

Configurations – Designs

Note de cours des 17èmes JCALM

6 mai 2017

1 Définition et premiers exemples

Pour tout entier q , on note \mathbb{Z}_q l'ensemble des entiers modulo q et on note $[q]$ l'ensemble $\{1, \dots, q\}$. On note K_n le graphe complet à n sommets, et $K_{m \times q}$ le graphe m -parti complet dont toutes les parties sont de taille q .

Definition 1. Une t - (n, k, λ) **configuration** est un ensemble de sous-ensembles, appelés **blocs**, de taille k , d'un ensemble V de n sommets tel que tout sous-ensemble de t sommets est dans exactement λ blocs.

Une t - (n, k, λ) configuration est **résoluble** si on peut grouper les blocs en **classes parallèles**, i.e. ensembles de blocs formant une partition de l'ensemble de sommets.

Dans le cas, $t = 2$, $\lambda = 1$, qui est celui que nous étudierons plus particulièrement dans ces notes, une 2 - $(n, k, 1)$ configuration (abrégée dans la suite en $(n, k, 1)$ **configuration**) n'est rien d'autre qu'une **décomposition de K_n** (i.e. partition de son ensemble d'arêtes) **en copies de K_k** . En effet, les blocs induisent des sous-graphes complets de taille k ; chaque paire d'éléments est dans exactement un bloc veut dire qu'une arête de K_n est dans une seule copie de K_k .

Dans le cas où $t = 2$, $k = 2$ et $\lambda = 1$, une configuration résoluble est une partition du graphe complet en couplages parfaits.

Exemple 2. $n = 7$, $k = 3$, $\lambda = 1$, $t = 2$. Il existe une $(7, 3, 1)$ configuration. Autrement dit, on peut décomposer K_7 en copies de K_3 . Les blocs sont $B_i = \{i, i + 1, i + 3\}$ pour $i \in \mathbb{Z}_7$. (Les indices sont modulo 7.) Voir Figure 1.

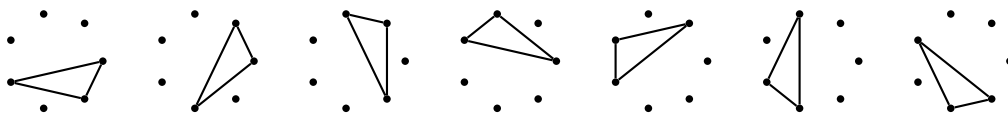


FIGURE 1 – Les 7 blocs d'une $(7, 3, 1)$ configuration ou comment décomposer K_7 en 7 copies de K_3 .

Exemple 3. $n = 13$, $k = 3$, $\lambda = 1$, $t = 2$. Il existe une $(13, 3, 1)$ configuration. Autrement dit, on peut décomposer K_{13} en copies de K_3 . Les blocs sont $B_i = \{i, i + 1, i + 4\}$ et $B'_i = \{i, i + 2, i + 7\}$ pour $i \in \mathbb{Z}_{13}$. (Les indices sont modulo 13.) Voir Figure 2.

Exemple 4. $n = 13$, $k = 4$, $\lambda = 1$, $t = 2$. Il existe une $(13, 4, 1)$ configuration. Autrement dit, on peut décomposer K_{13} en copies de K_4 . Les blocs sont $B_i = \{i, i + 1, i + 3, i - 4\}$, pour $i \in \mathbb{Z}_{13}$. (Les indices sont modulo 13.) Voir Figure 3.

Exemple 5. $n = 4$, $k = 2$, $\lambda = 1$, $t = 2$. Il existe une $(4, 2, 1)$ configuration résoluble. Autrement dit, on peut décomposer K_4 en six blocs (arêtes) qui peuvent être groupés par 2 pour faire une partition de l'ensemble de sommets (= couplage parfait). Voir Figure 4.

Exemple 6. $n = 9$, $k = 3$, $\lambda = 1$, $t = 2$. On peut trouver douze blocs (triplets) décomposant K_9 qui peuvent être groupés par 3 pour faire une partition de l'ensemble de sommets. Voir Figure 5.

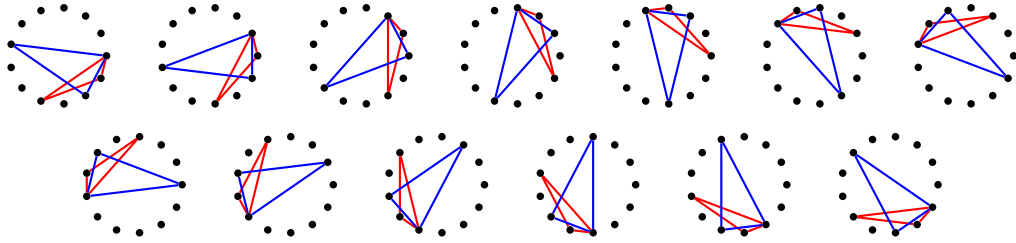


FIGURE 2 – Les 26 blocs d'une $(13, 3, 1)$ configuration ou comment décomposer K_{13} en 26 copies de K_3 .

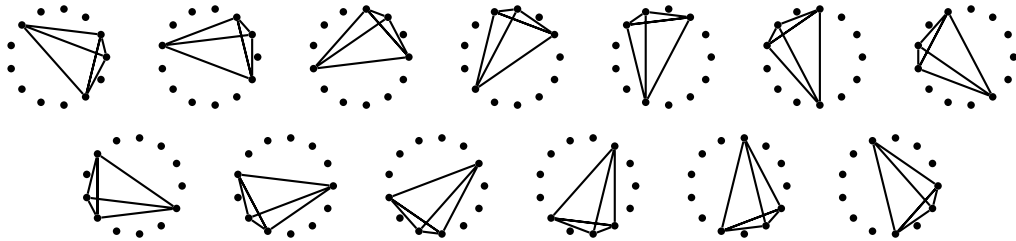


FIGURE 3 – Les 13 blocs d'une $(13, 4, 1)$ configuration ou comment décomposer K_{13} en 13 copies de K_4 .

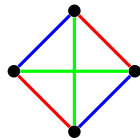


FIGURE 4 – $(4, 2, 1)$ configuration résoluble = décomposition de K_6 en trois couplages parfaits.

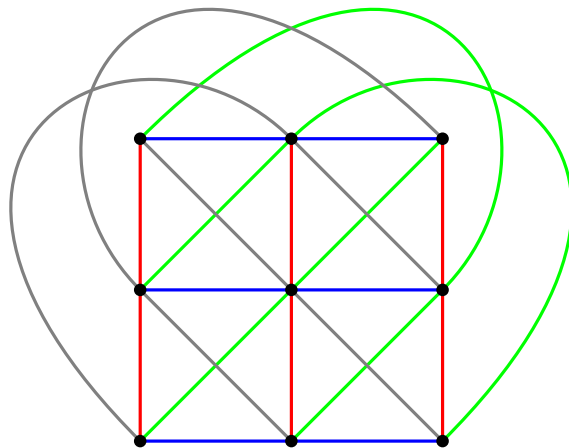


FIGURE 5 – Une $(9, 3, 1)$ configuration résoluble. Chaque couleur correspond à une classe de 3 triplets.

Exemple 7. $n = 15, k = 3, \lambda = 1, t = 2$. Les 105 arêtes de K_{15} se partitionnent en 35 blocs (triplets) se regroupant en 7 classes de 5 blocs, chacune d'entre elle étant une partition de l'ensemble de sommets. C'est une solution au fameux *Problème des Ecolières*. Ce problème, qui a été posé par le révérend Thomas P. Kirkman en 1850 [16], est le suivant :

“*Quinze jeunes filles se rendent à l'école en rang par 3 sept jours de suite. Est-il possible d'arranger les rangs de chacun des jours de manière à ce que deux écolières ne soient pas deux fois dans une même rangée de 3 ?*”
 La première solution de ce problème a été publiée par Cayley [6]. Peu après, Kirkman a publié une solution qui repose sur un cas particulier d'un résultat plus général publié en 1847 [15] sur les triplets de Steiner. Mulder [18] et Cole [8] ont montré qu'il n'existait que sept solutions non-isomorphes à ce problème. Autrement dit, il existe exactement sept $(15, 3, 1)$ configurations résolubles non-isomorphes. L'une d'entre elles est donnée Figure 6.

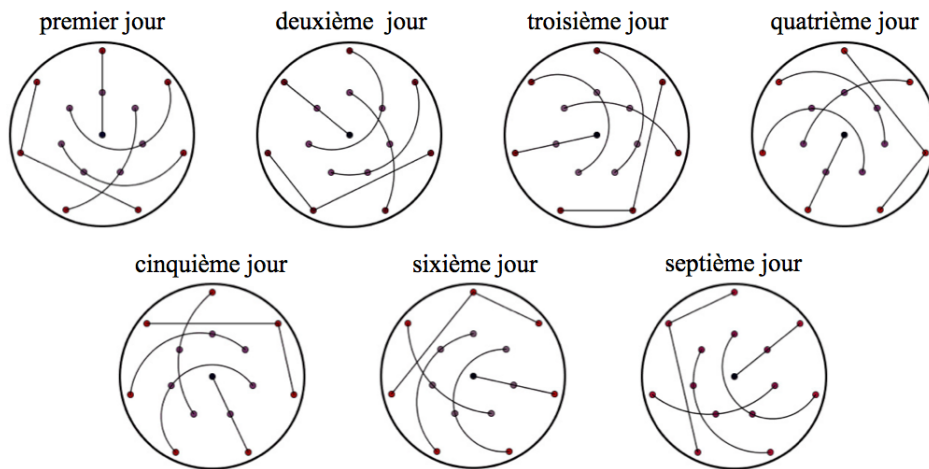


FIGURE 6 – Une solution au problème de Kirkman : $(15, 3, 1)$ configuration résoluble.

Une $(n, 3, 1)$ configuration est un **système de triplets de Steiner**. Le nom vient de ce que Steiner [23] a posé la question de leur existence en 1853, sans savoir que Kirkman [15] avait déjà prouvé leur existence en 1847. Leur existence fut établie (à nouveau) par Reiss [21] en 1859 et ce fut plus tard Witt [30] qui donna le nom de systèmes de triplets de Steiner aux $(n, 3, 1)$ configurations.

Le problème général consiste à trouver une t - (n, k, λ) configuration (résoluble ou non) ou à prouver sa non-existence. Dans ces notes, nous ne considérerons pas les configurations résolubles. De même, nous n'aborderons que très peu les nombreuses généralisations des configurations. Le lecteur curieux est invité à consulter le Handbook of Combinatorial Design [7] ou le livre de Stinson [24] ou le polycopié de Bermond-Sotteau [3].

Certaines autres configurations ou décompositions nous seront cependant utiles. Au lieu de décomposer un graphe complet en sous-graphes complets d'un seul type, on peut le décomposer en sous-graphes complets de plusieurs types (voir par exemple, le Théorème 31).

On peut également s'intéresser aux décompositions de n'importe quel graphe en sous-graphes complets. Par exemple, considérons les graphes multipartis complets. Le Lemme 23 établit que l'existence d'une décomposition de K_{qm+1} en K_{q+1} est équivalente à l'existence d'une décomposition de K_{m*q} en K_{q+1} .

Enfin, on peut décomposer un graphe, en particulier, un graphe complet en sous-graphes isomorphes à un même graphe H , pas forcément complet. Une n - H -**configuration** est une décomposition de K_n en copies de H .

2 Conditions nécessaires d'existence

La définition de t - (n, k, λ) configuration implique aisément certaines conditions nécessaires à son existence.

Proposition 8. Dans une t - (n, k, λ) configuration, le nombre de blocs est

$$b = \lambda \frac{\binom{n}{t}}{\binom{k}{t}}.$$

Preuve. Il y a $\binom{n}{t}$ sous-ensembles de taille t chacun devant être couvert λ fois, soit $\lambda \binom{n}{t}$ occurrences de sous-ensembles de taille t . Chaque bloc est de taille k et donc contient $\binom{k}{t}$ de ces occurrences. \square

En particulier, pour $k = 2, \lambda = 1$, le nombre de sous-graphes complets de taille k de la décomposition est $\frac{n(n-1)}{k(k-1)}$. On doit donc avoir

$$n(n-1) \equiv 0 \pmod{k(k-1)}. \quad (\text{CN1})$$

Dit autrement, le nombre d'arêtes de K_n doit être un multiple du nombre d'arêtes de K_k .

Proposition 9. Dans une t - (n, k, λ) configuration, tout sous-ensemble de i sommets, $i < t$, appartient à exactement $b_i = \lambda \frac{\binom{n-i}{t-i}}{\binom{k-i}{t-i}}$ blocs.

Preuve. Fixons un ensemble I de taille i . Le nombre de sous-ensembles à t éléments contenant I est $\binom{n-i}{t-i}$. Chacun de ces ensembles appartient exactement à λ blocs qui contiennent I . Or, le nombre de blocs contenant I est $\binom{k-i}{t-i}$ d'où l'égalité. \square

Pour $t = 2, \lambda = 1$ la proposition implique que tout sommet appartient à exactement $r = \frac{n-1}{k-1}$ sous-graphes de taille k . Dit autrement le degré $n-1$ d'un sommet de K_n doit être un multiple du degré $k-1$ dans chaque K_k auquel il appartient. Donc

$$n-1 \equiv 0 \pmod{k-1}. \quad (\text{CN2})$$

Pour des t -configurations, il faut de plus que tous les b_i soient des entiers et on a donc t conditions nécessaires.

Pour les triplets de Steiner, ($r = 2, k = 3, \lambda = 1$) les conditions nécessaires d'existence (CN1) et (CN2) donnent

Proposition 10. S'il existe un triplet de Steiner ($(n, 3, 1)$ configuration) alors

$$n \equiv 1 \text{ ou } 3 \pmod{6}.$$

Dans le cas d'une configuration résoluble, on a une autre condition nécessaire à savoir que le nombre d'éléments n doit être un multiple de k vu que les blocs d'une classe parallèle forment une partition de l'ensemble des éléments.

Proposition 11. Pour qu'il existe une t - (n, k, λ) configuration résoluble, il faut

$$n \equiv 0 \pmod{k}. \quad (\text{CN3})$$

Pour les H -configurations, on obtient de la même manière la proposition suivante.

Proposition 12. Soit H un graphe ayant p arêtes. Pour qu'il existe une n - H -configuration, il faut

- $\binom{n}{2} \equiv \text{mod } p$;
- $n-1$ doit être une combinaison linéaire des degrés des sommets de H .

Une première question est de savoir si ces conditions nécessaires sont suffisantes.

3 Quelques résultats

Dans ce cours, on prouvera en Section 6 que pour $t = 2, \lambda = 1, k = 3$, les conditions nécessaires (CN1) et (CN2) sont suffisantes pour l'existence d'une $(n, 3, 1)$ configuration.

Théorème 13 (Kirkman [15], 1847). *Pour tout $n \equiv 1$ ou $3 \pmod{6}$, le graphe complet K_n se décompose en copies de K_3 (= il existe un système de triplets de Steiner c.a.d. une $(n,3,1)$ configuration).*

Pour $t = 2$, $\lambda = 1$, $k = 4$ et $k = 5$, les conditions nécessaires sont là aussi suffisantes.

Théorème 14 (Hanani [13]). *Soit $k \in \{4, 5\}$. Si $n(n-1) \equiv 0 \pmod{k(k-1)}$ et $n-1 \equiv 0 \pmod{k-1}$, alors le graphe complet K_n se décompose en copies de K_k (= il existe une $(n, k, 1)$ configuration).*

Pour $t = 2$, $\lambda = 1$, et $k \geq 6$, les conditions ne sont pas suffisantes. S'il existait une $(43, 7, 1)$ configuration (plan projectif d'ordre 6 voir Section 5), il existerait une $(36, 6, 1)$ configuration avec une classe parallèle (plan affine d'ordre 6 voir Proposition 45) ou ce qui est équivalent une décomposition de K_{6*6} en K_6 et ceci impliquerait une décomposition de K_{4*6} en K_4 , ce qui est équivalent (voir Sous-section 5.2) au fameux *Problème des 36 officiers* qu'Euler a imaginé en 1782 pour distraire la cour du roi Frédéric de Prusse :

“Dans un pays, il y a 6 régiments et 6 grades possibles ; comment les faire défiler en carré (six lignes six colonnes) de manière à ce que dans chaque ligne et chaque colonne il n'y ait pas deux officiers du même régiment ni deux officiers de même grade ?”

L'impossibilité de ce problème a été prouvée par Tarry [26] en 1901. Fisher et Yates ont donné une preuve plus simple [10] en 1934 et une preuve courte a été donnée en 1984 par Stinson [25].

Pour $k = 6$, il a été montré qu'il n'existe pas de $(n, 6, 1)$ configuration pour $n \in \{16, 21, 36, 46\}$. En revanche, si les conditions nécessaires (CN1) et (CN2) sont satisfaites, une $(n, 6, 1)$ configuration existe toujours pour $n \geq 802$. Pour 21 valeurs de n , on ne sait pas si une $(n, 6, 1)$ configuration existe.

Euler avait conjecturé que pour tous les $q \equiv 2 \pmod{4}$, il n'existait pas de décomposition de K_{4*q} en K_4 . Cette conjecture a eu quelques preuves fausses avant d'être définitivement réfutée (voir Sous-section 5.2). En revanche, la question de la non-existence de décompositions de K_{q^2+q+1} en K_{q+1} pour ces valeurs de q reste ouverte. Un résultat de non-existence est donné par le théorème suivant

Théorème 15 (Bruck-Ryser [5]). *Si q n'est pas une puissance de premier, $q \equiv 1$ ou $2 \pmod{4}$ et q n'est pas la somme de deux carrés, alors il n'existe pas de $(q^2 + q + 1, q, 1)$ configurations.*

En revanche le problème est complètement résolu pour q puissance de premier (voir Section 5) :

Théorème 16. *Si q est une puissance d'un nombre premier, alors K_{q^2+q+1} se décompose en copies de K_{q+1} .*

Un des seuls autres cas où tout est résolu est l'existence de 3 -($n, 4, 1$) configuration. Là encore, les conditions nécessaires sont également suffisantes.

Théorème 17 (Hanani [12]). *Il existe une 3 -($n, 4, 1$) configuration si et seulement si $n \equiv 2$ ou $4 \pmod{6}$.*

Dans le cas des configurations résolubles, on a le résultat exact suivant :

Théorème 18 (Ray-Chaudhuri et Wilson [20]). *Pour tout $n \equiv 3 \pmod{6}$, le graphe complet K_n se décompose en copies de K_3 qu'on peut regrouper en partitions de l'ensemble sommets. Autrement dit, il existe un système de triplets de Kirkman c.a.d. une $(n,3,1)$ configuration résoluble.*

Une des avancées remarquables pour l'existence de configurations est donnée dans le théorème suivant.

Théorème 19 (Wilson [27, 28, 29]). *Pour tout triplet (k, λ, t) , il existe un n_0 tel que pour tout $n \geq n_0$ satisfaisant les conditions nécessaires, il existe une t -(n, k, λ) configuration.*

Parler des Théorèmes de Keevash et Kuhn Osthus

Donner une démonstration de tous ces résultats est bien au-delà de l'objet de ces notes de cours. Notre but ici est simplement de donner un aperçu de certaines idées qui sont utilisées. Pour cela, nous allons donner une preuve du Théorème 13, dont l'approche générale est similaire à l'approche de la preuve du Théorème de Wilson (Théorème 19). Cette méthode utilise des décompositions intermédiaires, des techniques pour passer d'une configuration/décomposition à une autre et l'existence de configurations simples.

4 D'une configuration à une autre

La proposition suivante découle immédiatement de la définition.

Proposition 20. *Si \mathcal{C}_1 et \mathcal{C}_2 sont une t - (n, k, λ_1) configuration et une t - (n, k, λ_2) configuration sur le même ensemble de points, alors $\mathcal{C}_1 \cup \mathcal{C}_2$ est une t - $(n, k, \lambda_1 + \lambda_2)$ configurations.*

Elle implique en particulier que s'il existe $(n, k, 1)$ t -configuration, alors il existe une t - (n, k, λ) configuration (qui est en fait λ fois la t - $(n, k, 1)$ configuration). C'est pourquoi, on se concentrera essentiellement ici au cas $\lambda = 1$.

Proposition 21. *S'il existe une t - (n, k, λ) configuration, alors il existe une $(t-1)$ - $(n-1, k-1, \lambda)$ configuration.*

Preuve. Soit \mathcal{C} une t - (n, k, λ) configuration sur un ensemble de n sommets V . Prenons un sommet v de V . Soit \mathcal{B} l'ensemble des blocs qui contiennent v et $\mathcal{C}' = \{B \setminus \{v\} \mid B \in \mathcal{B}\}$.

\mathcal{C}' est clairement une $(t-1)$ - $(n-1, k-1, \lambda)$ configuration. En effet, elle contient des blocs de taille $k-1$ pris dans un ensemble $V \setminus \{v\}$ de $n-1$ sommets. Soit S sous-ensemble de $t-1$ sommets de $V \setminus \{v\}$. L'application $f : \mathcal{B} \rightarrow \mathcal{C}'$ qui à chaque blocs de $B \in \mathcal{B}$ associe $B \setminus \{v\}$ est une bijection. Elle envoie les blocs contenant $S \cup \{v\}$ sur les blocs contenant S . Or comme \mathcal{C} est une t - (n, k, λ) configuration, il y a exactement λ blocs B_1, \dots, B_λ contenant le sous-ensemble $S \cup \{v\}$ qui est de taille t . Ainsi S est dans exactement λ blocs de \mathcal{C}' à savoir $f(B_1), \dots, f(B_\lambda)$. \square

On sait qu'il existe une 5-(12, 6, 1) configuration. Par la Proposition 21, cela implique l'existence d'une 4-(11, 5, 1) configuration, d'une 3-(10, 4, 1) configuration et d'une (9, 3, 1) configuration.

De même, il existe une 5-(24, 8, 1) configuration qui implique l'existence d'une 4-(23, 7, 1) configuration, d'une 3-(22, 6, 1) configuration et d'une (21, 5, 1) configuration.

Lemme 22. *K_{2m+1} se décompose en copies de K_3 si, et seulement si, K_{m*2} se décompose en copies de K_3 .*

Preuve. Soient $\{v_1, \dots, v_{2m+1}\}$ les sommets de K_{2m+1} . Soit \mathcal{D} une décomposition de K_{2m+1} en K_3 . Soit \mathcal{A} l'ensemble des éléments de \mathcal{D} qui contiennent v_{2m+1} . Observons que $|\mathcal{A}| = m$ car v_{2m+1} est adjacent à $2m$ arêtes dans K_{2m+1} et que chaque K_3 contenant ce sommet contient deux de ces arêtes. Sans perte de généralité, on peut supposer que $\mathcal{A} = \{\{v_i, v_{i+m}, v_{2m+1}\} \mid i \in [m]\}$. Maintenant, il est facile de voir que $\mathcal{D} \setminus \mathcal{A}$ est une décomposition en K_3 du graphe H obtenu à partir du graphe complet sur $\{v_1, \dots, v_{2m}\}$ en ôtant les arêtes $v_i v_{i+m}$, $i \in [m]$. Le graphe H est isomorphe à K_{m*2} .

Réciproquement, si \mathcal{D}' est une décomposition de H en copies de K_3 , alors $\mathcal{D} \cup \mathcal{A}$ est une décomposition de K_{2m+1} en copies de K_3 . \square

Ce lemme se généralise facilement de la façon suivante.

Lemme 23. *Soit q un entier positif. K_{qm+1} se décompose en copies de K_{q+1} si, et seulement si, K_{m*q} se décompose en copies de K_{q+1} .*

5 Cas particuliers

Dans cette partie, on étudie l'existence de $(n, k, 1)$ configurations pour des valeurs spéciales de n et k . Nous étudierons également d'autres types de configurations qui correspondent à des décompositions des graphes multipartis complets en graphes complets.

5.1 Plans projectifs

Définition 24. Un **plan projectif** (fini) est une paire d'ensembles de points et de droites tels que :

- (PP1) Par deux points passent une et une seule droite.
- (PP2) Deux droites s'intersectent en un seul point (pas de parallèles).
- (PP3) Il existe quatre points tels que trois quelconques d'entre eux ne sont pas colinéaires.

La condition (A3) est là pour éviter les cas dégénérés suivants :

- tous les points sur la même droite ;
- des droites concourantes en un même point ;
- tous les points sauf un sur la même droite.

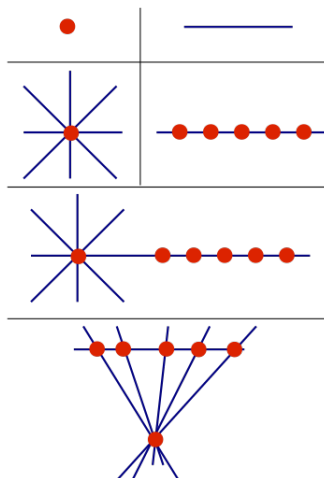


FIGURE 7 – Les cas dégénérés

Exemple 25. Le Plan de Fano est un plan projectif.

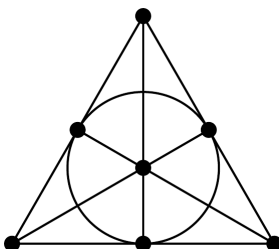


FIGURE 8 – Le Plan de Fano

Proposition 26. Soit Π un plan projectif fini. Il existe q , appelé **ordre** de Π , tel que :

- Chaque droite contient exactement $q + 1$ points.
- Chaque point est dans exactement $q + 1$ droites.
- Il y a $q^2 + q + 1$ droites et $q^2 + q + 1$ points.

Preuve. La preuve découle facilement de l'observation suivante qui est une conséquence immédiate de (PP1) et (PP2).

Si x est un point et D une droite ne contenant pas x , alors le nombre de droites passant par x est égal au nombre de points de D .

Prenons deux droites distinctes D_1 et D_2 . Alors par (PP3), il existe un point x qui n'est ni dans D_1 ni dans D_2 . Par l'observation ci-dessus D_1 et D_2 ont le même nombre de points (i.e. celui du nombre de droites passant par x). Ainsi toutes les droites ont le même nombre de points. De même, tous les points sont dans le même nombre de droites ; et ces deux constantes sont égales. Ceci prouve (i) et (ii).

(iii) Soit x un point. Tous les points sont contenus dans les droites passant par x par (PP1). D'après (i), il y a $q + 1$ droites passant par x , et d'après (ii) chacune d'entre elles contient q points différents de x . De plus,

par (PP2), ces $q(q+1)$ points sont tous distincts. Ainsi Π a $q^2 + q + 1$ points. De même, on montre que Π a $q^2 + q + 1$ droites. \square

La Proposition 26 implique que les plans projectifs correspondent aux $(q^2 + q + 1, q + 1, 1)$ configurations. En effet, au plan projectif d'ordre q , on peut associer la configuration dont les points sont les sommets et les droites sont les blocs. A l'inverse, on peut facilement montrer que toute $(q^2 + q + 1, q + 1, 1)$ configuration est issue d'un plan projectif.

Savoir s'il existe une $(q^2 + q + 1, q + 1, 1)$ configuration, savoir si K_{q^2+q+1} se décompose en copies de K_{q+1} , ou savoir s'il existe un plan projectif d'ordre q , sont donc le même problème. On sait construire un plan projectif d'ordre q à partir d'un corps fini d'ordre q . Comme il existe des corps finis pour tout q puissance d'un nombre premier, on obtient le théorème suivant.

Théorème 27. *Si q est une puissance d'un nombre premier, alors K_{q^2+q+1} se décompose en copies de K_{q+1} . Autrement dit, si q est une puissance d'un nombre premier, alors il y a un plan projectif d'ordre q .*

Cela implique l'existence de plan projectif pour $q = 2, 3, 4, 5$.

La seule condition suffisante connue de non-existence d'un plan projectif est la contraposée de la condition nécessaire d'existence suivante.

Théorème 28 (Bruck-Ryser [5]). *Soit $q \equiv 1$ ou $2 \pmod{4}$. S'il existe un plan projectif d'ordre q , alors q est la somme de deux carrés.*

6 n'étant pas la somme de deux carrés, il n'en existe pas de plan projectif d'ordre 6, ce qui répond par la négative au problème des 36 officiers d'Euler. Il a été prouvé [17] en 1989 qu'il n'existe pas de plan projectif d'ordre 10. Pour $q = 12, 15, 18, \dots$, l'existence d'un plan projectif d'ordre q reste ouvert.

5.2 Décompositions de tripartis et quadripartis complets

Théorème 29. *K_{3*q} se décompose en copies de K_3 .*

Démonstration. Soit (A, B, C) la tripartition de K_{3*q} , avec $A = \{a_i \mid i \in [q]\}$, $B = \{b_i \mid i \in [q]\}$, et $C = \{c_i \mid i \in [q]\}$. On peut vérifier que $\{\{a_i, b_j, c_{i+j}\} \mid i \in [q], j \in [q]\}$ (les indices sont modulo q) est une décomposition de K_{3*q} en copies de K_3 . \square

Il existe une décomposition de K_{4*q} en copies de K_4 si $q = 3, 4, 5, 7, 8, 9, 10$. Pour $q = 6$, il n'en existe pas. C'est équivalent au problème des 36 officiers d'Euler. En effet, soit (A, B, C, D) la quadripartition de K_{4*q} , avec $A = \{a_i \mid i \in [6]\}$, $B = \{b_j \mid j \in [6]\}$, $C = \{c_k \mid k \in [6]\}$, et $D = \{d_\ell \mid \ell \in [6]\}$. On peut voir chacune des arêtes $a_i b_j$ comme un officier de grade i dans le régiment j . Le sommets c_k comme la colonne k et le sommet d_ℓ comme la ligne ℓ . Un K_4 correspond donc à un officier à une place. L'arête $a_i c_k$ ne peut être que dans une seule copie de K_4 , donc il y a un seul officier de grade i dans la colonne k . De même, il y a un seul officier de chaque régiment par colonne et un seul officier de chaque grade (régiment) par ligne.

En fait, $q \neq 6$ est la seule valeur pour laquelle K_{4*q} ne se décompose pas en copies de K_4 .

Théorème 30 (Bose-Shrikhande-Parker [4]). *Pour tout $q \geq 3$, $q \neq 6$, K_{4*q} se décompose en copies K_4 .*

Preuve. Nous allons prouver ce théorème uniquement pour les valeurs de q dont nous aurons besoin plus tard, à savoir $q = 4$ et q impair.

Pour $q = 4$, cela dérive de l'existence d'un plan projectif d'ordre 4 (i.e. K_{21} se décompose en K_5), par le Lemme 23.

Dans le cas où q est impair, soit (A, B, C, D) la quadripartition de K_{4*q} , avec $A = \{a_i \mid i \in [q]\}$, $B = \{b_i \mid i \in [q]\}$, $C = \{c_i \mid i \in [q]\}$, et $D = \{d_i \mid i \in [q]\}$.

On considère l'ensemble de blocs $\{a_i, b_j, c_{i+j}, d_{i-j} \mid i \in [q], j \in [q]\}$. Montrons que c'est bien une décomposition de K_{4*q} .

Pour cela, il suffit de montrer qu'il n'existe pas deux couples (i, j) et (i', j') tels que $i + j = i' + j' \pmod{q}$ et $i - j = i' - j' \pmod{q}$. Supposons par l'absurde que $i + j = i' + j' \pmod{q}$ and $i - j = i' - j' \pmod{q}$. On a donc $2i = 2i' \pmod{q}$ and $2j = 2j' \pmod{q}$. Comme q est impair, cela implique que $i = i'$ et $j = j'$.

Dans le cas pair, ça ne marche pas car (i, j) et $(i + q/2, j + q/2)$ vérifie $i + j = i + q/2 + j + q/2 \pmod{q}$ et $i - j = i + q/2 - j + q/2 \pmod{q}$. \square

6 Preuve du Théorème de Kirkman

Le but de cette Partie est de prouver le Théorème de Kirkman, dont nous rappelons l'énoncé.

Théorème 13. *Si $n \equiv 1$ ou $3 \pmod{6}$, alors K_n se décompose en copies de K_3 .*

Afin de prouver ce théorème, nous prouvons les deux suivants.

Théorème 31. *Si $r \equiv 0$ ou $1 \pmod{3}$, alors K_r se décompose en copies de K_3 , K_4 et K_6 .*

Preuve du Théorème 13 en supposant le Théorème 31.

Posons $r = \frac{n-1}{2}$. Puisque $n \equiv 1$ ou $3 \pmod{6}$, alors $r \equiv 0$ ou $1 \pmod{3}$.

Par le Théorème 31, il y a une décomposition \mathcal{D} de K_r en copies de K_3 , K_4 et K_6 .

A chaque sommet de K_r on associe deux sommets u_1 et u_2 et on ajoute un sommet supplémentaire z . Nous avons ainsi n sommets.

Considérons le K_{r*2} obtenu à partir de K_r en remplaçant chaque sommet u par un stable de taille 2 $\{u_1, u_2\}$. Pour $i \in \{3, 4, 6\}$, chaque copie de K_i dans \mathcal{D} correspond alors à un K_{i*2} dans le K_{r*2} . Or chacun des K_{i*2} se décompose en K_3 . En effet, les Exemples 2, 6 et 3 nous montrent que K_7 , K_9 et K_{13} se décomposent en K_3 . Ainsi, par le Lemme 22, K_{3*2} , K_{4*2} et K_{6*2} se décomposent en copies K_3 . Ainsi K_{r*2} se décompose en copies de K_3 .

Le Lemme 22 implique alors que $K_{2r+1} = K_n$ se décompose en copies de K_3 . \square

Il nous reste maintenant à prouver le Théorème 31.

Preuve du Théorème 31. Par récurrence, le résultat étant trivialement vrai pour $r = 3, 4, 6$.

Posons $r = 9m + j$ avec $j \in \{0, 1, 3, 4, 6, 7\}$.

– Supposons que $r = 9m$. On partitionne $V(K_{9m})$ entre trois ensembles A_1, A_2, A_3 de taille $3m$. On décompose K_{9m} en trois K_{3m} induits par A_1, A_2 et A_3 et un K_{3*3m} de tripartition (A_1, A_2, A_3) .

Par hypothèse de récurrence, chacun des K_{3m} se décompose en copies de K_3, K_4 et K_6 et K_{3*3m} se décompose en K_3 par Théorème 29.

– Supposons que $r = 9m + 3$. On partitionne $V(K_{9m+3})$ entre trois ensembles A_1, A_2, A_3 de taille $3m + 1$. On décompose K_{9m+3} en trois K_{3m} induits par A_1, A_2 et A_3 et un $K_{3*(3m+1)}$ de tripartition (A_1, A_2, A_3) . Par hypothèse de récurrence, chacun des K_{3m+1} se décompose en copies de K_3, K_4 et K_6 et $K_{3*(3m+1)}$ se décompose en K_3 par Théorème 29.

– Supposons que $r = 9m + 1$. On partitionne $V(K_{9m+1})$ entre trois ensembles A_1, A_2, A_3 de taille $3m$ et un sommet z . On décompose K_{9m+1} en trois K_{3m+1} induits par $A_1 \cup \{z\}, A_2 \cup \{z\}$ et $A_3 \cup \{z\}$ et un K_{3*3m} de tripartition (A_1, A_2, A_3) . Par hypothèse de récurrence, chacun des K_{3m+1} se décompose en copies de K_3, K_4 et K_6 et $K_{3*(3m)}$ se décompose en K_3 par Théorème 29.

– Supposons que $r = 9m + 4, r = 9m + 6$ ou $r = 9m + 7$. On partitionne $V(K_{9m+3+h})$ entre trois ensembles A_1, A_2, A_3 de taille $3m + 1$ et un ensemble de h sommets. ($h \in \{1, 3, 4\}$). On décompose K_{9m+3+h} en trois K_{3m+1} induits par A_1, A_2 et A_3 , un $K_{3m+1, 3m+1, 3m+1, h}$ et éventuellement un K_3 ou K_4 si $h = 3$ ou $h = 4$ respectivement. Par hypothèse de récurrence, chacun des K_{3m+1} se décompose en copies de K_3, K_4 et K_6 . D'après le Théorème 30, $K_{4*(3m+1)}$ se décompose en K_4 . Cette décomposition se transforme en une décomposition de $K_{3m+1, 3m+1, 3m+1, h}$ en K_3 et K_4 en ôtant les sommets en trop. (Il y en a au plus un par K_4 de la décomposition car les sommets en trop forment un stable). \square

Remarque 32. Nous n'avons prouvé le Théorème 30 que dans le cas impair. La preuve précédente peut se prouver en utilisant que ce cas particulier. Il suffit dans le cas $r = 9m + 4, r = 9m + 6$ ou $r = 9m + 7$ et $3m + 1$ pair de partitionner K_r en trois ensembles A_1, A_2, A_3 de taille $3m$ (on aura $3m$ impair) et un ensemble de h' sommets avec $h' \in \{4, 6, 7\}$.

7 Rödl Nibble

Les $(n, k, 1)$ configurations que nous venons de voir sont des cas parfaits, où le graphe complet à n sommets peut se décomposer en copies de K_k . Nous avons cependant vu que de telles décompositions n'existent pas toujours, notamment à cause des conditions nécessaires triviales données dans la Partie 2.

Dans le cas, où il n'en existe pas on peut donc se poser les deux questions assez proches.

Combien de copies de K_k arête-disjointes peut on mettre dans K_n au maximum ?

Combien de copies de K_k au minimum faut-il pour couvrir toutes les arêtes de K_n ?

La première question consiste à déterminer la taille maximale $m(n, k)$ d'un paquet de K_k dans K_n . Un **paquet** de G_2 dans G_1 est un ensemble de copies arête-disjointes de G_2 dans G_1 . La seconde revient à trouver la taille minimale $M(n, k)$ d'un recouvrement de K_n par K_k . Un **recouvrement** de G_1 par G_2 est un ensemble de copies de G_2 telles que toute arête de G_1 soit dans une de ces copies.

Exemple 33. $n = 5, k = 3, \lambda = 1$. On ne peut pas décomposer K_5 en copies de K_3 . (Il n'existe pas de $(5, 3, 1)$ configuration.) En effet, la condition nécessaire (CN1) n'est pas vérifiée : K_5 possède 10 arêtes, ce qui n'est pas divisible par 3, le nombre d'arêtes de K_3 . Il est facile de voir qu'un paquet de K_3 dans K_5 et de taille au plus 2. Un paquet de taille 2 est représenté Figure 9. De même, un recouvrement de K_5 par des K_3 doit avoir au moins $\lceil 10/3 \rceil = 4$ K_3 . C'est faisable avec quatre K_3 comme dessiné Figure 9.



FIGURE 9 – Un paquet de deux K_3 dans K_5 (à gauche) et un recouvrement de K_5 par quatre K_3 (à droite).

Clairement $m(n, k) \leq \frac{\binom{n}{2}}{\binom{k}{2}} \leq M(n, k)$. L'Exemple 33 montre que $m(5, 3) = 2$ et $M(5, 3) = 4$. De plus, si K_n se décompose en copies de K_k , alors cette décomposition est à la fois un paquet de K_k dans K_n et un recouvrement de K_n par K_k et $m(n, k) = \frac{\binom{n}{2}}{\binom{k}{2}} = M(n, k)$.

Plus généralement, les t - $(n, k, 1)$ configurations peuvent être vues comme des décompositions de l'hypergraphe complet t -uniforme à n sommets $K_n^{(t)}$ en copies de $K_k^{(t)}$, l'hypergraphe complet t -uniforme à k sommets.

Exemple 34. $t = 3, n = 6, k = 3, \lambda = 1$. $K_6^{(3)}$ ne peut pas se décomposer en copies de $K_4^{(3)}$. (Il n'existe pas de 3 - $(6, 4, 1)$ configuration.) En effet, la condition nécessaire (CN2) n'est pas vérifiée : chaque sommet de $K_6^{(3)}$ est dans 10 hyperarêtes, et une copie de $K_4^{(3)}$ contient 3 hyperarêtes contenant chacun de ces sommets. On peut aisément voir qu'un paquet de $K_4^{(3)}$ dans $K_6^{(3)}$ contient au plus 3 éléments. Un tel paquet est représenté Figure 10. De plus, chaque sommet devant être dans au moins $\lceil 10/3 \rceil = 4$ $K_4^{(3)}$, il faut au moins six $K_4^{(3)}$ pour recouvrir $K_6^{(3)}$. La Figure 10 donne un recouvrement de $K_6^{(3)}$ par six $K_4^{(3)}$.

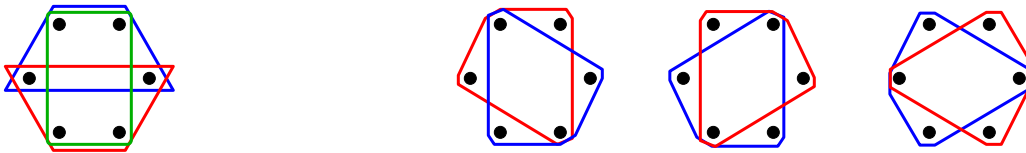


FIGURE 10 – Un paquet de trois $K_4^{(3)}$ dans $K_6^{(3)}$ (à gauche) et un recouvrement de $K_6^{(3)}$ par six $K_4^{(3)}$ (à droite).

On note $m(n, k, t)$ la taille maximale d'un paquet de $K_k^{(t)}$ dans $K_n^{(t)}$ et $M(n, k, t)$ la taille minimale d'un recouvrement de $K_n^{(t)}$ par $K_k^{(t)}$. Notons que $m(n, k) = m(n, k, 2)$ et $M(n, k) = M(n, k, 2)$. Généralisant ce qui a été écrit précédemment, nous avons

$$m(n, k, t) \leq \frac{\binom{n}{t}}{\binom{k}{t}} \leq M(n, k, t).$$

L'Exemple 34 montre que $m(6, 4, 3) = 3 < \frac{\binom{6}{3}}{\binom{4}{3}} = 5 < M(6, 4, 3) = 6$.

En 1963, Erdős et Hanani [9] ont conjecturé qu'asymptotiquement (i.e. quand n tend vers $+\infty$ et k et t ($k > t \geq 2$) sont fixés alors on s'approche du cas parfait des t - $(n, k, 1)$ configurations, à savoir

$$\lim_{n \rightarrow +\infty} \frac{M(n, k, t)}{\binom{n}{t} / \binom{k}{t}} = 1 \quad \text{et} \quad \lim_{n \rightarrow +\infty} \frac{m(n, k, t)}{\binom{n}{t} / \binom{k}{t}} = 1.$$

Comme Erdős et Hanani l'ont observé, il n'est pas très compliqué de voir que si l'une des deux limites vaut 1 alors l'autre aussi. En 1985, Rödl [22] a montré la conjecture d'Erdős et Hanani.

Théorème 35. *Soient k et t des entiers fixés.*

$$M(n, k, t) \leq (1 + o(1)) \binom{n}{t} / \binom{k}{t} \quad \text{et} \quad m(n, k, t) \leq (1 - o(1)) \binom{n}{t} / \binom{k}{t}.$$

Soit \mathcal{H} l'hypergraphe dont les sommets sont les sous-ensembles de taille t de $[n]$ et les hyperarêtes les ensembles des $\binom{k}{t}$ sous-ensembles de taille t qui sont dans un sous-ensemble de taille k . Autrement dit, les sommets de \mathcal{H} sont les arêtes de $K_n^{(t)}$ et les hyperarêtes de \mathcal{H} correspondent aux copies de $K_k^{(t)}$ dans $K_n^{(t)}$. Un paquet de $K_k^{(t)}$ dans $K_n^{(t)}$ correspond alors à un couplage dans \mathcal{H} . Un **couplage** dans un hypergraphe est un ensemble d'hyperarêtes deux à deux disjointes. De même, un recouvrement dans $K_n^{(t)}$ correspond à une couverture dans \mathcal{H} . Une **couverture** dans un hypergraphe est un ensemble d'hyperarêtes tel que tout sommet est contenu dans une de ces hyperarêtes. Observons que \mathcal{H} a $N = \binom{n}{t}$ sommets est r -uniforme avec $r = \binom{k}{t}$ et D -régulier avec $D = \binom{n-t}{k-t}$.

Rödl a montré que \mathcal{H} avait un couplage et une couverture de taille environ N/r . Plusieurs chercheurs ont généralisé ce résultat pour certaines classes d'hypergraphes D -réguliers r -uniformes. Ce fut tout d'abord fait par Frankl et Rödl [11]. Leur résultat a ensuite été simplifié et étendu par Pippenger et Spencer [19] ainsi que par Kahn et Alon, Kim, et Spencer [1]. Nous suivons ici la preuve de Pippenger et Spencer telle qu'expliquée dans le livre d'Alon et Spencer [2].

Pour un hypergraphe D -régulier r -uniforme d'ordre N , avoir un couplage de taille $\frac{N}{r}(1 - o(1))$ est équivalent à avoir une couverture de taille $\frac{N}{r}(1 + o(1))$. En effet, s'il y a un couplage de taille $\frac{N(1-\epsilon)}{r}$, alors il y a au plus ϵN sommets non-couverts par les hyperarêtes du couplage. En couvrant chacun de ces sommets par une hyperarête, on obtient alors une couverture de H de taille au plus $\frac{N(1-\epsilon)}{r} + \epsilon N$, ce qui tend vers N/r quand ϵ tend vers 0. Réciproquement, s'il y a une couverture \mathcal{C} de taille $\frac{N(1+\epsilon)}{r}$, alors pour tout sommet x qui est couvert par $d_{\mathcal{C}}(x)$ hyperarêtes, on choisit $d_{\mathcal{C}}(x) - 1$ hyperarêtes de \mathcal{A} qu'on enlève. On obtient ainsi un couplage. Le nombre d'hyperarêtes supprimées est au plus $\sum_{v \in V} (d_{\mathcal{C}}(x) - 1) = \frac{(1+\epsilon)N}{r} \times r - N = \epsilon N$. Ainsi on peut trouver un couplage de taille au moins $\frac{N(1-\epsilon)}{r} - \epsilon N$, ce qui tend vers N/r quand ϵ tend vers l'infini.

Dans la suite, nous nous concentrerons donc sur les couvertures.

L'idée de Rödl est de "grignoter" petit à petit l'hypergraphe : on choisit un ensemble d'environ $\epsilon N/r$ hyperarêtes au hasard. Avec forte probabilité, seulement $O(\epsilon^2 N)$ sommets seront couverts deux fois ou plus, et donc l'ensemble de sommets couverts par ces hyperarêtes est de taille $\epsilon N - O(\epsilon^2 N)$. On ôte les sommets couverts (et les hyperarêtes les contenant) et on recommence le processus jusqu'à ce qu'il ne reste plus qu' ϵN sommets non-couverts. On peut alors finalement couvrir chacun par une hyperarête chacun. Ce n'est pas très efficace mais comme ϵN est aussi petit qu'on veut, on peut le tolérer. Tout le problème est de trouver des conditions pour les étapes de grignotage qui soient stables (et qui recouvrent le cas de l'hypergraphe \mathcal{H} qui nous intéresse). Clairement, après un grignotage, on ne peut pas espérer que l'hypergraphe reste régulier. On va donc se donner un peu de mou en autorisant l'hypergraphe à être seulement presque régulier. On veut seulement que presque tous les sommets soient de degré presque D . (Voir condition (1) dans le Théorème 36.) On note $d = a \pm b$ pour $d \in]a - b, a + b[$. D'autres conditions doivent également être ajoutées pour pouvoir faire des grignotages successifs.

Pour toute paire de sommets distincts (x, y) , son **codegré**, noté $d(x, y)$ est le nombre d'hyperarêtes de H qui contiennent x et y . Observons que dans \mathcal{H} nous avons $d(x, y) = \binom{n-t-1}{k-t-1} = o(D)$ pour toute paire de sommets x et y . Nous allons prouver le théorème suivant du à Pippenger et Spencer [19].

Théorème 36. *Soit $r \geq 2$ un entier. Pour tous $\kappa \geq 1$ et $a > 0$, il existe $\gamma = \gamma(r, \kappa, a) > 0$ et $d_0 = d_0(r, \kappa, a)$ tels que l'assertion suivante soit vraie pour tout $N \geq D \geq d_0$.*

Tout hypergraphe r -uniforme $H = (V, \mathcal{E})$ à N sommets vérifiant les conditions

(0) $d(x) > 0$ pour tout $x \in V$.

(1) Tous les sommets x de V sauf au plus γN d'entre eux satisfont $d(x) = (1 \pm \gamma)D$.

(2) Pour tout $x \in V$, $d(x) < \kappa D$.

(3) Pour toute paire (x, y) de sommets distincts, $d(x, y) < \gamma D$.

à une couverture d'au plus $(1 + a)\frac{N}{r}$ arêtes.

La condition (0) n'est là que pour éviter les sommets isolés qui ne peuvent pas être couverts. Afin de prouver ce théorème, nous allons prouver le lemme suivant qui montre que sous les conditions (1), (2), (3) ci-dessus, on peut effectuer un "grignotage".

Lemme 37. Soit $r \geq 2$ un entier. Pour tous $K \geq 1$, $\epsilon > 0$ et $\delta' > 0$, il existe $\delta = \delta(r, K, \epsilon, \delta') > 0$ et $D^* = D^*(r, K, \epsilon, \delta')$ tels que l'assertion suivante soit vraie pour tout $N \geq D \geq D^*$. Tout hypergraphe r -uniforme $H = (V, \mathcal{E})$ à N sommets vérifiant les conditions

(i) Tous les sommets x de V sauf au plus δN d'entre eux satisfont $d(x) = (1 \pm \delta)D$.

(ii) Pour tout $x \in V$, $d(x) < KD$.

(iii) Pour toute paire (x, y) de sommets distincts, $d(x, y) < \delta D$.

contient un ensemble \mathcal{E}' d'hyperarêtes ayant les propriétés suivantes :

(iv) $|\mathcal{E}'| = \frac{N}{r}\epsilon(1 \pm \delta')$.

(v) L'ensemble $V' = V \setminus \bigcup_{e \in \mathcal{E}'} e$ est de cardinalité $Ne^{-\epsilon}(1 \pm \delta')$.

(vi) Tous les sommets x de V' sauf au plus $\delta'|V'|$ le degré $d'(x)$ de x dans l'hypergraphe induit par H sur V' vérifie $d'(x) = De^{-\epsilon(r-1)}(1 \pm \delta')$.

Avant de prouver le Lemme 37, nous allons montrer comment prouver le Théorème 36 avec lui.

Preuve du Théorème 36 (en supposant le Lemme 37). Soit $a > 0$.

Prenons δ et ϵ tels que $0 < \delta < 1/10$ et

$$(1 + 4\delta)\frac{\epsilon}{1 - e^{-\epsilon}} + r\epsilon < 1 + a.$$

Soit p un entier tel que $e^{-\epsilon p} < \epsilon$. On va montrer le théorème en appliquant p fois le Lemme 37.

Pour tout i , posons $K_i = \kappa e^{i(r-1)}$.

Quitte à diminuer δ , on peut supposer que $\prod_{i=0}^p (1 + \delta e^{-i\epsilon(r-1)}) \leq \frac{1+2\delta}{1+4\delta}$.

Posons $\delta_p = \delta$ et définissons par récurrence (inversée) $\delta_p > \delta_{p-1} > \dots > \delta_0$ tels que

$$\delta_{i-1} \leq \min(\delta(r, K_{i-1}, \epsilon, \delta_i), \delta_i e^{-\epsilon(r-1)}).$$

Pour $D \geq d_0$ (que nous déterminerons plus tard), notons $D_i = De^{-\epsilon i(r-1)}$. On va appliquer le Lemme 37 p fois, sur des hypergraphes r -uniformes $H = H_0, \dots, H_{p-1}$. A l'étape i , on applique le lemme à H_{i-1} pour ϵ , $K = K_{i-1}$, $\delta' = \delta_i$.

Comme $\delta_{i-1} \leq \delta(r, K_{i-1}, \epsilon, \delta_i)$ et $D_{i-1} \geq D^*(r, K_{i-1}, \epsilon, \delta_i)$, le Lemme 37, nous dit que l'hypergraphe H_{i-1} a un ensemble d'hyperarêtes \mathcal{E}'_i tel que

(iv) $|\mathcal{E}'_i| = \frac{\epsilon}{r}|V_{i-1}|(1 \pm \delta_i)$.

(v) L'ensemble $V_i = V_{i-1} \setminus \bigcup_{S \in \mathcal{E}'_i} S$ est de cardinalité $|V_{i-1}|e^{-\epsilon}(1 \pm \delta_i)$.

(vi) L'hypergraphe H_i induit par H sur V_i a la propriété que tous ses sommets x sauf au plus $\delta_i|V_i|$ sont de degré $D_{i-1}e^{-\epsilon(r-1)}(1 \pm \delta_i) = (1 \pm \delta_i)D_i$.

Pour voir que nous pouvons appliquer le lemme itérativement, il faut montrer qu'après l'étape i , le nouvel hypergraphe satisfait les conditions du Lemme 37 pour ϵ , $K = K_i$, $\delta' = \delta_{i+1}$. La condition (i) du lemme est donnée par la condition (vi) ci-dessus. La condition (ii) découle trivialement du fait que $d_{H_i}(x) < d_{H_{i-1}}(x)$ et $K_i D_i = K_{i-1} D_{i-1}$. La condition (iii) découle trivialement du fait que $d_{H_i}(x, y) < d_{H_{i-1}}(x, y)$ et $K_i D_i \geq K_{i-1} D_{i-1}$, par notre choix de δ_{i-1} .

Enfin, en choisissant pour chaque sommet de V_p une hyperarête qui le contient, on obtient un ensemble d'hyperarêtes \mathcal{E}'_{p+1} . Clairement, $\bigcup_{i \in [p+1]} \mathcal{E}'_i$ est une couverture de H . Posons $P = \prod_{i=0}^p (1 + \delta_i)$. Observons que $P \leq \prod_{i=0}^p (1 + \delta e^{-i\epsilon(r-1)}) \leq \frac{1+4\delta}{1+2\delta}$.

Maintenant pour tout $0 \leq i \leq p$, on a $|V_i| \leq |V_0|e^{-i\epsilon P} \leq |V_0|e^{-i\epsilon(1+2\delta)}$. De même, pour tout $1 \leq i \leq p$, on a $|\mathcal{E}'_i| = (\frac{\epsilon}{r}|V_{i-1}|)(1 \pm \delta_i) \leq \frac{\epsilon}{r}Ne^{-(i-1)\epsilon}(1 + 2\delta)P \leq \frac{\epsilon}{r}Ne^{-(i-1)\epsilon}(1 + 4\delta)$. Ainsi la couverture est de

taille au plus

$$\begin{aligned}
(1 + 4\delta) \frac{\epsilon}{r} N \sum_{i=0}^{p-1} e^{-i\epsilon} + |V_p| &\leq (1 + 4\delta) \frac{\epsilon N}{r} \frac{1}{1 - e^{-\epsilon}} + (1 + 2\delta) N e^{-\epsilon p} \\
&\leq \frac{N}{r} (1 + 4\delta) \left(\frac{1}{1 - e^{-\epsilon}} + r\epsilon \right) \\
&< (1 + a) \frac{N}{r}.
\end{aligned}$$

□

Il nous reste donc à montrer le Lemme 37.

Preuve du Lemme 37. Nous supposons que D et donc N sont suffisamment grands à chaque fois que ce sera nécessaire. De plus, nous notons $\delta_1, \delta_2, \dots$ des constantes strictement positives qui tendent vers 0 quand δ tend vers 0 et D tend vers l'infini et à r, K et ϵ fixés (et qui peuvent être explicitées). Ainsi en choisissant δ et D de manière appropriée, on peut s'assurer que toutes ces constantes seront plus petites que δ' .

Soit \mathcal{E}' un sous-ensemble aléatoire de \mathcal{E} obtenu en prenant indépendamment chaque hyperarête de \mathcal{E} avec probabilité $p = \epsilon/D$. Nous allons montrer qu'avec probabilité non-nulle, les propriétés (iv), (v) et (vi) du lemme sont vérifiées. Pour cela, nous allons montrer que chacune des propriétés (iv), (v), et (vi) sont vérifiées avec très forte probabilité, disons au moins 0,9. Cela impliquera que les trois ensemble seront vérifiées avec probabilité au moins 0,7 > 0.

La preuve pour (iv) est aisée. Par hypothèse, H a au moins $(1 - \delta)N$ sommets de degré au moins $(1 - \delta)D$. Il a donc au moins $\frac{1}{r}(1 - \delta)^2 DN$ hyperarêtes. De même, le nombre d'hyperarêtes de H n'excède pas $\frac{1}{r}(1 + \delta)DN + \delta KDN$. Ainsi $|\mathcal{E}| = (1 \pm \delta_1) \frac{DN}{r}$. Ainsi l'espérance¹ de la taille de \mathcal{E}' est $\mathbf{E}(|\mathcal{E}'|) = |\mathcal{E}|p = (1 \pm \delta_1) \frac{\epsilon N}{r}$ et sa variance est $\mathbf{Var}(|\mathcal{E}'|) = |\mathcal{E}|p(1 - p) \leq (1 \pm \delta_1) \frac{\epsilon N}{r}$. Ainsi, par l'Inégalité de Chebyshev, pour δ_2 bien choisi, nous avons

$$\Pr \left(|\mathcal{E}'| = (1 \pm \delta_2) \frac{\epsilon N}{r} \right) > 0,9.$$

Ceci montre que (iv) est vérifié avec probabilité au moins 0,9.

Regardons maintenant (v). Pour chaque sommet $x \in V$, on définit la variable aléatoire indicatrice I_x par $I_x = 1$ si $x \notin \bigcup_{e \in \mathcal{E}'} e$ et $I_x = 0$ sinon. Notons que $|V'| = \sum_{x \in V} I_x$.

Un sommet est dit **bon** si $d(x) = (1 \pm \delta D)$, et **mauvais** sinon. Si x est bon, alors

$$\mathbf{E}(I_x) = \Pr(I_x = 1) = (1 - p)^{d(x)} = \left(1 - \frac{\epsilon}{D}\right)^{(1 \pm \delta D)} = e^{-\epsilon(1 \pm \delta_3)}.$$

Si x est mauvais, alors, trivialement, $0 \leq \mathbf{E}(I_x) \leq 1$. Comme il y a au plus δN mauvais sommets, par la Linéarité de l'Espérance, l'espérance de $|V'|$ vaut $N e^{-\epsilon(1 \pm \delta_4)}$.

Pour calculer la variance de $|V'| = \sum_{x \in V} I_x$, observons que

$$\begin{aligned}
\mathbf{Var}(|V'|) &= \sum_{x \in V} \mathbf{Var}(I_x) + \sum_{x, y \in V, x \neq y} \mathbf{Cov}(I_x, I_y) \\
&\leq \mathbf{E}(|V'|) + \sum_{x, y \in V, x \neq y} \mathbf{Cov}(I_x, I_y)
\end{aligned}$$

Mais

$$\begin{aligned}
\mathbf{Cov}(I_x, I_y) &= \mathbf{E}(I_x I_y) - \mathbf{E}(I_x) \mathbf{E}(I_y) = (1 - p)^{d(x) + d(y) - d(x, y)} - (1 - p)^{d(x) + d(y)} \\
&\leq (1 - p)^{-d(x, y)} - 1 \leq \left(1 - \frac{\epsilon}{D}\right)^{-\delta(D)} - 1 \leq \delta_5.
\end{aligned}$$

Pour cette dernière ligne, nous avons besoin de la condition (iii) dans l'énoncé du Lemme 37. Ceci nous donne

$$\mathbf{Var}(|V'|) \leq \mathbf{E}(|V'|) + \delta_5 N^2 \leq \delta_6 (\mathbf{E}(|V'|))^2.$$

1. Les éléments de probabilité ne sont pas donnés dans ces notes de cours. Nous renvoyons le lecteur vers [2]

Par l'Inégalité de Chebyshev, on obtient qu'avec probabilité au moins $0,9$ nous avons

$$|V'| = (1 \pm \delta_7) \mathbf{E}(|V'|) = (1 \pm \delta_8) N e^{-\epsilon},$$

donc (v) est vérifiée.

Il reste à montrer que (vi) est vérifiée avec très forte probabilité.

Tout d'abord, notons que tous les sommets x sauf au plus $\delta_9 N$ satisfont les deux conditions suivantes :

(A) $d(x) = (1 \pm \delta)D$, et

(B) toutes les hyperarêtes e de \mathcal{E} contenant x sauf au plus $\delta_{10}D$ satisfont

$$|\{f \in \mathcal{E} \mid x \notin f, f \cap e \neq \emptyset\}| = (1 \pm \delta_{11})(r-1)D. \quad (\star)$$

En effet, (A) est vraie pour tous les sommets sauf au plus $\delta N < \delta_9 N/2$ sommets par hypothèse. De plus, le nombre total d'hyperarêtes contenant des sommets dont le degré n'est pas $(1 \pm \delta)D$ est au plus $\delta N K D$ et donc le nombre de sommets contenus dans plus de $\delta_{10}D$ telles hyperarêtes est au plus $\frac{\delta N K D r}{\delta_{10} D} \leq \delta_9 N/2$ pour des choix idoines de δ_9 et δ_{10} . De plus, si $x \in e$ et tous les sommets de e sont de degré $(1 \pm \delta)D$, alors comme $d(y, z) < \delta D$ pour tous y, z , le nombre d'hyperarêtes f ne contenant pas x et intersectant e est au plus $(r-1)(1+\delta)D$ et au moins $(r-1)(1-\delta)D - \binom{r-1}{2} \delta D$ et donc e satisfait (\star) .

Il nous suffit donc de montrer que pour presque tous les sommets x satisfaisant (A) et (B), $d'(x)$ satisfait la condition de (vi). Prenons un tel sommet x . Nous dirons qu'une hyperarête e contenant x est **bonne** si elle satisfait (\star) . Sachant que $x \in V'$, la probabilité qu'une bonne arête contenant x reste dans l'hypergraphe induit par V' est $(1-p)^{(1 \pm \delta_{11})(r-1)D}$. Ainsi l'espérance de $d'(x)$ vaut

$$\mathbf{E}(d'(x)) = (1 \pm \delta_{10} \pm \delta)D(1-p)^{(1 \pm \delta_{11})(r-1)D} \pm \delta_{10}D = e^{\epsilon(r-1)}D(1 \pm \delta_{12}).$$

Pour chaque hyperarête e contenant x , soit I_e la variable aléatoire qui vaut 1 si e est dans V' et 0 sinon. Ainsi le degré $d'(x) = \sum_{x \in e} I_e$. Ainsi

$$\begin{aligned} \mathbf{Var}(d'(x)) &\leq \mathbf{E}(d'(x)) + \sum_{e \ni x, f \ni x} \mathbf{Cov}(I_e, I_f) \\ &\leq \mathbf{E}(d'(x)) + 2\delta_{10}D^2(1 \pm \delta) + \sum_{e \ni x, f \ni x, e \text{ et } f \text{ bonnes}} \mathbf{Cov}(I_e, I_f). \end{aligned}$$

Il reste à borner $\Sigma^* = \sum_{e \ni x, f \ni x, e \text{ et } f \text{ bonnes}} \mathbf{Cov}(I_e, I_f)$. Pour chaque bonne hyperarête fixée e , la somme partielle qui lui correspond est de la forme $\sum_{f \ni x, f \text{ bonne}} \mathbf{Cov}(I_e, I_f)$. Il y a au plus $(r-1)\delta D$ hyperarêtes f dans cette somme qui intersectent e en un sommet autre que x , et leur contribution à la somme ne peut pas excéder $(r-1)\delta D$. Considérons maintenant un autre arête f , c'est-à-dire telle que $e \cap f = \{x\}$. Soit $t(e, f)$ le nombre d'arêtes ne contenant pas x qui intersectent à la fois e et f . Clairement, $t(e, f) \leq (r-1)^2 \delta D$. Il s'en suit que $\mathbf{Cov}(I_e, I_f) \leq (1-p)^{-t(e, f)} - 1 \leq \delta_{13}$. Ceci implique que pour toute bonne hyperarête e fixée,

$$\sum_{f \ni x, f \text{ bonne}} \mathbf{Cov}(I_e, I_f) \leq (r-1)\delta D + D(1+\delta)\delta_{13} \leq \delta_{14}D.$$

Comme Σ^* est la somme d'au plus $D(1+\delta)$ telles quantités, nous concluons que

$$\mathbf{Var}(d'(x)) \leq \mathbf{E}(d'(x)) + \delta_{15}D^2 \leq \delta_{16}(\mathbf{E}(d'(x)))^2.$$

Par l'Inégalité de Chebyshev, il vient qu'avec probabilité au plus δ_{17} , $d'(x)$, $d'(x)$ n'est pas dans $(1 \pm \delta_{18})De^{-\epsilon(r-1)}$. Par conséquent, l'Inégalité de Markov implique qu'avec probabilité au moins $0,9$, tous les sommets x sauf au plus $\delta_{19}n$ vérifient $d'(x) = (1 \pm \delta_{18})De^{-\epsilon(r-1)}$, c'est à dire que (vi) est satisfaite. \square

8 Le théorème de Keevash

Les résultats de Keevash portent sur les décompositions d'hypergraphes assez généraux (pseudo-almatoires) en des hypergraphes uniformes complets. Plutôt que de montrer ce résultat en toute généralité, nous allons nous restreindre à la décomposition en **triangles** (i.e. copies de K_3) d'un graphe ayant des propriétés adéquates.

Les propriétés adéquates sont les suivantes :

- (P1) le graphe doit être **tridivisible** : son nombre d'arêtes est divisible par 3 et les degrés des sommets doivent être pairs. (Ce sont les conditions nécessaires classiques).
- (P2) la densité d'arête doit être au moins une certaine constante δ .
- (P3) Le graphe doit être **typique**, c'est-à-dire avoir une propriété qu'ont les graphes aléatoires. Plus précisément il existe un entier c et un entier positif h tels que le nombre de voisins communs de tout ensemble d'au plus h sommets est au moins $1 - c$ et au plus $1 + c$ fois l'espérance de ce nombre de voisins dans un graphe aléatoire de même densité. (Attention, ceci est plus fort que d'être un graphe aléatoire ou pseudo-aléatoire : dans ce cas, seul la plupart des ensembles vérifient cette condition, et des déviations plus grandes sont autorisées.)

Théorème 38 (Keevash). *Un graphe ayant les propriétés (P1), (P2) et (P3) se décompose en triangles.*

Cette preuve se fait en quatre étapes :

1. D'abord, on met de côté une collection de triangles, appelés **spécimens**, qui seront utilisés à la fin.
2. Ensuite, on utilise le *Rödl nibble* pour couvrir par des triangles pratiquement toutes les arêtes non-spécimen. Les arêtes non-couvertes forme le **reste**.
3. On met les arêtes du reste dans des triangles en utilisant des arêtes des triangles spécimens. Ces dernières seraient donc utilisées deux fois si jamais on rajoutait les triangles spécimens. Elles forment le **surplus**, noté S .
4. On corrige les arêtes du reste en trouvant deux ensemble de triangles \mathcal{A} et \mathcal{B} , tels que $\bigcup_{A \in \mathcal{A}} E(A) \cup S = \bigcup_{B \in \mathcal{B}} E(B)$ et \mathcal{B} est un ensemble de triangles spécimens. On ajoute les triangles de \mathcal{A} et les triangles spécimens qui ne sont pas dans \mathcal{B} .

Donnons maintenant quelques détails sur chacune des quatre étapes.

Etape 1 : On plonge de manière aléatoire les n sommets du graphe dans un groupe abélien élémentaire d'ordre 2 (i.e. quelque chose de la forme $(\mathbb{Z}/2\mathbb{Z})^q$ pour un entier q) de taille entre deux et quatre fois n . Les spécimens sont alors les triangles $\{x, y, z\}$ pour lesquels $x + y + z = 0$ dans le groupe abélien.

Etape 2 : On utilise la version qui est décrite dans la Partie 7.

Etape 3 : Les arêtes du surplus S sont complétées en triangles à l'aide des arêtes des spécimens, en s'assurant que les paires d'arêtes utilisées soient disjointes. Ceci se fait à l'aide d'un algorithme glouton aléatoire. S'il n'y avait pas cette condition de disjonction, les choix pour compléter les arêtes en triangles seraient indépendants, et l'algorithme facile à analyser ; la version correcte est une perturbation plutôt faible de cela. Ainsi, on peut montrer que l'algorithme termine et qu'aucun sommet de gros degré n'est créé.

Etape 4 :

A l'aide de la typicité, on peut montrer qu'à l'étape précédente, en étant plus précautionneux, on peut choisir chaque nouveau triangle $\{x, y, z\}$ plongé dans un octaèdre dont les autres sommets sont $x + y$, $y + z$, et $z + x$ (dans le groupe abélien). Maintenant les huit faces se décomposent en deux groupes, l'un contenant $\{x, y, z\}$ et l'autre contenant des triangles tels que $\{x, y, x + y\}$ qui sont en fait des triangles spécimens.

9 Bestiaire

BIBD : balanced incomplete block design : (n, k, λ) -BIBD = 2- (n, k, λ) configuration = (n, k, λ) configuration.

9.1 Carrés latins

Definition 39. Un **carré latin d'ordre** q est un tableau à q lignes et q colonnes, telle que chaque ligne (resp. colonne) contient exactement un élément de $\{1, \dots, q\}$.

Il existe deux carrés latins d'ordre 2. Voir Figure 11.

Definition 40. Deux carrés latins $A = (a_{ij})_q$ et $B = (b_{ij})_q$ d'ordre q sont **orthogonaux** si $\{(a_{ij}, b_{ij}) \mid i \in [q], j \in [q]\} = [q] \times [q]$.

Des carrés latins sont **mutuellement orthogonaux** s'ils sont orthogonaux deux à deux.

1	2	2	1
2	1	1	2

FIGURE 11 – Les deux carrés latins d'ordre 2.

0	1	2	0	1	2	(0, 0)	(1, 1)	(2, 2)
1	2	0	2	0	1	(1, 2)	(2, 0)	(0, 1)
2	0	1	1	2	0	(2, 1)	(0, 2)	(1, 0)

FIGURE 12 – Deux carrés latins orthogonaux d'ordre 3 et le carré de leurs couples.

Definition 41. Un $m \times q$ -**tableau orthogonal** ou $OA(m, q)$ est un tableau (a_{ij}) á m lignes et q^2 colonnes tel que deux lignes distinctes i et i' sont **orthogonales** i.e $\{(a_{i,j}, a_{i',j}) \mid j \in [q^2]\} = [q] \times [q]$.

Exemple 42. Set $q = 3$ and $m = 4$.

0	0	0	1	1	1	2	2	2
0	1	2	0	1	2	0	1	2
0	1	2	1	2	0	2	0	1
0	1	2	2	0	1	1	2	0

Expliquer comment passer de carrés latins orthogonaux á tableau orthogonal.

Rapport avec les configurations. $m - 2$ carrés latin d'ordre q deux á deux orthogonaux est équivalent á partitionner $K_{m \times q}$ en K_m .

Soit A_1, \dots, A_m les stables de $K_{m \times q}$

$OA(3, q) =$ carré latin $= K_{q,q,q}$ en K_3 .

$OA(4, q)$, deux carrés latins d'ordre q orthogonaux correspondent á une décomposition de $K_{4 \times q}$ en K_4 .

9.2 Plans affines

Definition 43. Un **plan affine** est une paire d'ensembles de points et de droites tels que :

- (i) Par deux points passent une et une seule droite.
- (ii) Pour tout point p et toute droite D , il existe une unique droite paralléle á D (i.e. n'intersectant pas D) passant par p .
- (iii) Il existe trois points non colinéaires.

De manière similaire á la preuve de la Proposition 26, on peut montrer la proposition suivante.

Proposition 44. Soit A un plan affine fini. Il existe q , appelé **ordre** de A , tel que :

- Chaque droite contient exactement q points.
- Chaque point est dans exactement $q + 1$ droites.
- Il y a $q^2 + q$ droites et q^2 points.

La Proposition 44 implique que les plans affines sont des $(q^2, q, 1)$ configurations. On peut lá aussi montrer qu'il y'a bijection entre les plans affines et les $(q^2, q, 1)$ configurations.

On peut facilement voir que si on retire une droite et toutes les points qu'elle contient d'un plan projectif d'ordre q , on obtient un plan affine d'ordre q . A l'inverse, á partir d'un plan affine d'ordre q , on peut construire un plan projectif d'ordre q .

Proposition 45. Les deux assertions suivantes sont équivalentes.

- K_{q^2+q+1} se décompose en copies de K_{q+1} , i.e il existe un plan projectif d'ordre q .
- K_{q^2} se décompose en copies de K_q , i.e. il existe un plan affine d'ordre q .

Références

- [1] N. Alon, JH Kim et J. Spencer, *J. Isr. J. Math.* 100(1) : 171–187, 1997.
- [2] N. Alon et J. Spencer, *The Probabilistic Method*, 3rd edition, Wiley, 2008.
- [3] J-C. Bermond et D. Sotteau, (v, k, λ) -configurations, Polycopie du cours donné à U. Paris VI, 1972-1973
- [4] R.C. Bose et S.S. Shrikhande et E.T. Parker, Further results on the construction of sets of mutually orthogonal Latin squares and the falsity of Euler's conjecture , *Canadian J. Math.*, 12 : 189–203, 1960.
- [5] R. H. Bruck et H. J. Ryser, The nonexistence of certain finite projective planes, *Canadian J. Math.*, 1 : 88–93, 1949.
- [6] A. Cayley, On the triadic arrangements of seven and fifteen things, *Philosophical Magazine*, 37 : 50–53, 1850.
- [7] C.J. Colbourn et J.H. Dinitz (eds.), *Handbook of Combinatorial Designs, Second Edition*, Chapman & Hall/CRC, 2006.
- [8] F. W. Cole, Kirkman parades, *Bulletin of the American Mathematical Society*, 28 : 43–437, 1922.
- [9] P. Erdős et H. Hanani. On a limit theorem in combinatorial analysis, *Publ. Math. Debrecen*, 10 : 10–13, 1963.
- [10] R. A. Fisher et F. Yates, newblock The 6×6 latin squares, *Proc. Camb. Phil. Soc.*, 3 : 492–507, 1934.
- [11] P. Frankl and V. Rödl. Near perfect coverings in graphs and hypergraphs, *Europ. J. Combinatorics*, 6 : 317-326, 1985.
- [12] H. Hanani, On quadruple systems *Canad. J. Math.*, 12 : 145–157, 1960.
- [13] H. Hanani, Balanced incomplete block designs and related designs *Discrete Math.*, 11 : 255–369, 1975.
- [14] J. Kahn. Asymptotically good list colorings, *J. Combin. Theory, Ser. A*, 73 : 1–59, 1996.
- [15] T. P. Kirkman, On a Problem in Combinations, *The Cambridge and Dublin Mathematical Journal*, II : 19–204, 1847.
- [16] T. P. Kirkman, Query VI In *The Lady's and Gentleman's Diary* (pg.48), 1850.
- [17] C. W. H. Lam, L. Thiel, et S. Swiercz, The non-existence of finite projective planes of order 10, *Can. J. Math.*, XLI : 1117–1123, 1989.
- [18] P. Mulder, Kirkman-Systemen. *Groningen Dissertation*. Leiden, Netherlands, 1917.
- [19] N. Pippenger et J. H. Spencer. Asymptotic behaviour of the chromatic index for hypergraphs, *J. Combin. Theory, Ser. A*, 51 : 24–42, 1989.
- [20] D.K. Ray Chaudhuri et R.M. Wilson , Solution of Kirkman's s problem chooldgirl *Proc Symp. Pure Math. Amer. math Soc.* , 19 : 187–204, 1971.
- [21] M. Reiss, Ueber eine Steinersche combinatorische Aufgabe, welche im 45sten Bande dieses Journals, seite 181, gestellt worden ist, *J. Reine Angew. Math.*, 56 :326–344, 1859.
- [22] V. Rödl. On a packing and covering problem, *Eur. J. Combinatorics*, 6 : 69–78, 1985.
- [23] J. Steiner, Combinatorische Aufgabe, *Journal für die Reine und Angewandte Mathematik*, 45 : 181–182, 1853.
- [24] D.R. Stinson , *Combinatorial Designs Constructions and analysis*, Springer , 2006.
- [25] D.R. Stinson , A short proof of the non existence of orthogonal latin squares of order 6 *J. Combin. Theory, Ser. A*, 36 : 373–376, 1984.
- [26] G. Tarry, Le Problème de 36 Officiers, *Compte Rendu de l'Association Francaise pour l'Avancement de Science Naturel*, 2 : 170–203, 1901.
- [27] R.M. Wilson , An existence theory for pairwise balanced designs I Composition theorems and morphisms *J. Combin. Theory, Ser. A*, 13 : 220–245, 1972.
- [28] R.M. Wilson , An existence theory for pairwise balanced designs II the structure of PBD closed sets and the existence conjectures *J. Combin. Theory, Ser. A*, 13 : 246–273, 1972.
- [29] R.M. Wilson ,The necessary conditions for t-designs are sufficient for something *Utilitas Math.*, 4 : 207–215, 1973.
- [30] E. Witt, Über Steinersche Systeme, *Abh. Math. Sem. Univ. Hamburg*, 12 : 265– 275, 1938.