

Jouons un peu... ... à DOBBLE !

par Marie et David HÉZARD*

Résumé.

Dans cet article, nous nous intéressons au jeu DOBBLE. Après en avoir présenté le principe, nous ferons, dans un premier temps, des raisonnements de combinatoire élémentaires sur le jeu, puis nous parlerons de jeu optimal en utilisant des résultats de base d'arithmétique (identité de BÉZOUT) sur les corps finis de cardinal premier.

Dans un deuxième temps, nous parlerons des plans projectifs finis (qui sont autant de jeux DOBBLE !), qui nous permettront de construire explicitement des jeux DOBBLE optimaux.

I Règles du jeu DOBBLE

Commençons par préciser les règles du jeu DOBBLE¹.

Le jeu est constitué de 55 cartes : sur chaque carte, 8 symboles 2 à 2 différents. La particularité de ces cartes est que 2 cartes prises au hasard ont exactement un symbole en commun.

Chaque joueur dispose d'une pile de cartes et au milieu de la table se trouve une autre carte. Il faut être le premier à trouver l'unique symbole commun entre sa propre carte visible et celle du milieu.

On se pose ici les questions suivantes : combien de symboles au minimum doit-on avoir pour créer le jeu ? Quel est alors le cas optimal (c'est-à-dire qui maximise le nombre de cartes, le nombre de symboles étant donné) ? Peut-on alors décrire un algorithme permettant de construire un tel jeu ?

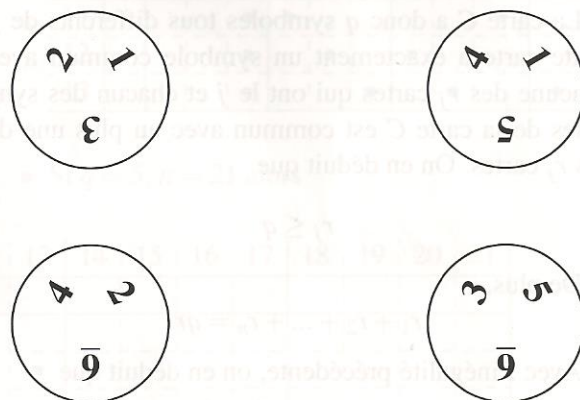
II Modélisation

Nous noterons ici les symboles 1, 2, 3, ... et nous supposons qu'il y en a n ($n = 57$ dans le jeu). Nous noterons r le nombre de cartes ($r = 55$ dans le jeu) et q le nombre de symboles 2 à 2 différents sur chaque carte ($q = 8$ dans le jeu).

Ainsi, si $n = 6$ et $q = 3$, on peut construire le jeu suivant, avec $r = 4$ cartes :

* Professeurs au Lycée DESCARTES de TOURS.

1. Jeu édité par ASMODÉE et PLAY FACTORY



A n et q fixés, on va déterminer quel est le plus gros jeu de cartes qu'on peut construire (c'est-à-dire on cherche r maximal).

Pour modéliser un jeu de telles cartes, on peut utiliser un tableau à n colonnes et r lignes tel que sur la ligne i , on place un • dans la j -ième colonne si le symbole j est présent sur la carte i . Sinon, on laisse la case vide.

Dans l'exemple précédent, on obtient le tableau :

•	•	•			
•			•	•	
	•		•		•
		•		•	•

Les questions se reformulent de la façon suivante : si on se donne le nombre de colonnes (c'est-à-dire n) et le nombre de cases non vides sur chaque ligne (c'est-

à-dire q), quel est le nombre maximal r de lignes que peut avoir un tableau avec les contraintes voulues ?

III Toutes les cartes ont un même symbole en commun

Ce cas n'a aucun intérêt d'un point de vue ludique mais examinons-le.

Notons par exemple 1 le symbole qui est commun à chaque carte. Alors, chaque carte a $q-1$ symboles qui ne sont présents sur aucune autre carte. Le nombre total de symboles est donc $n = 1 + r(q-1)$. Ainsi, si n et q sont fixés, alors le nombre maximal de cartes est $r = E\left(\frac{n-1}{q-1}\right)$.

IV Aucun symbole n'est présent sur toutes les cartes

IV.1 Quelques majorations

Soit $j \in \llbracket 1, n \rrbracket$. On note r_j le nombre de cartes qui contiennent le symbole j . Il existe donc au moins une carte C ne contenant pas le j .

La carte C a donc q symboles tous différents de j . Cette carte a exactement un symbole commun avec chacune des r_j cartes qui ont le j et chacun des symboles de la carte C est commun avec au plus une de ces r_j cartes. On en déduit que

$$r_j \leq q$$

De plus,

$$r_1 + r_2 + \dots + r_n = qr$$

Avec l'inégalité précédente, on en déduit que

$$r \leq n \quad (1)$$

Par ailleurs, quitte à renommer les symboles, on peut supposer qu'une carte C a exactement les symboles $1, 2, \dots, q$. Soit E_j l'ensemble des cartes ayant le symbole j . Comme toute carte a exactement un symbole en commun avec cette carte, on a $\text{Card}(E_1 \cup E_2 \cup \dots \cup E_q) = r$. De plus, comme C est l'unique carte appartenant à l'intersection de deux quelconques des E_j , on a :

$$\text{Card}(E_1 \cup E_2 \cup \dots \cup E_q) = r_1 + \dots + r_q + 1 - q$$

On en déduit une seconde inégalité :

$$r \leq q^2 - q + 1 \quad (2)$$

Enfin, si $j \in \llbracket 1, n \rrbracket$, on a :

$$r_j \leq E\left(\frac{n-1}{q-1}\right) \quad (3)$$

En effet, chacune des r_j cartes ayant le symbole j a d'une part le symbole j et $q-1$ autres symboles qui ne sont pas sur les autres r_j-1 cartes ayant le j . Sur l'ensemble des r_j cartes ayant le symbole j , on utilise donc $r_j(q-1) + 1$ symboles d'où : $r_j(q-1) \leq n-1$.

IV.2 Peut-on avoir $r = n$?

Supposons qu'on ait $r = n$. Alors, on a nécessairement, pour tout $j \in \llbracket 1, n \rrbracket$, $r_j = q$ et la formule du crible utilisée précédemment donne alors $n = r = q^2 - q + 1$.

Dans ce cas, nous allons essayer de créer un jeu avec $r = n$ cartes (qui est donc optimal d'après (1)). On procède de la façon suivante :

- On place $1, 2, \dots, q$ sur la première carte.
- On place $1, q+1, q+2, \dots, 2q-1$ sur la seconde carte.
- ...
- On place $1, k(q-1)+2, k(q-1)+3, \dots, k(q-1)+q$ sur la $k+1$ -ième carte où $k \in \llbracket 0, q-1 \rrbracket$.

On a ainsi défini les q premières cartes, ce qui donne sur les q premières lignes du tableau carré de taille n (pour $q=4, r=n=13$) :

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	•	•	•	•									
2	•				•	•	•						
3	•							•	•	•			
4	•										•	•	•

- Sur les $q-1$ cartes suivantes (cartes numérotées de $q+1$ à $2q-1$), on place le symbole 2,
- Sur les $q-1$ cartes suivantes, on place le symbole 3,
- ...
- Sur les $q-1$ dernières cartes, on place le symbole q .

Cela donne, sur le tableau :

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	•	•	•	•									
2	•				•	•	•						
3	•							•	•	•			
4	•										•	•	•
5		•											
6		•											
7		•											
8			•										
9			•										
10			•										
11				•									
12				•									
13				•									

Reste un sous tableau carré, que l'on appellera le sous tableau bordant, de taille $q^2 - 2q + 1 = (q-1)^2$ que l'on peut découper en blocs carrés de taille $q-1$: il y a $q-1$ tels blocs en ligne et en colonne (ces blocs sont marqués en pointillés sur les exemples).

Les blocs placés en première colonne sont tous identiques et sont diagonaux. Lorsqu'on décrit les blocs de la première ligne de blocs, on part du premier bloc et on décale tous les • de 0 case. Lorsqu'on décrit les blocs de la deuxième ligne de blocs, on part du premier bloc et on décale tous les • de 1 case (modulo $q-1$). Lorsqu'on décrit les blocs de la troisième ligne de blocs, on part du premier bloc et on décale tous les • de 2 cases (modulo $q-1$). Lorsqu'on décrit les blocs de la i -ème ligne de blocs, on part du premier bloc et on décale tous les • de $i-1$ cases (modulo $q-1$), pour i variant entre 1 et $q-1$.

Pour certains exemples, on obtient :

- Si $q = 2, n = 3$ alors

	1	2	3
1	•	•	
2	•		•
3		•	•

- Si $q = 3, n = 7$ alors

	1	2	3	4	5	6	7
1	•	•	•				
2	•			•	•		
3	•					•	•
4		•		•		•	
5		•			•		•
6			•	•		•	•
7			•		•	•	

- Si $q = 4, n = 13$ alors

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	•	•	•	•									
2	•				•	•	•						
3	•							•	•	•			
4	•										•	•	•
5		•			•			•			•		
6		•				•			•			•	
7		•					•			•			•
8			•		•			•				•	
9			•			•			•		•		
10			•				•			•		•	
11				•	•					•		•	
12				•		•		•					•
13				•			•		•		•		

- Si $q = 5, n = 21$ alors

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	•	•	•	•	•																
2	•					•	•	•	•												
3	•									•	•	•	•								
4	•													•	•	•	•				
5	•																	•	•	•	•
6		•				•				•				•				•			
7		•					•				•				•				•		
8		•						•				•				•				•	
9		•							•				•				•				•
10			•			•					•					•				•	
11			•				•					•					•				•
12			•					•					•					•			
13			•						•					•					•		
14				•		•					•			•					•		
15				•			•					•			•					•	
16				•				•					•			•					•
17				•					•					•			•				
18					•	•					•				•				•		
19					•		•					•				•				•	
20					•			•					•				•				•
21					•				•					•				•			

On constate que la méthode ne fonctionne pas pour $q = 5$: par exemple, les cartes 6 et 14 ont les symboles 6 et 14 en commun, ce qui est contradictoire avec ce que l'on voulait. Nous allons voir que le problème vient du fait que $q - 1$ est non premier.

IV.3 Cas où $q - 1$ est premier

Montrons que, dans ce cas, notre construction nous donne un jeu correct.

Soient deux cartes du jeu, il faut montrer qu'elles ont un et un seul symbole en commun. Si, au moins l'une des deux cartes est une carte dont le numéro est compris entre 1 et q , cela est clair. Étudions donc le cas où les deux cartes appartiennent au sous tableau bordant.

1. Cas où les deux cartes appartiennent à la même ligne i de blocs du sous tableau bordant, l'une des cartes étant la a -ème et la deuxième la b -ème du bloc avec $1 \leq a < b \leq q - 1$.

Alors ces deux cartes ont un et un seul symbole en commun dont le numéro est compris entre 1 et q : c'est $i + 1$.

Dire qu'ils ont un symbole en commun dont le numéro est strictement supérieur à q , signifie qu'il existe $k \in \llbracket 0, q - 2 \rrbracket$ tel que $a + k(i - 1) \equiv b + k(i - 1) \pmod{q - 1}$, soit $a \equiv b \pmod{q - 1}$ avec $1 \leq a < b \leq q - 1$, ce qui est absurde.

2. Cas où les deux cartes n'appartiennent pas à la même ligne de blocs du sous tableau bordant. La première carte est la a -ème de la i -ème ligne de blocs et la deuxième est la b -ème de la j -ème ligne de blocs avec $1 \leq a, b \leq q - 1$ et $1 \leq j < i \leq q - 1$.

Alors ces deux cartes n'ont pas de symbole en commun dont le numéro est compris entre 1 et q .

Dire qu'ils ont un symbole en commun dont le numéro est strictement supérieur à q , signifie qu'il existe $k \in \llbracket 0, q - 2 \rrbracket$ tel que $a + k(i - 1) \equiv b + k(j - 1) \pmod{q - 1}$, soit $k(i - j) \equiv b - a \pmod{q - 1}$. Or $i - j \in \llbracket 1, q - 2 \rrbracket$. Comme $q - 1$ est premier, $i - j$ est premier avec $q - 1$ et donc inversible dans $\mathbb{Z}/(q - 1)\mathbb{Z}$, et admet un unique inverse dans le corps $\mathbb{Z}/(q - 1)\mathbb{Z}$, qui admet un unique représentant k dans $\llbracket 0, q - 2 \rrbracket$. Ainsi les deux cartes n'ont qu'un seul symbole en commun dont le numéro est strictement supérieur à q .

On en conclut que les deux cartes n'ont qu'un seul symbole en commun.

Ainsi le jeu est correctement construit.

IV.4 Cas où $q - 1$ est composé

Remarquons que notre raisonnement ne tient plus car nous avons utilisé précédemment la primalité de $q - 1$.

Replaçons dans le même contexte et dans le cas $q = 5$, on a l'équation : $k(i - j) \equiv b - a \pmod{4}$ d'inconnue $k \in \llbracket 0, q - 2 \rrbracket$. Nous n'avons pas unicité de la solution k si $i - j$ n'est pas inversible dans $\mathbb{Z}/4\mathbb{Z}$, c'est-à-dire si $i - j$ n'est pas premier avec 4, les couples de lignes de blocs du sous tableau bordant posant problème sont (3, 1) et (4, 2), l'équation est alors $2k = b - a \pmod{4}$. Par exemple, si $b = a$ alors, il y a deux solutions $k = 0$ et $k = 2$ donc deux symboles en commun, c'est le cas des cartes 14 (première carte de la ligne 3 de blocs) et 6 (première carte de la ligne 1 de blocs). En revanche, si $a = 1$ et $b = 2$ alors il n'y a pas de solution donc aucun symbole en commun, c'est le cas des cartes 14 (première carte de la ligne 3 de blocs) et 7 (deuxième carte de la ligne 1 de blocs).

Dans le cas général $q - 1$ non premier, on montre de même que notre construction ne fonctionne pas. Soit $d \in \llbracket 2, q - 2 \rrbracket$ un diviseur de $q - 1$, on pose alors $i = d + 1 \in \llbracket 3, q - 1 \rrbracket$ et $j = 1 \in \llbracket 0, q - 2 \rrbracket$. Prenons la première ($a = 1$) carte de la ligne i de blocs et la deuxième ($b = 2$) de la ligne j de blocs.

Alors ces deux cartes n'ont pas de symbole en commun dont le numéro est compris entre 1 et q ($i \neq j$).

Dire qu'ils ont un symbole en commun dont le numéro est strictement supérieur à q , signifie qu'il existe $k \in \llbracket 0, q - 2 \rrbracket$ tel que $1 + k(i - 1) \equiv 2 + k(j - 1) \pmod{q - 1}$, soit $kd \equiv 1 \pmod{q - 1}$. Or d n'est pas inversible dans $\mathbb{Z}/(q - 1)\mathbb{Z}$ donc l'équation n'a aucune solution. On en conclut que les deux cartes n'ont aucun symbole en commun.

Ainsi, la construction est fautive si $q - 1$ n'est pas premier.

IV.5 Cas où $q = 5$ soit $q - 1 = 4$

Voici la construction d'un jeu optimal obtenu par une construction différente de la précédente.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	•	•	•	•	•																
2	•					•	•	•	•												
3	•									•	•	•	•								
4	•													•	•	•	•				
5	•																	•	•	•	•
6		•				•				•				•				•			
7		•					•				•				•				•		
8		•						•				•				•				•	
9		•							•				•				•				•
10			•			•					•					•					•
11			•				•			•							•			•	
12			•					•				•		•					•		
13			•						•				•			•			•		
14				•		•						•					•		•		
15				•			•						•			•		•			
16				•				•		•					•			•			•
17				•					•		•			•					•		
18					•	•						•			•					•	
19					•		•				•			•						•	
20					•			•			•				•			•			•
21					•				•	•					•				•		

V Retour sur DOBBLE

Dans le jeu, on connaît $r = 55$ et $q = 8$. Combien de symboles ont au minimum été nécessaires pour construire le jeu ? On est certain qu'il y en a au moins 55 d'après (1). De plus, $q^2 - q + 1 = 57$ donc $r < q^2 - q + 1$: on n'est pas dans un cas optimal.

Si $n = 55$ ou 56 : on a alors $E\left(\frac{n-1}{q-1}\right) = 7$. Donc $r_1 + \dots + r_{55} \leq 7 \times 55$. Mais, $r_1 + r_2 + \dots + r_{55} = 8 \times 55$ ce qui aboutit à une contradiction : il y a au moins 57 symboles utilisés. On aurait aussi pu dire $r = r_1 + \dots + r_8 - q + 1 \leq 8 \times 7 - 8 + 1 = 49$: impossible car on a 55 cartes.

Si $n = 57$: alors $n = q^2 - q + 1$ avec $q - 1 = 7$ premier, et il est donc possible de construire un jeu optimal de 57 cartes (et donc de 55 cartes). Au minimum, il y a donc 57 symboles utilisés dans DOBBLE et sans changer ceci, on aurait pu construire un jeu de 57 cartes. Effectivement, après vérification, il y a 57 symboles dans le jeu et on peut ajouter deux cartes dans le jeu commercialisé.

VI Plans projectifs finis

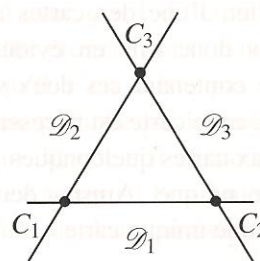
Nous allons voir ici, que les jeux DOBBLE optimaux sont en fait des objets mathématiques connus : les plans projectifs finis.

VI.1 Définition

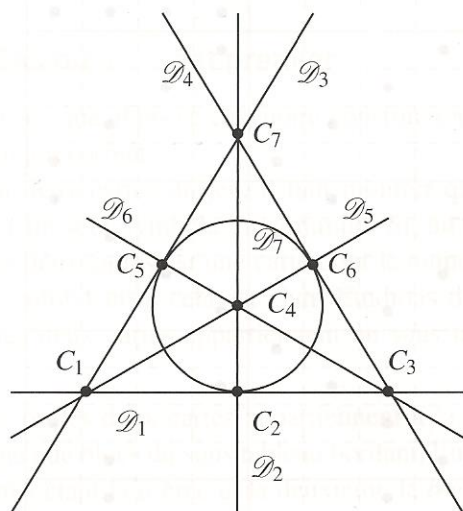
Qu'est-ce qu'un plan projectif fini ? Un plan projectif fini est un couple $(\mathcal{P}, \mathcal{D})$ où les éléments de $\mathcal{P}$ sont appelés les points et ceux de $\mathcal{D}$ les droites vérifiant les axiomes :

- (1) Deux points distincts appartiennent à une unique droite,
- (2) Deux droites distinctes se coupent en un unique point,
- (3) Chaque droite passe par au moins 3 points,
- (4) Il existe au moins trois points non alignés.

Voici un exemple, qui n'est pas un plan projectif fini, car l'axiome (3) n'est pas vérifié, néanmoins, on visualise bien sur cet exemple les axiomes (1) et (2).



Voici, un autre exemple, qui est bien un plan projectif fini mais dont la représentation n'est pas aussi simple : il s'agit du plan de Fano :



Nous avons 7 droites : les 6 droites « classiques » ($\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4, \mathcal{D}_5, \mathcal{D}_6$) ainsi que le cercle inscrit ($\mathcal{D}_7$), et sur chacune de ces droites, nous avons 3 points.

VI.2 Lien avec DOBBLE

Vérifions qu'à un jeu de DOBBLE optimal avec $q \geq 3$ correspond un plan projectif fini. Soit un jeu de DOBBLE optimal avec $q \geq 3$. On note $\mathcal{P}$ l'ensemble des cartes du jeu et $\mathcal{D}$ l'ensemble des symboles du jeu. Un point C de $\mathcal{P}$ appartient à une droite i de $\mathcal{D}$ signifie que la carte C contient le symbole i . ($\mathcal{P}, \mathcal{D}$) vérifie bien les quatre axiomes précédents :

- (1) Deux cartes (distinctes) ont en commun un unique symbole autrement dit : « par deux cartes distinctes passe un unique symbole ».
- (2) Deux symboles différents se trouvent sur une unique carte : en effet soit (i, j) deux symboles, $i \neq j$. On sait, qu'il y a q cartes contenant le symbole i (voir 4.2). Sur ces q cartes sont donc présents $1 + q(q - 1)$ symboles soit $q^2 - q + 1$ symboles c'est à dire la totalité des symboles. En particulier, l'une des cartes a le symbole j . Nous avons donc mis en évidence l'existence d'une carte contenant ces deux symboles i et j . Par ailleurs, cette carte est nécessairement unique puisque deux cartes quelconques ont en commun un symbole unique. Ainsi « deux symboles se coupent en une unique carte ».
- (3) Chaque symbole est présent sur au moins 3 cartes : en effet, chaque symbole est présent sur

q cartes. Ainsi, « chaque symbole passe par au moins 3 cartes ».

- (4) Il existe au moins trois cartes n'ayant pas un symbole commun puisque c'est l'hypothèse dans laquelle nous nous sommes placés afin que le jeu ait un intérêt ludique. Ainsi, « il existe au moins trois cartes non alignées ».

Inversement, tout plan projectif fini $(\mathcal{P}, \mathcal{D})$ nous donne un jeu DOBBLE puisque qu'on peut voir chaque point de $\mathcal{P}$ comme une carte sur laquelle on inscrirait la liste des droites auxquelles il appartient. Alors, d'après le premier axiome, on obtient ainsi un jeu DOBBLE, et celui-ci a un intérêt ludique par l'axiome (4). De plus, le jeu obtenu est optimal : en effet, soit r le nombre de cartes (c'est-à-dire le nombre de points) du jeu obtenu, on peut montrer qu'il existe $q \in \mathbb{N}$ tel que $r = q^2 - q + 1$, qu'il y a $n = r$ symboles et q symboles par carte.

Plus précisément : soit i un symbole et C une carte ne contenant pas i . A chaque symbole j de C on peut associer une unique carte contenant i et j (d'après l'axiome (2)), en terme de cardinal, cela donne que le nombre de symboles de C est égal au nombre de cartes contenant i et ainsi, toutes les cartes ne contenant pas i ont le même nombre de symboles. Soit maintenant C' une carte contenant i , et soit k un symbole ne se trouvant ni sur C ni sur C' (son existence vient des axiomes (3) et (4)²), alors C et C' ont le même nombre de symboles (qui vaut le nombre de cartes contenant le symbole k) et ainsi, chaque carte contenant i a autant de symboles que C .

Conclusion : toutes les cartes ont le même nombre de symboles : notons-le q . C'est aussi le nombre de cartes contenant un symbole donné.

Ensuite, en considérant l'ensemble des symboles des cartes contenant i (il y en a q), on obtient l'ensemble des symboles utilisés : il y en a donc : $1 + q(q - 1)$.

Enfin, si r est le nombre de cartes, comme chaque symbole est présent sur q cartes, on a $rq = (1 + q(q - 1))q$ donc $r = 1 + q(q - 1)$.

On a donc autant de symboles que de cartes : le jeu est optimal.

Remarquons au passage, que nous avons en fait montré que dans un plan projectif fini, il y a autant de droites que de points, que ce nombre s'écrit sous la forme $q^2 - q + 1$ et q vaut aussi le nombre de points par

2. On considère le symbole commun à C et C' (c'est-à-dire la droite passant par C et C') : il existe une troisième carte le contenant (c'est-à-dire il existe un troisième point sur cette droite) et on considère k un symbole de cette carte qui ne soit pas le symbole commun (ce point appartient à une autre droite que la droite (CC')).

droite ou encore le nombre de droites auxquelles appartient un point quelconque. $q-1$ est appelé l'ordre du plan projectif fini.

Le premier exemple donné, qui n'est pas un plan projectif, nous donne le jeu décrit précédemment pour $q=2$ et $r=3$. En effet, les droites sont les symboles : numérotions-les de 1 à 3. Les points sont les cartes : sur chaque carte figurent les droites auxquelles appartient la carte. Ainsi, nous avons trois cartes : $C_1 = (12)$, $C_2 = (13)$ et $C_3 = (23)$.

Pour le deuxième exemple, on obtient le jeu : $C_1 = (1\ 3\ 5)$, $C_2 = (1\ 2\ 7)$, $C_3 = (1\ 4\ 6)$, $C_4 = (2\ 5\ 6)$, $C_5 = (3\ 6\ 7)$, $C_6 = (4\ 5\ 7)$ et $C_7 = (2\ 3\ 4)$: cela correspond au jeu décrit en 4.2 à une permutation près des symboles : par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 3 & 7 & 2 & 6 & 5 \end{pmatrix}$.

VI.3 Construction d'un plan projectif fini

On a vu que construire un jeu DOBBLE optimal c'est construire un plan projectif fini. Or, nous savons construire des plans projectifs finis d'ordre p^f où p est un nombre premier et f est un entier naturel non nul et ainsi, nous savons construire des jeux DOBBLE optimaux avec $n = r = (p^f + 1)^2 - p^f - 1 + 1$ cartes et autant de symboles et avec $p^f + 1$ symboles sur chaque carte.

On procède de la façon suivante pour construire un plan projectif fini d'ordre p^f : on note $\mathbb{F}_{p^f}$ le corps fini à p^f éléments et on considère le $\mathbb{F}_{p^f}$ -espace vectoriel $(\mathbb{F}_{p^f})^3$, qui est de dimension 3. Dans cet espace vectoriel, on considère d'une part l'ensemble des droites vectorielles : $\mathcal{D}_1, \dots, \mathcal{D}_r$, puis l'ensemble des plans vectoriels $\mathcal{P}_1, \dots, \mathcal{P}_r$ et on appelle $\mathcal{P} = \{\mathcal{D}_1, \dots, \mathcal{D}_r\}$ et $\mathcal{D} = \{\mathcal{P}_1, \dots, \mathcal{P}_r\}$. Le couple $(\mathcal{P}, \mathcal{D})$ est un plan projectif fini d'ordre p^f : en effet,

- (1) Deux points distincts appartiennent à une unique droite puisque deux droites distinctes de $(\mathbb{F}_{p^f})^3$ appartiennent à un unique plan de $(\mathbb{F}_{p^f})^3$,
- (2) Deux droites distinctes se coupent en un unique point puisque deux plans distincts de $(\mathbb{F}_{p^f})^3$ se coupent selon une unique droite de $(\mathbb{F}_{p^f})^3$,
- (3) Chaque droite passe par au moins trois points puisque chaque plan de $(\mathbb{F}_{p^f})^3$ contient au moins trois droites,
- (4) Il existe au moins trois points non alignés puisque qu'il existe au moins trois droites de $(\mathbb{F}_{p^f})^3$ non coplanaires.

Explicitons cette construction des plans projectifs finis d'ordre p^f pour construire un jeu DOBBLE : prenons $p=2$ et $f=1$: cela va nous permettre de

construire un jeu DOBBLE avec 7 cartes (nommées $C_1, C_2, \dots, C_7$), 7 symboles et 3 symboles par carte.

$(\mathbb{F}_2)^3 = \{(0,0,0), (0,0,1), (0,1,0), (1,0,0), (0,1,1), (1,0,1), (1,1,0), (1,1,1)\}$, et les droites de cet espace sont engendrées par chacun des 7 vecteurs non nuls, et comme ils ne sont pas colinéaires, on obtient exactement 7 droites (7 qui est le nombre de points de notre plan projectif fini et donc aussi le nombre de cartes du jeu qu'on est en train de construire...) : $\mathcal{D}_1 = \text{Vect}\{(0,0,1)\}$, $\mathcal{D}_2 = \text{Vect}\{(0,1,0)\}$, $\mathcal{D}_3 = \text{Vect}\{(1,0,0)\}$, ... Les plans de cet espace sont au nombre de 7 et sont :

$$\begin{aligned} \mathcal{P}_1 &= \text{Vect}\{(0,0,1), (0,1,0)\} \\ &= \{(0,0,0), (0,0,1), (0,1,0), (0,1,1)\} \\ \mathcal{P}_2 &= \text{Vect}\{(0,0,1), (1,0,0)\} \\ &= \{(0,0,0), (0,0,1), (1,0,0), (1,0,1)\} \\ \mathcal{P}_3 &= \text{Vect}\{(1,0,0), (0,1,0)\} \\ &= \{(0,0,0), (1,0,0), (0,1,0), (1,1,0)\} \\ \mathcal{P}_4 &= \text{Vect}\{(1,1,1), (0,0,1)\} \\ &= \{(0,0,0), (1,1,1), (0,0,1), (1,1,0)\} \\ \mathcal{P}_5 &= \text{Vect}\{(1,1,1), (0,1,0)\} \\ &= \{(0,0,0), (1,1,1), (0,1,0), (1,0,1)\} \\ \mathcal{P}_6 &= \text{Vect}\{(1,1,1), (1,0,0)\} \\ &= \{(0,0,0), (1,1,1), (1,0,0), (0,1,1)\} \\ \mathcal{P}_7 &= \text{Vect}\{(1,1,0), (0,1,1)\} \\ &= \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\} \end{aligned}$$

Pour construire le jeu, on considère d'abord $\mathcal{D}_1$ et sur C_1 on met les numéros correspondant aux plans qui contiennent $\mathcal{D}_1$: donc $C_1 = (1\ 2\ 4)$, puis de même, $C_2 = (1\ 3\ 5)$, $C_3 = (2\ 3\ 6)$, $C_4 = (1\ 6\ 7)$, $C_5 = (2\ 5\ 7)$, $C_6 = (3\ 4\ 7)$ et $C_7 = (4\ 5\ 6)$. Cela correspond au jeu décrit dans 4.2, à une permutation près des symboles (la transposition $(3\ 4)$).

VI.4 Et pour les autres valeurs ?

- Si $q-1$ est une puissance d'un nombre premier, alors il existe un jeu optimal.
- On ne connaît pas de jeu optimal (ou de plan projectif fini) avec $q-1$ différent d'une puissance d'un nombre premier mais on ne sait pas non plus montrer qu'il n'en existe pas. On a cependant une réponse partielle par le théorème de BRUCK-RYSER qui dit que s'il existe un jeu optimal et que $q-1$ est congru à 1 ou 2 modulo 4 alors $q-1$ est la somme de deux carrés.
- Grâce aux ordinateurs, on sait qu'il n'existe pas de jeu optimal pour $q-1=10$.

Voici donc un petit résumé sur les entiers de 1 à 15 de l'état de nos connaissances sur l'existence d'un jeu optimal :

q	$q-1$	q^2-q+1	notes
2	1	3	(1)
3	2	7	(2)
4	3	13	(2)
5	4	21	(3)
6	5	31	(2)
7	6	43	(4)
8	7	57	(2)
9	8	73	(3)
10	9	91	(3)
11	10	111	(5)
12	11	133	(2)
13	12	157	(6)
14	13	183	(2)
15	14	211	(4)

Notes :

- (1) : on a vu l'existence d'un jeu optimal dans ce cas.
- (2) : $q-1$ est premier : il existe un jeu optimal dont on a donné une construction par les tableaux (et les plans projectifs finis).
- (3) : $q-1$ est la puissance d'un nombre premier : il existe un jeu optimal dont on a donné une construction par les plans projectifs finis.
- (4) : il n'existe pas de jeu optimal dans ce cas (à l'aide du théorème de BRUCK-RYSER qui peut se traduire par : s'il existe un jeu optimal et que $q-1$ est congru à 1 ou 2 modulo 4 alors $q-1$ est la somme de deux carrés).
- (5) : il n'existe pas de jeu optimal dans ce cas à l'aide d'une recherche exhaustive par ordinateur.
- (6) : la question est ouverte ! $q=13$ est le plus petit entier pour lequel la question est ouverte : existe-t-il un jeu DOBBLE optimal avec 13 symboles sur chacune des 157 cartes ? Existe-t-il un plan projectif fini d'ordre 12 ?

Plus généralement, existe-t-il un plan projectif fini d'ordre qui ne soit une puissance d'un nombre premier ? Cette question, ouverte, fait l'objet d'une conjecture (voir [6]).

VII Annexe : procédures Maple

On présente ici des procédures MAPLE construisant un jeu DOBBLE optimal contenant $q+1$ symboles par carte, $(q+1)^2 - (q+1) + 1$ cartes et symboles où $q = p^f$, p étant un nombre premier : on utilise l'algorithme sur les plans projectifs finis présenté dans ce qui précède.

On commence par définir p , le nombre premier avec lequel on travaille, f un entier non nul et $q = p^f$. On définit aussi $G = \mathbb{F}_q$.

```
> p := 2; f := 2; q := p^f;
> G := GF(p, f);
```

Notons maintenant que nous disposons de plusieurs fonctions MAPLE dans le corps $G = \mathbb{F}_q$:

- $G:-input(i)$: G est composé de q éléments que MAPLE numérote de 0 à $q-1$, pour i un entier compris entre 0 et $q-1$, $G:-input(i)$ renvoie le i -ème terme du corps G , $G:-input(0)$ renvoyant le 0 du corps G ,
- $G:-'+(a,b)$: effectue la somme dans G des deux éléments de G , a et b ,
- $G:-'*(a,b)$: effectue le produit dans G des deux éléments de G , a et b .

La procédure `espace` renvoie l'ensemble des vecteurs non nuls de $(\mathbb{F}_q)^3$.

```
> espace := proc ()
local l, i, j, k;
l := NULL;
for i from 0 to q-1 do
  for j from 0 to q-1 do
    for k from 0 to q-1 do
      if not(k = 0 and j = 0 and i = 0)
      then l := l, [G:-input(i), G:-input(j),
G:-input(k)] fi;
    od;
  od;
od;
{l};
end;
```

La procédure `planeng` renvoie, sous forme d'ensemble, le sous espace, privé du vecteur nul, de $(\mathbb{F}_q)^3$ engendré par les deux vecteurs u et v .

```
> planeng := proc (u, v)
local p, i, j, g;
p := NULL;
for i from 0 to q-1 do
  for j from 0 to q-1 do
    g := [G:-'+(G:-'*(G:-input(i), u[1]),
G:-'*(G:-input(j), v[1])),
G:-'+(G:-'*(G:-input(i), u[2]),
G:-'*(G:-input(j), v[2])),
G:-'+(G:-'*(G:-input(i), u[3]),
G:-'*(G:-input(j), v[3]))];
    if g <> [G:-input(0), G:-input(0),
G:-input(0)] then p := p, g fi;
  od;
od;
{p};
end;
```

La procédure `sev` renvoie la séquence de deux ensembles. Le premier ensemble est constitué des droites de $(\mathbb{F}_q)^3$ et le second des plans de $(\mathbb{F}_q)^3$. Pour cela, on prend tous les sous espaces de $(\mathbb{F}_q)^3$ engendrés par deux vecteurs non nuls de $(\mathbb{F}_q)^3$: on obtient toutes les droites et les plans de $(\mathbb{F}_q)^3$. Ensuite, pour les distinguer, on utilise que les droites sont constituées de q points et les plans de q^2 points. A noter que dans nos programmes, on a ôté le vecteur nul de tous les espaces vectoriels.

```
> sev := proc ()
local l, p, i, j, plan, droite;
l := espace(); p := NULL; plan := NULL;
droite := NULL;
for i from 1 to nops(l) do
  for j from i to nops(l) do
    p := planeng(l[i], l[j]);
    if nops(p) = q-1
    then droite := droite, p
    else plan := plan, p fi;
  od;
od;
{droite}, {plan};
end;
```

La procédure `dobble` construit un jeu DOBBLE optimal : chaque droite de $(\mathbb{F}_q)^3$ est une carte et les symboles la constituant sont les plans contenant cette droite.

```
dobble := proc ()
local p, d, l, i, j, ll, sev;
sev := sev2(); d := sev[1]; p := sev[2];
l := NULL;
```

```
for i from 1 to nops(d) do
  ll := NULL;
  for j from 1 to nops(p) do
    if member(d[i][1], p[j])
    then ll := ll, j fi;
  od;
  l := l, [ll]
od;
l;
end;
```

Il faut tout de même noter les temps de calcul importants de ces programmes même pour des valeurs relativement petites de q , l'une des causes étant les calculs de MAPLE dans $\mathbb{F}_q$.

Références

- [1] Maxime BOURRIGAN, *Dobble et la géométrie finie*, Images des Mathématiques, CNRS, 2011.
<http://images.maths.cnrs.fr/Dobble-et-la-geometrie-finie.html>
- [2] Clement W. H. LAM, *The Search for a Finite Projective Plane of Order 10*, <http://www.cecm.sfu.ca/organics/papers/lam/paper/html/paper.html>
- [3] http://en.wikipedia.org/wiki/Projective_plane
- [4] <http://mathworld.wolfram.com/Bruck-Ryser-ChowlaTheorem.html>
- [5] <http://www.math.unh.edu/~dvf/532/7proj-plane.pdf> (démonstration élémentaire du théorème de BRUCK-RYSER)
- [6] <http://symomega.wordpress.com/2010/02/26/open-problems-in-finite-geometry-the-prime-power-conjecture/>