SET : la pêche à la ligne

Gabriel Pallier

Septembre 2016 *

Résumé

On expose diverses questions d'analyse combinatoire et de géométrie discrète soulevées par le jeu de cartes SET $^{\circledR}$ 1, très populaire aux Etats-Unis. Mathématiquement, le jeu est un système de triplets de Steiner avec une popriété de transitivité. Dans la version commerciale, cette structure est réalisée par un espace affine sur le corps fini \mathbb{F}_3 . Les SETs (combinaison de cartes qui se gagnent au cours du jeu) peuvent être vus comme des droites, ou bien des progressions arithmétiques. Il y a eu des progrès récents (mai 2016) assez spectaculaires sur des analogues en grande dimension, grâce à une méthode élémentaire dite polynomiale que nous reprendrons.

Table des matières

1	1 Principe du jeu					
2	La géométrie de SET	3				
3 Petite dimension						
4	La dimension quatre4.1 Plus grand jeu sans set	10				
5	Grande dimension	12				

^{*}Une version de cet article est parue dans le numéro 106 de Quadrature (octobre 2017) sous le titre Le jeu SET ou la pêche à la ligne.

^{1.} SET images © 1988, 1991 Cannei, LLC, tous droits réservés; SET® est une marque déposée de Cannei, LLC.

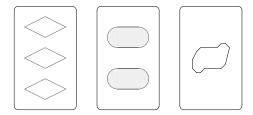


FIGURE 1 – Un SET (sans les couleurs).

6	Var	Variantes et généralisations					
	6.1	Classification des jeux de set	15				
	6.2	Planète	17				
	6.3	Questions non abordées	18				

1 Principe du jeu

Conçu par Marsha J. Falco en 1974, SET est un jeu de réflexion et de rapidité comportant 81 cartes. Chaque carte porte, sur l'une de ses faces, 1, 2 ou 3 motifs. Les motifs inscrits sur une carte sont d'une même couleur, d'une même forme et de même remplissage, sachant qu'il existe 3 couleurs, 3 formes et 3 types de remplissage (vide, hachuré ou rempli).

Au cours du jeu, un certain nombre de cartes sont retournées faces visible, et les joueurs doivent repérer parmi celles-ci un SET, c'est-à-dire 3 cartes telles que pour toute caractéristique donnée (couleur, forme du motif, remplissage du motif, nombre de motifs) ces cartes diffèrent toutes, ou coïncident toutes. En particulier, deux cartes quelconques étant données, il existe toujours une unique carte qui les complète en un SET. Quand un joueur a repéré un SET valide, il remporte les cartes correspondantes, qui sont remplacées par celles de la pioche. Un exemple est donné sur la figure 1.

Les règles du jeu recommandent de retourner 12 cartes à la fois, et l'on constate en pratique que c'est souvent suffisant pour garantir la présence d'un SET. Toutefois, il peut arriver qu'aucun n'apparaisse, auquel cas trois cartes sont rajoutées. Des questions que se posent de nombreux joueurs sont les suivantes :

- 1. A partir de quel nombre de cartes placées sur la table est-on certain de pouvoir trouver un *SET*?
- 2. Dans un jeu de n cartes typique, quelle est la probabilité de rencontrer un SET?
- 3. Dans un jeu de n cartes, combien trouve-t-on de SETs en moyenne?

+	-1	0	1	×	-1	0	1
-1	1	-1	0	-1	1	0	-1
0	-1	0	1	0	0	0	0
1	0	1	-1	1	-1	0	1

Tables d'addition et de multiplication dans \mathbb{F}_3 .

2 La géométrie de SET

Nous allons décrire une correspondance entre l'ensemble des cartes du jeu et un espace affine qui permet de traduire le jeu en termes géométriques. Signalons que cette construction est aussi expliquée en français par [11] avec un langage un peu moins technique. On désigne par $\mathbb{F}_3 = \{-1,0,1\}$ le corps à 3 éléments, et on rappelle les règles de calcul ayant cours dans \mathbb{F}_3 sur le tableau 1.

Proposition 1. Soit $f: \mathbb{F}_3 \to \mathbb{F}_3$ une application. S'équivalent

- i. f est constante ou une bijection.
- ii. f est affine.
- *iii.* f(-1) + f(0) + f(1) = 0.

 $D\acute{e}monstration$. On démontre $i \implies ii$; les autres implications sont laissées en exercice. Si f est constante, alors f est affine. D'autre part, $x \mapsto x-1$ est une permutation circulaire, et $x \mapsto -x$ une transposition (ainsi qu'on le constate par exemple sur la première ligne du tableau 1); donc 2 toutes les permutations de \mathbb{F}_3 sont affines.

Identifions l'ensemble des cartes du jeu à l'espace vectoriel $E = \mathbb{F}_3^4$ en faisant correspondre à chaque caractéristique (couleur, nombre de symboles, forme des symboles, style de remplissage) une coordonnée. Un triplet de cartes (x^{-1}, x^0, x^1) forme un SET si, et seulement si, $i \mapsto x_j^i$ est constante ou une permutation pour tout $j = 1 \dots 4$, autrement dit si $i \mapsto x^i$ paramétrise une droite affine. Le jeu consiste donc à repérer une droite affine (le SET) dans un sous-ensemble de \mathbb{F}_3^4 .

Remarque 1. L'équivalence $i \iff ii$ dans la proposition 1 est aussi valable pour le corps \mathbb{F}_2 . Toutefois le jeu de Set correspondant serait un peu trop facile pour être intéressant (tout couple de cartes y formerait un set).

^{2.} Il n'est pas vrai en général qu'un n-cycle et une transposition quelconques engendrent S_n . Cela dit, c'est vrai pour S_3 . On pourra utilement réfléchir au lien avec la règle dite de Sarrus qui permet le calcul du déterminant des matrices 3×3 .

d	n_d	$n_d^{1/d}$	Réference
2	4	2	
3	9	2.080	
4	20	2.115	Pellegrino 1971 [16]
5	45	2.141	Edel 2002 [8]
6	112	2.196	Potechin 2008 [17]
≥ 7	?	≤ 2.756	Ellenberg-Gijswijt 2016 [9]

TABLE 2 – Tailles connues des plus grands $X \subset \mathbb{F}_3^d$ sans droite affine.

On dira qu'un sous ensemble A d'un espace affine est un aset s'il ne contient aucune droite. La question 1 équivaut à la détermination du cardinal maximal d'un aset 3 de \mathbb{F}^4_3 . Sous cette forme, c'est un corollaire d'un théorème de Pellegrino [16] (1971) qui apporte la réponse : il existe dans \mathbb{F}^4_3 des asets à 20 points, aucun à 21 points (nous donnerons une preuve en section 4). Mieux, on connaît maintenant les cardinaux maximaux n_d des asets de \mathbb{F}^d_3 pour $d \leq 6$. Ils sont consignés dans le tableau 2 suivant (on les retrouve aussi sous l'étiquette A090245 sur OEIS).

La saveur affine du jeu, que nous venons de dévoiler, permet déjà quelques observations :

- 1. Si $A \subset \mathbb{F}_3^d$ est un aset, c'est aussi le cas de $A \cap W$ pour tout sous-espace affine W. Cette remarque a de l'importance quand on souhaite estimer n_d par récurrence sur la dimension, cf. les sections 3 et 4.
- 2. Le plus grand groupe qui opère sur \mathbb{F}_3^4 en envoyant droite sur droite (donc en préservant les asets), est le groupe affine $G = \mathrm{GA}(4,3)$. Les éléments de ce groupe sont complètement déterminés par leur effet sur un repère affine, c'est-à-dire une origine et 4 vecteurs linéairement indépendants; de plus, pour deux tels repères \mathcal{R} et \mathcal{R}' il existe $g \in G$ envoyant \mathcal{R} sur \mathcal{R}' (on dit que l'opération de G sur les repères est simplement transitive). Il y a donc autant d'éléments dans G que de repères affines, soit

$$N = 81 \cdot (81 - 1)(81 - 3)(81 - 9)(81 - 27)$$

= 1965150720.

A titre de comparaison, le groupe du Sudoku, qui opère sur le même espace, a pour cardinal seulement $2 \cdot 6^8 = 3359232$. Le groupe G permet, à partir d'un aset A, d'en déduire beaucoup ⁴ d'autres : les g(A) pour $g \in G$. On dira que A et A' sont congruents s'ils s'envoient l'un sur l'autre par une transformation affine.

^{3.} Attention, un aset peut être maximal pour la relation d'inclusion parmi les asets sans être de cardinal maximal. Dans la littérature en anglais, un aset est un *cap*, et une *calotte* pour Pellegrino.

^{4.} Ce "beaucoup" dépend du nombre de symétries que possède déjà A, selon la formule des classes. On y reviendra en section 4.

D'autre part, la structure vectorielle de \mathbb{F}_3^d (qui transparaît seulement dans la condition iii) permet de donner à la condition d'alignement une forme agréable : x, y, z distincts sont alignés si et seulement si

$$x + y + z = 0, (1)$$

autrement dit, si z = -x - y = (x+y)/2. On vérifie, par exemple à l'aide de la formule (1), qu'en toute dimension d l'ensemble $\{0,1\}^d$ constitue un aset; géométriquement, sa classe de congruence est formée des $\mathbb{F}_3^d \setminus (H_1 \cup \cdots \cup H_d)$, où les H_i sont des hyperplans affines d'intersection réduite à un point. Cet aset est maximal pour l'inclusion, ceci résulte de la reformulation suivante :

Lemme 1. Un aset $A \subset \mathbb{F}_3^d$ est maximal pour l'inclusion si et seulement si l'ensemble des droites passant par deux points distincts de A recouvre \mathbb{F}_3^d .

Cependant, ainsi que nous allons le voir, l'aset $\{0,1\}^d$ n'est de cardinal maximal que pour $d \leq 2$.

3 Petite dimension

Puisqu'une telle démarche est souvent instructive, on commence par l'étude des petites dimensions d=2,3.

Proposition 2. Le cardinal maximal d'un aset de \mathbb{F}_3^2 est 4.

Démonstration. Supposons par l'absurde que A est un aset de \mathbb{F}_3^2 à 5 éléments. Soient H_1, H_2, H_3 trois droites parallèles d'union \mathbb{F}_3^2 . Quitte à permuter les H_i on peut faire en sorte que

$$|A \cap H_1| = |A \cap H_2| = 2 \quad ; \quad |A \cap H_3| = 1 ;$$
 (2)

nous proposons à partir de là deux manières de conclure (la seconde, a priori moins directe, sert d'échauffement à ce qui va suivre).

- a. Quitte à noter $\{s_1\} = H_1 \setminus A$ et $\{s_2\} = H_2 \setminus A$ et D la droite qu'ils engendrent, $A \cap \{H_1 \cup H_2\}$ est égal à $\mathbb{F}_3^2 \setminus H_3 \cup D$. Posons $A' = A \cap \{H_1 \cup H_2\}$; par construction, A' est congruent à $\{0,1\}^2$, ce qui contredit la maximalité de ce dernier telle qu'elle nous est donnée par le lemme 1.
- b. Il y a 4 manières différentes de choisir la partition $\{H_1, H_2, H_3\}$ de \mathbb{F}_3^d , donc $8 = 2 \times 4$ façons de choisir les H_i de sorte que la répartition (2) est respectée. Mais il y a 10 paires de points distincts dans A et chaque paire $\{s,t\}$ donne lieu à un triplet (H_1, H_2, H_3) , où H_1 est la droite passant par s et t, ce qui est une contradiction car $8 \neq 10$.

Il y a une conséquence ludique :

Corollaire 1. Le jeu de morpion sur un tore donne une stratégie gagnante au premier joueur.

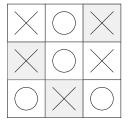


FIGURE 2 – Situation finale - les X gagnent. Une ligne est grisée (il y en a deux).

du corollaire. Supposons par l'absurde que le second joueur possède une stratégie lui permettant d'arriver à la partie nulle. Soit $\mathbb{F}_3^2 = \mathbf{X} \sqcup \mathbf{O}$ une position finale de cette stratégie, avec \mathbf{X} (resp. \mathbf{O}) l'ensemble des coups joués par le premier (resp. second) joueur. Alors $|\mathbf{X}| = 5$; donc d'après la proposition 2, il y a une droite contenue dans \mathbf{X} , soit un alignement gagnant (voir la figure 2).

Remarque 2. En fait, le jeu de morpion sur $(\mathbb{Z}/3\mathbb{Z})^2$ est terminé au plus tard au 7ème coup si le premier joueur suit une stratégie optimale⁵.

Pour une expérience du jeu en immersion complète, on pourra consulter la page de Jeffrey Weeks [21] qui en a fait un programme à vocation pédagogique.

Proposition 3. Les plus grands asets de \mathbb{F}_3^3 ont 9 éléments.

Avant de commencer la preuve, effectuons un rappel.

Lemme 2. Soit q une puissance d'un nombre premier, et V un espace vectoriel de dimension $d \ge 2$ sur le corps \mathbb{F}_q à q éléments. Alors

- i. Le nombre de droites vectorielles de V est $\frac{q^d-1}{q-1}$.
- ii. Par deux points distincts s et t dans V passent exactement $\frac{q^{d-1}-1}{q-1}$ 2-plans.

La démonstration de ce lemme est laissée au lecteur qui en aurait besoin.

de la proposition 3. La preuve qui suit est reprise de Maclagan 6 et Davis, [14, proposition 3]. Par l'absurde, soit A un aset de \mathbb{F}_3^3 à 10 points. D'après le point i du lemme 2, l'espace vectoriel 7 \mathbb{F}_3^3 compte $\frac{27-1}{2}=13$ droites vectorielles, donc autant de partitions en 3 plans

^{5.} Dans un sens, le jeu sur un tore est plus facile à analyser que le jeu classique, parce qu'il a plus de symétries : tout le groupe affine GA(2,3) qui est 3-transitif, de sorte que les 3 premiers coups d'une partie sont toujours essentiellement les mêmes.

^{6.} Les auteurs rapportent dans [14] une forte tradition du jeu parmi les doctorants de Berkeley dans les années 1990, à laquelle ils ont pris part.

^{7.} Plus exactement, son dual.

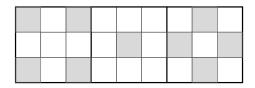


FIGURE 3 – Un aset de \mathbb{F}_3^4 à 9 éléments.

parallèles et disjoints $\{H_i\}$. On dit qu'une telle partition est de type $\{p_1, p_2, p_3\}$ si les p_i sont les cardinaux des asets de $A \cap H_i$. Puisqu'un aset de \mathbb{F}_3^2 a au plus 4 points, les partitions de A sont de type $\{3,3,4\}$ ou $\{2,4,4\}$; disons qu'il y en a x_{334} et x_{244} respectivement. Alors nous avons montré que

$$x_{334} + x_{244} = 13. (3)$$

D'autre part, d'après le rappel ii, toute paire de points distincts $\{s,t\} \subset A$ est contenue dans 4 deux-plans. Il y a donc exactement $4\binom{10}{2} = 180$ couples de la forme $(H,\{s,t\})$ avec H un plan et $\{s,t\} \subset H \cap A$. Mais ces couples se dénombrent également à partir des x_{334} et x_{244} :

$$\left[2\binom{3}{2} + \binom{4}{2}\right] x_{334} + \left[2\binom{4}{2} + 1\right] x_{244} = 180,$$

c'est-à-dire

$$12x_{334} + 13x_{244} = 180. (4)$$

Le système d'équations formé par (3) et (4) n'admet pas de solution en entiers naturels, puisque $13 \times (3) - (4)$ donne $x_{334} = -11$. Il reste à exhiber un aset à 9 points. Il y en a un sur la figure 3.

4 La dimension quatre

On entre ici dans le coeur du sujet, puisque l'espace \mathbb{F}_3^4 correspond exactement au jeu SET usuel. On apporte successivement des réponses aux questions 1, 2 et 3.

4.1 Plus grand jeu sans set

Dans [14, prop 5], Maclagan et Davis montrent que leur méthode de double comptage s'adapte (avec de l'ingéniosité) pour obtenir $n_4 = 20$. Nous présenterons ici une autre approche, celle de Bierbrauer et Edel [2] suivant une idée initiée par Meshulam [15]. Les espaces vectoriels \mathbb{F}_3^d sont aussi des groupes abéliens finis d'exposant 3 et à ce titre, on peut y développer une analyse de Fourier. On adoptera pour cela les notations suivantes : \mathbf{F} désigne \mathbb{F}_3^d , \mathbf{F}' son dual. j est le nombre complexe $e^{2\pi i/3}$; pour tout $\lambda \in \mathbf{F}$, l'écriture j^{λ}

fait sens car $3\lambda = 0$. Enfin, pour toute forme linéaire $\varphi \in \mathbf{F}'$, $\langle \varphi, x \rangle$ désigne l'évaluation de φ en x.

Définition 1. Soit $f: \mathbf{F} \to \mathbb{C}$ une fonction. On définit sa transformée de Fourier $\hat{f}: \mathbf{F}' \to \mathbb{C}$ par

$$\widehat{f}(\varphi) := \sum_{x \in \mathbb{F}_2^d} f(x) j^{\langle \varphi, x \rangle}.$$

Il existe aussi des formules d'inversion, de Parseval, de Poisson (cf. [18] pour un ouvrage complet consacré au sujet). On s'intéressera particulièrement, une partie $A \subset \mathbf{F}$ étant fixée, à la transformée de Fourier de la fonction caractéristique 1_A qui sera toujours désignée par τ . Remarquons que pour toute forme linéaire φ non nulle

$$\tau(\varphi) = |A \cap \{\varphi = 0\}| + |A \cap \{\varphi = 1\}|j$$

+
$$|A \cap \{\varphi = -1\}|j^2,$$
 (5)

tandis que $\tau(0) = |A|$. Ainsi, la seule connaissance des $\tau(\varphi)$ permet de reconstituer la répartition de A dans les partitions d'hyperplans parallèles $\{\varphi = c\}$. Par ailleurs la formule de Parseval s'écrit

$$\|\tau\|_2^2 = \sum_{\varphi \in \mathbf{F}'} |\tau(\varphi)|^2 = 3^d \|\mathbf{1}_A\|_2^2 = 3^d |A|.$$
 (6)

Il existe une jolie formule dénombrant les droites de A à partir de sa transformée de Fourier τ , démontrée par Bierbrauer et Edel dans ⁸ [2].

Proposition 4 (Bierbrauer, Edel [14, prop 6], [2, lem 2]). Soit ℓ le nombre de droites affines de A. Alors

$$|A| + 6\ell = 3^{-d} \sum_{\varphi} \tau^3(\varphi). \tag{7}$$

Démonstration. En vertu de (1), pour tout triplet $(x, y, z) \in A^3$, x+y+z=0 si et seulement si x=y=z ou bien x,y,z forment une ligne. Puisqu'il y a 3!=6 manières d'énumérer les éléments d'une droite dans \mathbf{F} ,

$$|A| + 6\ell = \left| \{ (x, y, z) \in A^3 : x + y + z = 0 \} \right|$$

$$= \sum_{(x, y, z) \in A^3} 3^{-d} \sum_{\varphi \in \mathbf{F}'} j^{\langle \varphi, x + y + z \rangle}$$

$$= 3^{-d} \sum_{\varphi \in \mathbf{F}'} \left(\sum_{(x, y, z) \in A^3} j^{\langle \varphi, x \rangle} \right)^3 = 3^{-d} \sum_{\varphi} \tau^3(\varphi),$$

où l'on utilise l'inversion dans la deuxième inégalité que $\sum_w j^{\langle \varphi, w \rangle} = 0$ si $\varphi \neq 0$ et 3^d si $\varphi = 0$.

^{8.} La formulation de Bierbrauer et Edel est un peu différente, parce que les auteurs font le choix de ne pas mentionner la transformée de Fourier.

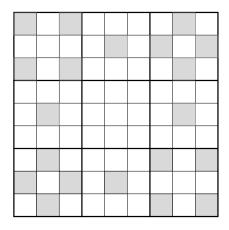


FIGURE 4 – Un aset de \mathbb{F}_3^4 à 20 points dessiné dans la grille de Sudoku.

Lemme 3. Supposons que A est un aset. Pour toute $\varphi \neq 0$ on a $|\tau(\varphi)| \leq 3n_{d-1} - |A|$.

Démonstration. Reprenons (5). Pour tout $\lambda \in \mathbb{F}_3$, $A \cap \{\varphi = \lambda\}$ est un aset dans l'hyperplan affine, donc $n_{d-1} - |A \cap \{\varphi = c\}|$ est un entier naturel. Il s'ensuit que

$$|\tau(\varphi)| \leqslant \sum_{\lambda \in \mathbb{F}_3} \left| (n_{d-1} - |A \cap \{\varphi = \lambda\}|) j^{\lambda} \right|$$

$$= 3n_{d-1} - |A|.$$

Théorème 1 (Bierbrauer, Edel [2, th 2]). Pour $d \ge 2$,

$$n_d \leqslant \frac{3n_{d-1} + 1}{1 + 3^{1-d}n_{d-1}}. (8)$$

Démonstration. Soit A un aset de cardinal maximal n_d . A ne contient aucune ligne, donc la proposition 4 donne

$$S := \sum_{\varphi \in \mathbf{F}' \setminus \{0\}} \tau^3(\varphi) = 3^d |A| - \tau^3(0)$$
$$= 3^d |A| - |A|^3. \tag{9}$$

Puisque $|A| \ge 2^d$, $|A|^3 > 3^d |A|$ et donc |S| = -S. D'autre part, le lemme 3 puis la formule de Parseval (6) donnent que

$$|S| \leq (3n_{d-1} - |A|) \sum_{\varphi \neq 0} |\tau(\varphi)|^{2}$$

$$= (3n_{d-1} - |A|) (||\tau||_{2}^{2} - |A|^{2})$$

$$\stackrel{(6)}{=} (3n_{d-1} - |A|) |A| (3^{d} - |A|). \tag{10}$$

Remplaçant |A| par n_d , la combinaison de (9) et (10) amène, après division par n_d , $n_d^2 - 3^d \le (3n_{d-1} - n_d)(3^d - n_d)$, d'où, en développant le membre de droite et en retranchant n_d^2 de chaque côté,

$$-3^{d} \leqslant 3^{d+1} n_{d-1} - 3^{d} n_{d} - 3n_{d-1} n_{d}. \tag{11}$$

De là,
$$1 \ge -3n_{d-1} + n_d + 3^{1-d}n_{d-1}n_d$$
 d'où l'on déduit (8).

Si l'on connaît la valeur de $n_1=2$, le théorème donne successivement $n_2<21/5$ (donc $n_2 \leq 4$), $n_3 \leq 9$ puis $n_4 \leq 21$. Finalement, on peut vérifier qu'il n'y a pas égalité dans l'inégalité du lemme 3 quand d=4, donc $n_4 \leq 20$. Il reste à exhiber un aset à 20 points, ce qui fait l'objet de la figure 4.

Remarque 3. Dans son travail de 1971, Pellegrino [16] s'intéressait surtout au problème analogue dans $\mathbf{P}^4\mathbb{F}_3$, mais la solution laisse un hyperplan projectif non occupé, donc on peut la regarder dans une carte affine, ce qui donne le dessin de la figure 4. L'aset de Pellegrino a été indépendamment redécouvert par de nombreux joueurs de SET assez persevérants. En dimension 5, le meilleur aset s'obtient également en retirant un hyperplan à la solution dans $\mathbf{P}^5\mathbb{F}_3$ (dûe à Hill en 1974), mais cette fois-ci 11 points sont perdus [8].

4.2 Combien de jeux sans SET?

En 2001, Donald Knuth s'est intéressé à SET, et a implémenté des compteur d'asets, disponibles en ligne [13]. Voici par exemple, quelques nombre d'asets déterminés par l'algorithme SETSET-ALL de Knuth.

Commentons ces résultats, dans le sens de la question 2 du début. Le groupe affine G tout entier est utilisé par l'algorithme de Knuth 9 . Le nombre de "cas" renvoyé par l'algorithme correspond au nombre d'asets modulo l'action de ce groupe, i.e. le nombre de classes de congruence d'asets dans notre terminologie.

^{9.} En fait, Knuth a écrit deux programmes, SETSET et SETSET-ALL, de conceptions un peu différentes. Nous référons ici à SETSET-ALL. Le programme SETSET, aussi disponible sur sa page utilise un sousgroupe de G.

asets à 3 points.

Le nombre d'asets de cardinal 3 est très proche du coefficient binomial $\binom{81}{3} = 85320$: la probabilité que 3 cartes prises au hasard forment un SET est faible. Géométriquement, cela correspond à la probabilité p qu'un triplet de 3 points distincts (X_1, X_2, X_3) pris au hasard uniforme dans \mathbb{F}_3^4 forme une droite;

$$p = \mathbb{P}[X_3 = -X_1 - X_2 \mid X_3 \notin \{X_1, X_2\}] = \frac{1}{79}.$$

On vérifie en effet que $\frac{84240}{85320}=\frac{78}{79}$; c'est la probabilité de l'évènement complémentaire " $\{X_1,X_2,X_3\}$ est un aset".

asets à 12 points.

Les asets à 12 points sont nettement plus difficiles à dénombrer. La seconde sortie de l'algorithme de Knuth, indispensable dans ce cas, nous indique qu'il y en a 2284535476080, ce qui représente environ 3.23~% des $\binom{81}{12}$ sous-ensembles de même taille. Ceci répond à la question 2: il y a environ une chance sur 31 de ne pas trouver de SET dans un jeu de 12 cartes posé sur la table. Au cours d'une vraie partie, cette probabilité est légèrement plus élevée, parce que l'on retire des sets régulièrement et que le jeu n'est pas complètement renouvelé (la question est étudiée en détail par [19] à l'aide de simulations). En présence de 15 cartes aléatoires, il est plus rare de rencontrer un aset : ceci arrive 1 fois sur 2740, d'après l'algorithme de Knuth.

asets à 19 ou 20 points.

Bien que l'algorithme de Knuth nous informe que les asets de cardinal 20 se déduisent tous l'un l'autre par transformation affines, leur nombre est bien inférieur à l'ordre de G. Ceux-ci doivent donc posséder un grand nombre de symétries. En effet, rappelons que d'après la formule des classes, quand un groupe H opère sur un ensemble \mathcal{X} (ici, on doit penser à \mathcal{X} comme à l'ensemble des asets), le cardinal de l'orbite d'un élément $A \in \mathcal{X}$ est donné par le quotient $|H|/|H_X|$, où $H_A = \{h \in H : h.A = A\}$ est le stabilisateur de A dans G. Spécifiquement, dans notre situation (si N désigne toujours l'ordre du groupe affine G),

$$N = 144 \cdot 13646880$$
$$= 2880 \cdot 682344,$$

ce qui indique via la formule des classes que les asets de cardinal 20 (resp. 19) admettent des groupes de symétries de cardinal 2880 (resp. 10 144).

On pourra vérifier à l'aide des données précédentes que le stabilisateur de l'aset de Pellegrino (celui de la figure 4) dans G opère simplement transitivement sur cet aset.

^{10.} Pour comparaison, les 2284535476080 asets de 12 cartes se répartissent en 1437 classes. Le rapport de ces deux nombres est proche de N, ce qui implique que leur groupe de symétries est le plus souvent trivial.

n	8	12	16	20	24
$\mathbb{E}[\ell]$	0.709	2.785	7.089	14.430	25.620

Table 3 – Nombre moyen de sets dans un jeu de n cartes.

4.3 Combien de SETs dans un jeu?

La question 3 se révèle finalement la moins ardue à traiter mathématiquement. Désignons par Δ l'ensemble des $40 \cdot 27 = 1080$ droites affines de \mathbb{F}_3^4 . Soit A un sous-ensemble aléatoire de \mathbb{F}_3^4 à n sommets. Par linéarité de l'espérance, si l'on désigne par ℓ la variable aléatoire correspondant au nombre de droites affines contenues dans A,

$$\mathbb{E}[\ell] = \sum_{\delta \in \Delta} \mathbb{P}(\delta \subset A). \tag{12}$$

Etant donnée l'invariance par transformation affine, les termes de la sommes sont égaux, donc si $\delta_0 \in \Delta$ est une droite quelconque,

$$\mathbb{E}[\ell] = |\Delta| \mathbb{P}(\delta_0 \subset A) = 1080 \cdot \frac{n(n-1)(n-2)}{81 \cdot 80 \cdot 79}$$
$$= \frac{n(n-1)(n-2)}{474}.$$

Pour fixer les idées, on a renseigné quelques valeurs de $\mathbb{E}[\ell]$ selon n dans le tableau 3. L'expression de $\mathbb{E}[\ell]$ se généralise sans mal au cas à d dimensions :

$$\mathbb{E}[\ell] = \frac{n(n-1)(n-2)}{6(3^d - 2)},\tag{13}$$

où l'on retrouve que $\mathbb{E}[\ell]$ s'exprime aussi comme une somme sur les triplets non ordonnés Θ de A de la probabilité que Θ forme une droite.

5 Grande dimension

Dans le tableau 2 de la section 2 nous avons inscrit les valeurs connues de $n_d^{1/d}$ pour d petit. Si A_1 (resp. A_2) est un aset de $\mathbb{F}_3^{d_1}$ (resp. de $\mathbb{F}_3^{d_2}$) alors $A_1 \times A_2 \subset \mathbb{F}_3^{d_1+d_2}$ est un aset à $|A_1||A_2|$ éléments. Il s'ensuit que

$$n_{d_1+d_2} \geqslant n_{d_1}n_{d_2}$$
.

En corollaire (par sous-additivité),

$$L := \limsup_{d} n_d^{1/d} = \sup_{d} n_d^{1/d} = \lim_{d} n_d^{1/d}.$$
 (14)

Inférieurement, nous savons que $L \geqslant 2.196$ grâce au résultat de Potechin ¹¹ sur les asets en dimension 6. La question de savoir si L=3 est restée ouverte jusqu'en mai 2016, quand Lev, Croot et Pach ont réalisé une percée [6] sur un problème proche concernant les progressions arithmétiques dans $(\mathbb{Z}/4\mathbb{Z})^n$. Quelques jours plus tard, Ellenberg et Gijswijt [9] ont pu expliquer comment adapter la méthode à un ensemble de situations dont relève SET. Nous allons reprendre ici le principe de leur preuve avec quelques allègements, sans chercher l'optimalité.

On commence par un lemme probabiliste qui nous rendra des services d'ordre combinatoire.

Lemme 4. Soient $X_1, \ldots X_d, \ldots$ une suite de variables aléatoires indépendantes uniformément distribuées dans $\{0,1,2\}$, et $(S_d)_{d\geqslant 1}$ leurs sommes partielles. Alors

$$\mathbb{P}\left(S_d \leqslant 2d/3\right) \leqslant c^d,$$

où c est une constante, $c \in]0,1[$.

Démonstration. Il s'agit d'un résultat de grande déviation. D'après l'inégalité de Hoeffding,

$$\mathbb{P}\left(S_d \leqslant 2d/3\right) = \mathbb{P}\left(S_d - \mathbb{E}(S_d) \leqslant -d/3\right)$$
$$\leqslant \exp\left(-\frac{2(d/3)^2}{4d}\right) = c^{-d},$$

avec $c = \exp(-1/18) \approx 0.946$.

Remarque 4. L'inégalité de Bienaymé-Tchebichev, plus classique, peut aussi être employée ici; cependant elle n'est pas assez forte pour prédire la décroissance exponentielle.

Soit n un entier naturel. On écrira $\mathbb{F}_3^n[t_1, \dots t_d]$ pour référer à l'espace des polynômes à d variables sur le corps \mathbb{F}_3 de degrés partiels ≤ 2 et de degré total inférieur ou égal à n. On désignera par $M_{(n,d)}$ l'ensemble de ses monômes, qui forme une base de cet espace.

Lemme 5. Soit $A \subseteq \mathbb{F}_3^d$. Supposons que $P \in \mathbb{F}_3^n[t_1, \dots t_d]$ est un polynôme tel que pour toute paire $\{a, b\}$ d'éléments distincts de A, P(a + b) = 0. Alors

$$|(-A) \cap \{P \neq 0\}| \leq 2 \dim \mathbb{F}_3^{\lfloor n/2 \rfloor}[t_1, \dots t_d]$$
 (15)

Démonstration. Soit $M=(m_{a,b})$ la matrice à coefficients dans \mathbb{F}_3 dont les lignes et colonnes sont indicées par A, et telle que $m_{a,b}=P(a+b)$. Par hypothèse, M est diagonale ; d'autre part, ses termes diagonaux sont les P(-c) pour $c \in A$. Il suffit donc de montrer que le rang de M est plus petit que le membre de droite dans (15). Pour cela, écrivons

$$P(x+y) = \sum_{i} \alpha_i u_i(x) v_i(y),$$

^{11.} En modifiant légèrement la construction du produit, Edel [7] obtient mieux : $L \ge 2.217$.

où les u_i et v_i sont des monômes. Dans chaque terme de la somme, soit u soit v est de degré total plus petit que $\lfloor n/2 \rfloor$. Donc P admet une décomposition (non unique)

$$P(x+y) = \sum_{u \in M_{(\lfloor n/2 \rfloor, d)}} u(x) F_u(y) + \sum_{v \in M_{(\lfloor n/2 \rfloor, d)}} v(y) G_v(x).$$

Mais alors $m_{a,b} = \sum u(a)F_u(b) + \sum v(b)G_v(a)$, donc M est somme d'au plus $2|M_{(\lfloor n/2\rfloor,d)}|$ matrices de rang au plus 1 (soit parce que toutes leurs lignes, ou bien toutes leur colonnes, sont colinéaires). Donc

$$\operatorname{rg}(M) \leqslant 2 \dim \mathbb{F}_3^{\lfloor n/2 \rfloor}[t_1, \dots t_d]$$

comme souhaité.

Avec ceci nous avons les moyens pour démontrer le

Théorème 2. L < 2.837.

Démonstration. Cette preuve suit dans les grandes lignes [9, th 4]. Soit A un aset de \mathbb{F}_3^d . On introduit les ensembles $B = (-A)^c$ et

$$C = A + A = \{a + b : (a, b) \in A^2, a \neq b\}.$$

Puisque A est un aset, $C \subseteq B$. Soit n un entier naturel, et V le sous-espace de $\mathbb{F}_3^n[t_1, \dots t_d]$ formé des polynômes qui sont nuls en restriction à B. Prenons $P \in V$ dont le support $\Sigma = \{P \neq 0\}$ est maximal parmi les éléments de V. Observons que $|\Sigma| \geqslant \dim V$: si ce n'était pas le cas, il existerait un polynôme Q dans V s'annulant sur Σ mais non identiquement nul; mais alors P + Q contredirait la maximalité de Σ . D'après le lemme 5,

$$\dim V \leqslant 2 \dim \mathbb{F}_3^{\lfloor n/2 \rfloor}[t_1, \dots t_d].$$

D'un autre côté, par définition de V, sa dimension est d'au moins dim $\mathbb{F}_3^n[t_1, \dots t_d] - |B| = \dim \mathbb{F}_3^n[t_1, \dots t_d] - 3^d + |A|$. De cet encadrement de dim V on déduit

$$|A| \leqslant \dim V + 3^d - \dim \mathbb{F}_3^n[t_1, \dots t_d]$$

$$\leqslant 2|M_{(\lfloor n/2\rfloor, d)}| + \left(3^d - |M_{(n,d)}|\right). \tag{16}$$

Suivant [9], remarquons que l'expression entre parenthèses est exactement le nombre de monômes en d variables de degrés partiels ≤ 2 et de degré total > n. Ceux-ci sont mis en bijection avec $M_{(2d-n-1,d)}$, par l'application $t_1^{\alpha_1} \cdots t_d^{\alpha^d} \mapsto t_1^{2-\alpha_1} \cdots t_d^{2-\alpha_d}$, donc nous pouvons réécrire (16) sous la forme

$$|A| \leq 2|M_{(\lfloor n/2\rfloor,d)}| + |M_{(2d-n-1,d)}|$$

$$\leq 2|M_{(\lfloor n/2\rfloor,d)}| + |M_{(2d-n,d)}|$$
(16')

On cherche finalement à optimiser (16'), c'est-à-dire à choisir n tel que le membre de droite soit le plus petit possible. Supposons $3 \mid d$, et prenons n = 2d/3. Le lemme probabiliste 4 nous informe, dans ce cas, que

$$2|M_{(d/3,d)}| + |M_{(2d-2d/3,d)}| = 3|M_{(d/3,d)}| \le 3(3c)^d.$$

Pour conclure, nous avons vu que $L = \lim_d n_d^{1/d}$; cette limite ne change pas quand on considère la suite extraite des d multiples de 3. Si c est la constante donnée par le lemme 4, alors 3c < 2.837, ce qui termine la preuve.

Remarque 5. Ellenberg et Gijswijt obtiennent L < 2.756 à l'aide du théorème de Cramér sur les grandes déviations, qui exprime la constante c comme une valeur de transformée de Legendre-Fenchel.

6 Variantes et généralisations

6.1 Classification des jeux de set

Peut-on construire d'autres jeux partageant les mêmes caractéristiques que SET? On a déjà vu que c'était possible en variant la dimension. Plus formellement, Davis et Maclagan proposent de capturer l'essence du jeu dans la définition suivante :

Définition 2 ([14]). Un jeu de set abstrait est la donnée d'un ensemble de cartes E et d'un ensemble de triplets non ordonnés $S \subset \mathcal{P}(E)$ tels que

- S1 E est fini.
- **S2** Toute paire d'éléments de E est contenue dans un unique $S \in \mathcal{S}$.
- **S3** Le groupe G des bijections φ de E respectant S (i.e. $\varphi(S) \in S$ pour tout $S \in S$) est deux fois transitif¹² sur E.

Les axiomes S1 et S2 seuls définissent la notion de système de triplets de Steiner (STS). L'axiome additionel S3 assure que tous les sets se déduisent l'un l'autre par des transformations de G. Davis et Maclagan observent que les espaces affines \mathbb{F}_3^d ne sont pas les seuls objets d'origine géométrique à correspondre à la définition 2 : c'est aussi le cas des espaces projectifs $\mathbf{P}^d\mathbb{F}_2$, avec pour S l'ensemble des droites projectives. Il est plus difficile, mais encore possible, d'en faire un jeu effectivement praticable et plaisant à l'aide de symboles permettant d'identifier visuellement les sets 13 (nous renvoyons à [14, p.17] pour une méthode particulièrement astucieuse avec $\mathbf{P}^5\mathbb{F}_2$, construisant un jeu de 63 cartes, attribuée à H.T. Hall). La classification des jeux de set abstraits s'appuie sur une théorie

^{12.} Ceci signifie que G opère transitivement sur les couples d'éléments distincts

^{13.} Bien entendu, une méthode est d'attribuer un symbole par set (comme dans le jeu de Dobble [10]). Cependant cela revient à privilégier la rapidité plus que la réflexion.

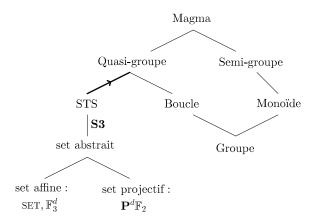


FIGURE 5 – Set et quelques cousins et cousines.

difficile, étrangère à l'auteur; elle a été menée à son terme au milieu des années 1980 et l'on sait à présent que tout jeu de set abstrait est affine ou projectif, i.e. isomorphe à \mathbb{F}_3^d ou $\mathbf{P}^d\mathbb{F}_2$ pour un entier naturel d. Les plus petits STS qui ne vérifient pas **S3** ont 13 éléments [1, p.637], et l'on peut montrer qu'il existe un système de triplets de Steiner d'ordre n si et seulement si $n \equiv 1$ ou 3 modulo 6. Il existe une loi de composition interne naturelle sur un système de triplet de Steiner (E, \mathcal{S}) :

Définition 3. Soit F = (E, S) un système de triplets de Steiner. Pour tout $(x, y) \in E$, on pose $x \star y = z$ si $x \neq y$ et $\{x, y, z\} \in S$, et $x \star y = x$ si x = y. La loi \star fait de F un quasigroupe, c'est-à-dire un magma où tous les éléments sont réguliers à droite et à gauche (cf. Bourbaki [4, § 3, ex. 6]).

Sur \mathbb{F}_3^4 , la loi de quasigroupe associée au jeu de SET usuel est décrite à partir de la structure vectorielle par $x \star y = (x+y)/2$ (cette construction s'applique à tout espace vectoriel de caractéristique $\neq 2$). Curieusement, il existe une autre strucure de quasi-groupe sur \mathbb{F}_3^4 , découverte par H. Zassenhaus :

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \blacklozenge \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \\ x_4 + y_4 + x \diamondsuit y \end{pmatrix},$$

avec $x \diamondsuit y = (x_3 - y_3)(x_1y_2 - x_2y_1)$. Cette loi possède en plus une forme d'associativité faible qui en fait une boucle de Moufang. Au sujet des quasi-groupes et des boucles nous renvoyons à Wikipédia en anglais [22, 23], qui est très détaillé concernant ces strucures un peu à l'écart de la hiérarchie classique mais dignes d'intérêt. On a résumé les informations de cette sous-section sur la figure 5.

Sur la figure 5, remonter dans le graphe revient à oublier de la structure. Par exemple, la flèche épaisse correspond à la construction de la définition 3, qui revient à regarder un STS comme un quasi-groupe. On vérifie que si φ est un morphisme entre les quasi-groupes sous-jacents à des systèmes de triplets de Steiner F et F', alors φ envoie chaque set de F sur un point ou un set de F'; autrement dit φ est un morphisme de STS. Dans les termes abstraits de la théorie des catégories [3], on dirait que le foncteur d'oubli STS \to Quasi - groupe donné par la définition 3 est plein. On pourra chercher d'autres foncteurs pleins sur la figure 5.

6.2 Planète

Nous décrivons ici une variante de SET qui se pratique avec le paquet usuel. Cette variante (à quelque nuances près) à été proposée indépendamment par de nombreuses personnes. Nous reprendrons le vocabulaire de Jalinière [11], qui est très judicieux. Le principe consiste à élargir l'enjeu – on ne recherche plus simplement des SETs, mais également des planètes, c'est-à-dire des ensembles de 4 points coplanaires. Les planètes gravitent sur deux orbites de l'action du groupe G:

- A Celles formées par un SET et un point extérieur.
- B Celles formées par la réunion de deux *SETs* concourants, diminuée de leur point d'intersection.

Les deux types de planètes sont dessinés sur la figure 6, dans le plan qu'elles engendrent.

Proposition 5. Dans un ensemble de 10 cartes, il y a toujours au moins une planète (de manière équivalente, un SET ou une planète de type B).

 $D\acute{e}monstration$. Soit $B \subset \mathbb{F}_3^4$ un ensemble à 10 éléments. La fonction qui aux couples (b_1, b_2) d'éléments distincts associe le vecteur $b_1\vec{b}_2$ ne peut être injective, car la source possède 90 éléments, et le but 81. Il existe donc (b_1, b_2) et (b'_1, b'_2) tels que

$$b_1\vec{b}_2 = b_1'\vec{b}_2'$$

Si $\{b_1, b_2\} \cap \{b'_1, b'_2\} = \emptyset$, alors b_1, b'_1, b_2, b'_2 forment une planète de type B. Sinon, ces éléments forment un SET S, et quitte a choisir $c \in B \setminus S$, $S \cup \{c\}$ est une planète de type A. \square

A	
A	A
A	

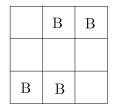


FIGURE 6 – Planète de type A et B.

Les planètes ne sont donc pas rares, mais il est sensiblement plus difficile de repérer une planète de type B à l'oeil nu qu'un SET. Pour rétribuer cette difficulté, on introduit la règle additionnelle suivante :

Variante Planète Si un joueur repère une planète de type B, il l'annonce, et remporte alors toutes les cartes présentes sur la table qui sont dans le plan affine engendré par cette planète 14 .

Ainsi, une planète de type B rapporte entre 4 et 9 cartes, ce qui est toujours plus qu'un SET.

Définition 4. Un extraterrestre ¹⁵ (E.T.) est la donnée de 9 cartes ne possédant aucune planète.

Les E.Ts sont très rares [20], même si le cours du jeu tend à favoriser leur apparition (on retire des *SETs* et des planètes), et il est très difficile d'en repérer dans les conditions réelles du jeu. C'est pourquoi on propose la variante suivante, plutôt destinée aux joueurs de SET professionnels.

Variante E.T. On joue avec au minimum 15 cartes; les règles de la variante Planète s'appliquent. De plus, si un joueur repère un E.T., il l'annonce. Les autres joueurs sont alors chargés de vérifier qu'il s'agit bien d'un E.T.

- a. Si, au cours de cette vérification, une erreur est repérée par un joueur (l'E.T. proposé possède en fait un SET ou une planète de type B), ce joueur remporte le SET ou la planète en question.
- b. Sinon, toutes les cartes sur la table reviennent au joueur qui a repéré l'E.T.

La variante Planète peut aussi se jouer avec le paquet de set projectif de Hall (cf. 6.1). Par contre la détection des planètes de type B y est moins rentable, et il n'y a pas d'E.T. dans $\mathbf{P}^5\mathbb{F}_2$ (on pourra le vérifier en exercice).

6.3 Questions non abordées

Dans l'analyse qui précède, on a laissé de côté de nombreuses questions également naturelles. En voici quelques-unes :

- 4. Combien de pièces au minimum doit compter une partition de \mathbb{F}_3^4 en asets? Autrement dit, combien de paquets sans SET peut-on former au minimum avec le jeu complet?
- 5. Soit $p \leq 4$. Dans \mathbb{F}_3^d , quel est le cardinal maximal d'une partie sans p-plan affine?

^{14.} Cette étape est assez rapide et ne ralentit pas trop le jeu, même pour des débutants : il suffit de tester la présence de 5 sets dans le jeu.

^{15.} notre définition est plus restrictive que celle de [11].

6. Quel est le cardinal minimal d'un aset maximal pour l'inclusion?

Il semble que les techniques employées ici ne suffisent pas à répondre entièrement à ces questions.

Remerciements

Je remercie Anne-Elisabeth Falq, qui m'a appris à jouer (et contre qui je n'ai jamais gagné), ainsi que les deux rapporteurs de cet article, qui m'ont aidé à l'améliorer de manière décisive, notamment en y détectant des erreurs. Enfin, Eva Philippe m'a permis d'apporter les ultimes corrections par sa relecture attentive.

Références

- [1] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, 1st edition, 1985.
- [2] J. Bierbrauer et Y. Edel. Bounds on affine caps. *Journal of Combinatorial Designs*, **10** (2):111–115, 2002.
- [3] E. Biland, Le langage des catégories I, Quadrature 87: 38-44, 2013.
- [4] N. Bourbaki, Algèbre, chapitre 1, Masson, 1970.
- [5] B. Conrey, B. Donaldson, SET, http://www.mathteacherscircle.org./assets/session-materials/BConreyBDonaldsonSET.pdf, Mots-clés: Conrey Donaldson set.
- [6] E. Croot, V. Lev et P. Pach, Progression-free sets in \mathbb{Z}_4^n are exponentially small, arXiv:1605.01506v2, 2016.
- [7] Y. Edel, Extensions of generalized product caps, *Designs, Codes and Cryptography*, **31** (1), 5 14, 2004.
- [8] Y. Edel, S. Ferret, I. Landjev, et L. Storme. The classification of the largest caps in AG(5, 3). *Journal of Combinatorial Theory, Series A*, **99** (1):95-110, 2002.
- [9] J. S. Ellenberg, D. Gijswijt On large subsets of \mathbb{F}_q^n with no three-term arithmetic progression, Annals of math, 185 (1):339-343, 2017.
- [10] M. Hézard, D. Hézard, Jouons un peu ... à Dobble! Quadrature 87:21-29, 2013.
- [11] P. Jalinière, Le jeu Set, http://images.math.cnrs.fr/Le-jeu-Set.html, 2013 (CNRS), Mots-clés: image math set Jalinière.
- [12] E. Klarreich, Set proof stuns mathematicians, Quanta magazine https://www.quantamagazine.org/set-proof-stuns-mathematicians-20160531/ mai 2016.
- [13] D. Knuth, http://www-cs-faculty.stanford.edu/~uno/programs/setset-all.w, 2001, En ligne, consulté le 19-Sept-2016, Mots-clés: Knuth setset-all.

- [14] B. Lent Davis et D. Maclagan. The card game set. *The Mathematical Intelligencer*, **25** (3):33–40, 2003.
- [15] R. Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. *Journal of Combinatorial Theory, Series A*, **71** (1):168 172, 1995.
- [16] G. Pellegrino, Sul massimo ordine delle calotte in S4, *Matematiche* (Catania), **25** (1970),1-9.
- [17] A. Potechin. Maximal caps in AG(6,3). Designs, Codes and Cryptography, 46 (3):243–259, 2008.
- [18] G. Peyré. L'algèbre discrète de la transformée de Fourier. Ellipses, 2004.
- [19] H. Warnes, SET probabilities revisited https://henrikwarne.com/2011/09/30/set-probabilities-revisited/ Mots-clés: Henrik Warnes set probabilities
- [20] H. Warnes, SET Card Game Variation https://henrikwarne.com/2013/04/07/ set-card-game-variation-complementary-pairs/ Mots-clés: Henrik Warnes set variation
- [21] J. Weeks. Torus games. http://www.geometrygames.org/TorusGames/index.html.

 Mots-clés: Jeff Weeks
- [22] Wikipedia, Quasigroup, https://en.wikipedia.org/wiki/Quasigroup
- [23] Wikipedia, Moufang loop, https://en.wikipedia.org/wiki/Moufang_loop