps afin d'en construire un qui serait efficace.

Appendice

Notions élémentaires d'algèbre - Corps finis

Les corps finis nous permettent d'alléger la nomenclature et d'aborder avec plus de simplicité certains aspects techniques des designs. Cette section parcourt les corps finis et est tirée du livre *Cours d'arithmétique* de Jean-Pierre Serre [Serre].

Définition A.1 Soit K un corps, on définit sa *caractéristique*, notée $car(K)$ comme le plus petit entier positif p tel que $p \cdot 1 = 0$. Si un tel p n'existe pas, alors on dit de K qu'il est de *caractéristique 0*.

Remarque A.2 Par définition, $p \cdot 1 = \underbrace{(1 + 1 + \cdots + 1)}_{p \text{ fois}}$. Donc, on trouve facilement que $(p \cdot 1) \cdot (q \cdot 1) = pq \cdot 1$ dans K. Puisqu'un corps ne peut contenir de diviseur de zéro, la caractéristique $car(K)$ doit être nulle ou un nombre premier.

Continuons avec un lemme important pour la suite.

Lemme A.3 La transformation $Fr : K \to K, x \mapsto x^p$, où $car(K) = p$, est appelée la fonction de Frobenius. Cette fonction est un homomorphisme. De plus, si le corps K est fini, Fr est un automorphisme.

Démonstration. En effet, puisque p est premier, si on développe $(x - y)^p$ tous les coefficients binomiaux sont divisibles par p sauf le premier et le dernier, donnant $x^p - y^p$. Ensuite, tout homomorphisme d'un corps est injectif, car il n'y a pas de diviseur de zéro. Ainsi Fr est un isomorphisme $K \to K^p$. Mais puisque K est un corps fini, on obtient aisément que $K^p = K$, car Fr est une bijection et donc $|K^p| = |K|$. ■

Exemple A.4 Soit p un nombre premier, l'anneau $\mathbb{Z}/(p)$ est un corps. En effet, tous les résidus non nuls modulo p sont inversibles. Nous utilisons la notation $\mathbf{Z}_p$, pour désigner ce corps.

Le prochain théorème complète notre étude des corps finis. Il nous fournit les connaissances nécessaires pour comprendre les exemples de constructions de designs présentés à la section 3.3. Nous prendrons comme définition d'un corps algébriquement clos Ω, un corps où tout polynôme d'une variable s'écrit comme un produit de facteur de degré un.

Théorème A.5 Soit p un nombre premier, f un entier positif, $q = p^f$ et Ω un corps algébriquement clos de caractéristique p. Alors

1. L'équation $x^q - x = 0$ possède q solutions différentes dans Ω ;
2. L'ensemble de ces solutions est un sous-corps de Ω (on le note $GF(q)$) ;
3. Tout corps K tel que $|K| = q$ est isomorphe à $GF(q)$;
4. Le corps $GF(p)$ est isomorphe à $\mathbf{Z}_p$;
5. $GF(p) \subset GF(q)$.

Démonstration.
1. L'équation $x^q - x$ doit se diviser en facteurs de degré un dans Ω. Sa dérivée est -1 dans Ω, ainsi il n'y a pas de racine double. Ainsi, l'équation possède q solutions distinctes.
2. Par définition cet ensemble est égal à $\{x \in \Omega : Fr^f(x) = x\}$. Puisque Fr^f est un homomorphisme, cet ensemble est un sous-corps.
3. Si $|K| = q$ alors $q \cdot 1 = 0$, puisque l'ordre du groupe additif annule tous les éléments. Ainsi, $car(K) = p$. Ensuite, puisque Ω est algébriquement clos, tout corps à p^f éléments peut être plongé dans Ω par inclusion, nous posons ainsi $L = \{\text{Image de } K \text{ dans } \Omega\}$. Donc, $|L| = |K| = q$ implique que $|L^*| = q - 1$. Alors pour tout $x \in L^*$, $x^{q-1} = 1$ et alors $x^q = x$. De plus, la dernière équation est vraie pour zéro. Puisque L est isomorphe à la fois à K (par l'inclusion) et à $GF(q)$ par les propriétés que nous venons de voir, le résultat suit.
4. Il est facile de voir que le corps $GF(p)$ est le sous-corps de $GF(q)$ qui contient les multiples entiers de 1 dans $GF(q)$. (Ainsi **5.** est aussi démontré) Ensuite, par le petit théorème de Fermat on constate que $GF(p)$ est bel et bien isomorphe à $\mathbf{Z}_p$.
■

Bibliographie

[Berge] BERGE, C. *Graphes et hypergraphes*, Paris, Dunod, 1970, 502 p.

[Beth] BETH, T. JUNGNICKEL, D. et LENZ, H. *Design Theory*, Volume 1 & 2, Cambridge, Cambridge University Press, 1999, 1100 p.

[Gyarfas] GYÁRFÁS, A. *Advanced combinatorics handouts*, Budapest, Budapest Semesters in Mathematics, 2005, 57 p.

[Hanani] HANANI, H., RAY-CHAUDHURI D. K. et WILSON R. M. *On resolvable designs*, Discrete Mathematics, 3, 1972, p. 343-357.

[Hoffman] HOFFMAN, P. *The man who loved only numbers*, Fourth Estate, London, 1998, 302 p.

[Kirkman] KIRKMAN T.P. *On a problem in combinatorics*, Cambridge and Dublin Math. Journal, 2, p. 191-204.

[Plücker] PLÜCKER, J. *System der analytischen Geometrie, auf neue Betrachtungsweisen gegründet, und insbesondere eine ausführliche Theorie der Curven dritter Ordnung enthaltend*, Duncker und Humblot, Berlin, 1835.

[Ray-Chaudhuri] RAY-CHAUDHURI D. K. et WILSON R. M. *Solution of Kirkman's schoolgirl problem*, Symp. Pure Math., 19, 1971, p. 187-203.

[Serre] SERRE, J.-P. *Cours d'arithmétique*, Presse Universitaire de France, 1977, 188 p.

[Steiner] STEINER, J. *Combinatorische Aufgabe*, J. renine angew. Math., 45, p. 181-182.

[Woolhouse] WOOLHOUSE, W.S.B. *Prize question 1733*, Lady's and gentleman's Diary, 1844.