

# Une analyse du Cube Hongrois

Matthieu BARREAU

## Sommaire

<b>1</b>	<b>Les mathématiques dans le cube</b>	<b>2</b>
1.1	Préliminaires . . . . .	2
1.2	Les groupes du Cube . . . . .	5
<b>2</b>	<b>Les algorithmes du cube</b>	<b>14</b>
2.1	L'intérêt des mathématiques . . . . .	14
2.2	Algorithmes de bases et conséquences . . . . .	15
2.3	Algorithme de résolution . . . . .	18

## Introduction

Le Rubik's Cube, ou bien simplement Cube, est un casse-tête inventé en 1974 par Ernő Rubik. Les possibilités de mouvements et sa formidable complexité de résolution en font un admirable objet mathématique. En effet, ses mécanismes internes fascinent et ceux qui arrivent à le résoudre ne semblent plus vraiment humains.

Pourtant par l'approche mathématique, nous allons montrer que le cube ne défie pas la logique et que rigueur et patience permettent sa résolution par tous. Internet est encore un bon exemple, il fleurit de sites proposant des algorithmes de résolutions, et la seule compétence demandée est une bonne mémoire...

Dans la résolution du cube, la science informatique y a joué une grande place. La recherche d'algorithme est à la portée de tous et sa concrétisation par ordinateur est une réussite. L'étude du sujet est d'autant plus importante qu'elle représente encore un réel défi. Effectivement, les algorithmes du Cube sont très intéressants mais deviennent rapidement très complexes quant à l'optimisation du nombre de mouvements. Ce sujet sera traité dans notre dernière partie.

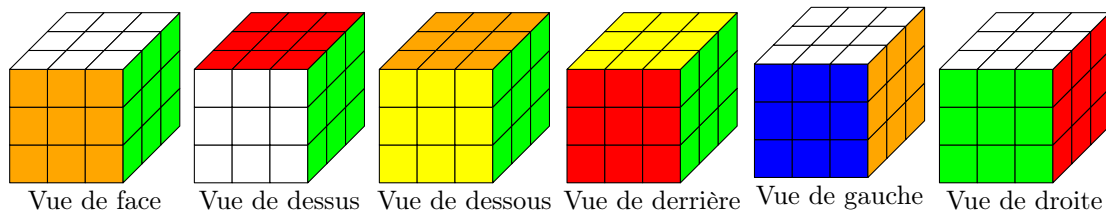
## 1 Les mathématiques dans le cube

### 1.1 Préliminaires

Le cube semble un objet bien trop logique pour ne pas avoir une facette mathématique. Bien qu'à l'origine, son constructeur voulait faire étudier son mécanisme à ses élèves, il se révèle que le cube illustre parfaitement bien une branche très abstraite des mathématiques : **la théorie des groupes**.



Pour étudier cet aspect, nous allons avoir besoin de travailler avec des chiffres et des lettres.



Nous utiliserons les représentations ci dessus durant cet exposé.

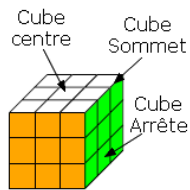
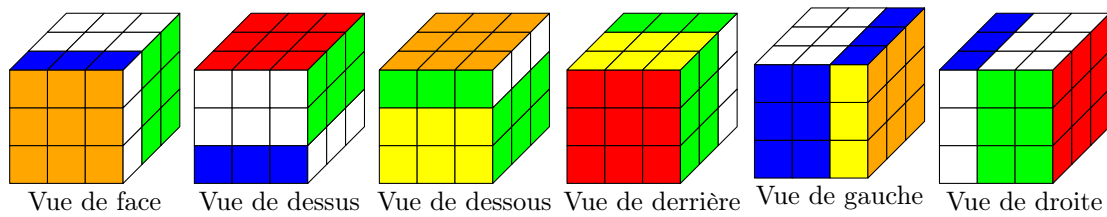
Nous étudions les déplacements des petits cubes (nous les appellerons dorénavant les **cubes secondaires**) au cours des mouvements.

Si nous prenons la face orange devant nous, nous avons plusieurs mouvements possibles :

- Rotation de la face orange (frontale) : F
- Rotation de la face rouge (face arrière) : B
- Rotation de la face verte (à droite) : R
- Rotation de la face bleue (à gauche) : L
- Rotation de la face blanche (au dessus) : T
- Rotation de la face jaune (au dessous) : D

Tous ces mouvements se font dans le sens horaire. Un mouvement anti-horaire se notera X' avec X la rotation voulue.

La vue du cube après une rotation F est visible sur la figure ci-après :



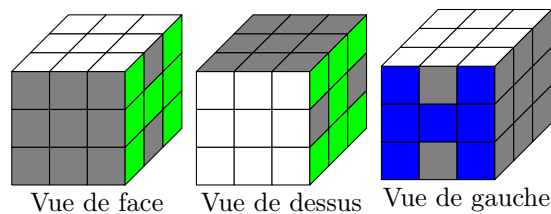
Éclairons ces rotations par des objets mathématiques. Nous pouvons constater qu'après une rotation F, le cube reste un cube. Chaque cube secondaire a permuté avec un autre ou est resté à sa place. Il y a donc eu **permutation**. Il existe deux types de permutation qui permettent de rendre compte de la totalité des mouvements du cube (preuve dans la section suivante.). En effet, les permutations peuvent se « ranger » par catégorie en fonction des cubes secondaires qu'elles déplacent. Nous en distinguons trois sortes : **Cube centre** (CC), **Cube sommet** (CS) et **Cube Arête** (CA).

Ainsi, nous pouvons à partir du cube terminé définir une position par une suite de permutations. Nous énoncerons diverses propositions par la suite à ce sujet.

Cependant, dire que chaque position du cube est issue d'une composition de permutations est fausse. En effet, il nous manque une donnée capitale, **la rotation du cube secondaire sur lui même**.

Pour tenter de donner un sens à cette affirmation, nous pouvons prendre arbitrairement un cube secondaire et nous grisons une de ses faces. **Chaque cube secondaire doit avoir une seule face grisée**. Nous pouvons omettre les cubes centraux qui sont des invariants du mouvement.

Pour faire simple, et ce tout au long de cet exposé, les faces des cubes secondaires marquées seront les faces oranges, puis les faces vertes et bleues de la deuxième couronne<sup>1</sup> et enfin l'intégralité de la dernière face. Schématiquement, nous obtenons la figure ci-dessous :



Chaque cube secondaire se voit attribuer un numéro. La position de référence (ici le cube fait) est mémorisée. On compare la position des cubes gris après permutation avec ceux du cube de référence. Traitons d'abord les cubes sur les arêtes.

- Si la face grisée du cube secondaire est **au même endroit** dans le cube de référence, nous attribuons **1** comme indice de rotation.
- Si la face grisée **ne coïncide pas** avec le cube de référence, son indice de rotation est **-1**.

On a donc 12 chiffres, -1 ou 1, représentant les indices de rotation des cubes arêtes secondaires. Ces chiffres sont rangés dans une matrice 1x12 :  $\mathcal{M}_A$ .

De même, on a pour les cubes sommets :

- Si la face grisée du cube secondaire est **au même endroit** dans le cube de référence, nous attribuons **0** comme indice de rotation.
- Si la face grisée est à **120°<sup>2</sup>** par rapport au cube de référence, son indice de rotation est **1**
- Si la face grisée est à **-120°** par rapport au cube de référence, son indice de rotation est **-1**.

1. Une couronne est un plan du cube parallèle à une face (chaque couronne contient donc 9 cubes secondaires, exceptée la deuxième couronne, au milieu, qui n'en contient que 8).

2. les angles sont orientés selon le sens trigonométrique en positionnant le cube secondaire en face de nous.

On a donc 8 chiffres, 0, 1 ou -1, représentant les indices de rotation des cubes sommets secondaires soit une matrice  $1 \times 8$  :  $\mathcal{M}_S$ .

La connaissance de la permutation  $\sigma$ , et des matrices  $\mathcal{M}_A$  et  $\mathcal{M}_S$  permet de coder toutes les positions du cube. Une position du cube se note alors :

$$[\sigma, \mathcal{M}_A, \mathcal{M}_S]$$

## 1.2 Les groupes du Cube

Cette partie s'articulera autour d'un échange Proposition/Preuve.

**Définition 1.** *L'ensemble des positions possibles du rubik's Cube est un ensemble appelé  $G$ .*

**Proposition 1.**  *$G$  est l'ensemble des positions engendrées par une composition des 6 mouvements élémentaires.<sup>3</sup>*

Preuve :

L'ensemble des positions possibles du Rubik's Cube sont celles qui résultent des manipulations de l'utilisateur. Ainsi, c'est l'ensemble des mouvements que l'on peut faire.

Nous ne pouvons faire que des mouvements de rotation de  $90^\circ$ ,  $180^\circ$  ou  $270^\circ$ . Il y a 9 rotations possibles. Cependant, les rotations des couronnes du milieu sont équivalentes à des rotations des deux couronnes qui les entourent. Six rotations engendrent donc l'ensemble des positions du rubik's cube.

**Proposition 2.** *Toute permutation du Rubik's Cube est une permutation des sommets  $\sigma_S$  et une permutation des arêtes  $\sigma_A$ .*

Preuve : Il y a douze cubes arêtes et 8 cubes sommets. On peut alors nommer  $\sigma_S \in \mathfrak{S}_8$  la permutation des sommets et  $\sigma_A \in \mathfrak{S}_{12}$  celle des arêtes. Comme un CS reste un CS et un CA reste un CA, ce sont des permutations à supports disjoints. Pour simplifier leur écriture, nous différencieront désormais les CA des CS. Ainsi, les CS seront numérotés de 1 à 8 et les CA de 1 à 12.

---

3. Un mouvement élémentaire est une rotation d'une des 6 faces.

Chaque position possible est engendrée par un mouvement élémentaire. Considérons uniquement un mouvement élémentaire de  $90^\circ$ , alors  $\sigma_S$  et  $\sigma_A$  sont des 4-cycles donc des permutations. On sait alors que chaque rotation de face s'exprime avec deux permutations. Or les rotations des 6 faces élémentaires engendrent  $G$ , donc tous les mouvements autorisés sont représentés par deux permutations  $\sigma_S \in \mathfrak{S}_8$  et  $\sigma_A \in \mathfrak{S}_{12}$ . On a alors ce que l'on désire prouver.

**Théorème 1** (fondamental). *Soit un quadruplé  $(r, s, x, y)$  avec  $r \in \mathfrak{S}_8, s \in \mathfrak{S}_{12}, x \in \{-1, 0, 1\}^8, y \in \{-1, 1\}^{12}$ , on a :*

$$(r, s, x, y) \in G \Leftrightarrow \begin{cases} \varepsilon(r) = \varepsilon(s) \\ \sum_{i=1}^8 x_i \equiv 0[3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2] \text{ avec } y = (y_1, \dots, y_{12}) \end{cases}$$

Preuve : Chaque permutation du Rubik's Cube est la composée de mouvements élémentaires. Supposons  $\sigma$  une permutation possible du Rubik's Cube qui se décompose en  $n$  mouvements élémentaires<sup>4</sup>.

Un mouvement élémentaire est composé de deux 4-cycles, l'un des sommets, l'autre des arêtes, respectivement  $\sigma_S$  et  $\sigma_P$ . On note également  $\sigma_{S_k}$  la  $k^{me}$  permutation des sommets et  $\sigma_{A_k}$  la  $k^{me}$  permutation des arêtes.

On aura aussi besoin de  $\Sigma_{S_k} = \sigma_{S_k} \circ \dots \circ \sigma_{S_1}$  et  $\Sigma_{A_k} = \sigma_{A_k} \circ \dots \circ \sigma_{A_1}$ . On sait alors que  $\Sigma_{S_n} = \sigma_S$  et  $\Sigma_{A_n} = \sigma_A$ .

Soit  $\mathcal{P}(k) : \ll \varepsilon(\Sigma_{S_k}) = \varepsilon(\Sigma_{A_k}) \gg$ .

On applique l'identité au cube fait. On a donc  $\sigma_{S_0} = \sigma_{A_0} = id$ . d'où  $\varepsilon(\sigma_{S_0}) = \varepsilon(\sigma_{A_0})$ , soit  $\mathcal{P}(0)$  est vraie.

Supposons  $\mathcal{P}(k)$  vraie pour  $k \in \llbracket 1; n \rrbracket$ .

Soit  $\sigma_{S_{k+1}}$  la  $(k+1)^{me}$  permutations des sommets. On a alors  $\Sigma_{S_{k+1}} = \sigma_{S_{k+1}} \circ \sigma_{S_k} \circ \dots \circ \sigma_{S_1} = \sigma_{S_{k+1}} \circ \Sigma_{S_k}$ .

Comme la signature est un morphisme de groupe on a :  $\varepsilon(\Sigma_{S_{k+1}}) = \varepsilon(\sigma_{S_{k+1}}) \times \varepsilon(\Sigma_{S_k}) = (-1)^3 \times \varepsilon(\Sigma_{S_k}) = -\varepsilon(\Sigma_{S_k})$ , car  $\sigma_{S_k}$  est un 4-cycle.

---

4. Rappel : L'identité (qui consiste à ne rien tourner), n'est pas un mouvement élémentaire.

Soit  $\sigma_{A_{k+1}}$  la  $(k+1)^{me}$  permutations des arêtes. On a alors  $\Sigma_{A_{k+1}} = \sigma_{A_{k+1}} \circ \sigma_{A_k} \circ \dots \circ \sigma_{A_1} = \sigma_{A_{k+1}} \circ \Sigma_{A_k}$ .

Comme la signature est un morphisme de groupe on a :  $\varepsilon(\Sigma_{A_{k+1}}) = \varepsilon(\sigma_{A_{k+1}}) \times \varepsilon(\Sigma_{A_k}) = (-1)^3 \times \varepsilon(\Sigma_{A_k}) = -\varepsilon(\Sigma_{A_k})$ , car  $\sigma_{A_k}$  est un 4-cycle.

D'où  $\varepsilon(\sigma_{S_{k+1}}) = \varepsilon(\sigma_{A_{k+1}})$  d'après l'hypothèse de récurrence. Alors  $\mathcal{P}(k+1)$  est vraie. La proposition est vraie au rang 0 et est héréditaire, d'après le principe de récurrence, on a :

$$\forall n \in \mathbb{N}, \mathcal{P}(n) \text{ est vraie.}$$

Soit  $\mathcal{Q}(k)$  : « La somme des indices de rotation des arêtes après  $k$  mouvements élémentaires est multiple de deux ».

Un mouvement élémentaire est composé de deux 4-cycles, l'un des sommets, l'autre des arêtes. On s'occupe ici des arêtes.

On applique l'identité au cube fait. Le cube reste fait, son indice de rotation des arêtes est nul. Il est donc bien multiple de deux. Alors  $\mathcal{Q}(0)$  est vraie.

Supposons  $\mathcal{Q}(k)$  vraie pour  $k \in \llbracket 1; n \rrbracket$ .

La somme des indices de rotation des arêtes après  $k$  mouvements élémentaires est donc multiple de deux. On notera  $I_k \equiv 0[2]$ .

Le  $(k+1)^{me}$  mouvement élémentaire est une rotation de face. Notons cette face  $F$ . Pour plus de lisibilité, une face secondaire marquée sera notée 2 et une non-marquée sera notée 1.

– 1<sup>er</sup> cas : Les quatre cubes secondaires ont leurs faces marquées sur  $F$

Après la rotation de  $F$ , les quatre faces 2 sont encore sur cette face. Ainsi les indices de rotation sont les mêmes qu'après  $k$  rotations. On a donc  $I_k = I_{k+1}$ .

– 2<sup>me</sup> cas : Aucun des quatre cubes secondaires n'ont leurs faces marquées sur  $F$

Après la rotation de  $F$ , les quatre faces 1 sont encore sur cette face. Ainsi les indices de rotation sont les mêmes qu'après  $k$  rotations. On a donc  $I_k = I_{k+1}$ .

– 3<sup>me</sup> cas : Il y a trois faces marquées sur  $F$ .

La rotation de  $F$  va entraîner une permutation entre une face 2 et la face 1. Ainsi, on a :

$$I_{k+1} \equiv I_k - 2[2] \text{ soit } I_{k+1} \equiv 0[2].$$

– Dernier cas : Il y a deux faces marquées sur  $F$ .

– 1<sup>er</sup> sous cas : Les deux faces marquées sont côte à côte.

Alors la rotation de  $F$  amènera une face 2 à l'emplacement d'une autre face 2 et une face 1 sera emmenée à l'emplacement d'une face 2. On a aussi une face 2 qui sera déposée à la place d'une face 1. Deux indices de rotation sont différents.  $I_{k+1} \equiv I_k - 2[2]$ , on a donc  $I_{k+1} \equiv 0[2]$

– 2<sup>nd</sup> sous cas : Les deux faces marquées sont opposées.

Une rotation de  $F$  engendrera une inversion. Les faces 1 deviendront 2 et les faces 2 deviendront 1. On a donc quatre indices de rotation différents.  $I_{k+1} \equiv I_k - 4[2]$  soit  $I_{k+1} \equiv 0[2]$

Ainsi,  $I_{k+1} \equiv 0[2]$ . Donc  $\mathcal{Q}(k+1)$  est vraie. D'après le principe de récurrence, on a :

$$\forall n \in \mathbb{N}, \mathcal{Q}(n) \text{ est vraie.}$$

Procéder de même avec les sommets serait extrêmement laborieux. Nous allons donc adopter une autre technique. Pour cela, nous allons avoir besoin de quelques propositions préalables.

**Définition 2.** On définit :

- l'ensemble  $C_k = \mathbb{Z}/k\mathbb{Z}$ .
- les applications :

$$\begin{aligned} I : \quad \mathfrak{G}_8 &\rightarrow C_3 \\ (\sigma, (x_1, \dots, x_8)) &\mapsto \sum_{i=1}^8 x_{\sigma(i)} \end{aligned}$$

$$\begin{aligned} A : \quad \mathfrak{G}_8 \times (C_3)^8 &\rightarrow (C_3)^8 \\ (\sigma, (x_1, \dots, x_8)) &\mapsto (x_{\sigma(1)}, \dots, x_{\sigma(8)}) \end{aligned}$$

$$\begin{aligned} S : \quad G \times (C_2)^{12} &\rightarrow (C_2)^{12} \\ (\sigma, (x_1, \dots, x_{12})) &\mapsto (x_{\sigma(1)}, \dots, x_{\sigma(12)}) \end{aligned}$$

- la loi  $\star$  telle que pour tout quadruplé  $(r, s, x, y)$  avec  $r \in \mathfrak{G}_8, s \in \mathfrak{G}_{12}, x \in \{-1, 0, 1\}^8, y \in \{-1, 1\}^{12}$  et  $(r', s', x', y')$  avec  $r' \in \mathfrak{G}_8, s' \in \mathfrak{G}_{12}, x' \in \{-1, 0, 1\}^8, y' \in \{-1, 1\}^{12}$ , on ait :

$$(r, s, x, y) \star (r', s', x', y') = (r' \circ r, s' \circ s, x + A(r^{-1}, x'), y + S(s^{-1}, y'))$$



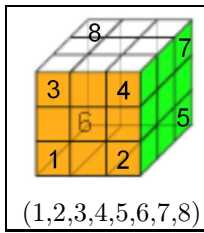
 <p>(1,2,3,4,5,6,7,8)</p>	Q	Indice de rotation des sommets	Somme des indices
	F	(0,0,0,0,0,0,0,0)	0
	B	(0,0,0,0,0,0,0,0)	0
	R	(0,-1,0,1,1,0,-1,0)	0
	L	(1,0,-1,0,0,-1,0,1)	0
	T	(0,0,1,-1,0,0,1,-1)	0
	D	(1,1,0,0,-1,-1,0,0)	0

TABLE 1 – Récapitulatif des indices de rotation

Remarque : La loi  $\star$  correspond physiquement à la succession de deux manipulations du rubik's cube. En effet, on applique bien  $r$  puis  $r'$  (et  $s$  puis  $s'$ ). Il reste à additionner les indices de rotation. Cette dernière affirmation reste encore à prouver.

Preuve : On appelle  $R$  l'indice de rotation d'un emplacement. Un emplacement est différent d'un cube secondaire en ce qu'il ne change pas au fil des mouvements, il garde toujours la même place. Ainsi, soit  $R_1$  son indice après un premier mouvement 1. On refait alors le cube. On note  $R_2$  l'indice de rotation de cet emplacement après un autre mouvement 2. Si on fait le mouvement 1 puis le mouvement 2, on note  $R_t$  l'indice de rotation du cube après ces deux mouvements.

Une fois les choses écrites ainsi, il vient :  $R_t = R_1 + R'_2[k]$  avec  $k = 2$  s'il est question des arêtes,  $k = 3$  pour les sommets. Le terme  $R'_2$  semble inexplicable... Il s'agit simplement de  $R_2$  mais une permutation  $\sigma$  a déjà modifiée le cube. Ainsi, on applique  $R_2$  au cube après  $\sigma^{-1}$ . On a donc :  $R'_2 = K(\sigma_K, R_2)$  où  $K = A$  s'il s'agit des arêtes,  $S$  si l'on modifie les sommets.

Fin de la preuve du théorème.

Soit  $\mathcal{R}(k)$  : « La somme des indices de rotation des sommets après  $k$  mouvements élémentaires est multiple de trois ».

On applique l'identité au cube fait. Le cube reste fait, son indice de rotation des sommets est nul. Il est donc bien multiple de trois. Alors  $\mathcal{R}(0)$  est vraie.

Supposons  $\mathcal{R}(k)$  vraie pour  $k \in \llbracket 1; n \rrbracket$ .

La somme des indices de rotation des sommets après  $k$  mouvements élémentaires est donc multiple de trois. On notera  $I(\Sigma_k, (0, \dots, 0)) = 0$ .

Le  $(k + 1)^{me}$  mouvement élémentaire est une rotation de face. Appelons  $Q$  cette rotation.

Le tableau récapitulatif des différentes valeurs de la somme des indices de rotation en fonction de  $Q$  est présenté en table 1.

$$\begin{aligned} I(\Sigma_{k+1}, (0, \dots, 0)) &\equiv I(\Sigma_k, (0, \dots, 0)) + I(\Sigma_k^{-1}, S(\Sigma_k, (0, \dots, 0))) [3] \\ &\equiv 0 + 0 [3] \end{aligned}$$

Ainsi,  $I(\Sigma_{k+1}, (0, \dots, 0)) \equiv 0 [3]$ . Donc  $\mathcal{R}(k + 1)$  est vraie. On a donc, d'après le principe de récurrence :

$$\forall n \in \mathbb{N}, \mathcal{R}(n) \text{ est vraie.}$$

Finalement,

$$(r, s, x, y) \in G \Rightarrow \begin{cases} \varepsilon(r) = \varepsilon(s) \\ \sum_{i=1}^8 x_i \equiv 0 [3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0 [2] \text{ avec } y = (y_1, \dots, y_{12}) \end{cases}$$

La réciproque sera prouvée après quelques résultats remarquables nécessaires.

**Conséquences directes :**

- Il est impossible de permuter seulement deux CS.

Preuve : Raisonnons par l'absurde. Supposons une telle permutation possible, on a :

$$\exists (i, j) \in \llbracket 1; 12 \rrbracket^2 \ i \neq j, \begin{cases} \sigma_S = id \\ \sigma_A = \begin{pmatrix} i & j \end{pmatrix} \end{cases} \Rightarrow \begin{cases} \varepsilon(\sigma_S) = 1 \\ \varepsilon(\sigma_A) = -1 \end{cases}$$

Ce qui est impossible.

- Il est impossible de permuter seulement deux CA.

Preuve : Raisonnons par l'absurde. Supposons une telle permutation possible, on a :

$$\exists (i, j) \in \llbracket 1; 8 \rrbracket^2 \ i \neq j, \begin{cases} \sigma_S = \begin{pmatrix} i & j \end{pmatrix} \\ \sigma_A = id \end{cases} \Rightarrow \begin{cases} \varepsilon(\sigma_S) = -1 \\ \varepsilon(\sigma_A) = 1 \end{cases}$$

Ce qui est impossible.

- Le cardinal de  $G$  est au plus de 43 252 003 274 489 856 000.

Preuve : D'après le théorème fondamental (uniquement dans le sens prouvé), on sait qu'il ne peut y avoir qu'un seul coin d'indice de rotation non nul et une seule arête d'indice

de rotation non nul. Par conséquent, si l'on place 7 sommets correctement, le 8ème l'est nécessairement. De même si on place 11 arêtes dans leurs positions correctes, la 12ème est bien placée.

On a donc  $7!$  positions de sommets, et  $11!$  positions d'arêtes. Le nombre d'orientations possibles pour les sommets est  $3^7$  et  $2^{11}$  pour les arêtes. Ceci est un maximum car on ne sait pas si ces deux critères sont suffisants, donc s'ils déterminent toutes les positions du Rubik.

Ainsi,  $card(G) \leq 7! \times 3^7 \times 11! \times 2^{11}$ .

**Proposition 3** (et définition). Soit  $G' = \left\{ (r, s, x, y) / \begin{cases} \varepsilon(r) = \varepsilon(s), (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \\ \sum_{i=1}^8 x_i \equiv 0[3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2] \text{ avec } y = (y_1, \dots, y_{12}) \end{cases} \right\}$

Le cardinal de  $G'$  est 43 252 003 274 489 856 000.

Preuve :

On a  $G' \subset F$  avec  $F = \{(r, s, x, y) / (r, s, x, y) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \times \{-1, 0, 1\}^8 \times \{-1, 1\}^{12}\}$

$$card(F) = 8! \times 12! \times 3^8 \times 2^{12}.$$

Or  $\varepsilon(s) = \varepsilon(r) \Leftrightarrow \varepsilon(s \circ r) = 1$ , si  $J = \{s \circ r / (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \text{ r et s à supports disjoints.}\}$  alors  $card(J) = 8! \times 12!$ . On cherche le cardinal de  $J_A$ , le groupe des permutations paires de  $J$ , et on a  $card(J_A) = \frac{card(J)}{2}$ .

$$\text{Donc, } card(G') = \frac{1}{2} \frac{1}{3} \frac{1}{2} \times card(F) = \frac{519\ 024\ 039\ 293\ 878\ 272\ 000}{12} = 43\ 252\ 003\ 274\ 489\ 856\ 000$$

Preuve réciproque du théorème fondamental :

$$\left[ (r, s, x, y) \in G \Rightarrow \begin{cases} \varepsilon(r) = \varepsilon(s), (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \\ \sum_{i=1}^8 x_i \equiv 0[3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2] \text{ avec } y = (y_1, \dots, y_{12}) \end{cases} \right] \Leftrightarrow G' \subset G$$

Donc :  $card(G') \leq card(G) \Leftrightarrow card(G) \geq 43\ 252\ 003\ 274\ 489\ 856\ 000$ .

On a donc  $card(G) = 43\ 252\ 003\ 274\ 489\ 856\ 000$ . Or deux ensembles avec une relation d'inclusion l'un dans l'autre et de même cardinal sont identiques. Alors  $G = G'$ . C'est ce que l'on voulait démontrer. L'équivalence est vérifiée.

**Définition 3.** Soit  $H$  l'ensemble tel que :

$$H = \left\{ (r, s, x, y) / \left\{ \begin{array}{l} (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \\ \sum_{i=1}^8 x_i \equiv 0[3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2] \text{ avec } y = (y_1, \dots, y_{12}) \end{array} \right. \right\}$$

**Proposition 4.**  $G \subset H$ . On dit que  $H$  est l'ensemble élargi des positions du Rubik's Cube.

En effet,  $H$  est l'ensemble des positions possibles en « remontant mal » le rubik's Cube.

Preuve :

$$(r, s, x, y) \in G \Leftrightarrow \left\{ \begin{array}{l} \varepsilon(r) = \varepsilon(s), (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \\ \sum_{i=1}^8 x_i \equiv 0[3] \text{ avec } x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2] \text{ avec } y = (y_1, \dots, y_{12}) \end{array} \right. \Rightarrow \left\{ \begin{array}{l} (r, s) \in \mathfrak{G}_8 \times \mathfrak{G}_{12} \\ \sum_{i=1}^8 x_i \equiv 0[3], x = (x_1, \dots, x_8) \\ \sum_{i=1}^{12} y_i \equiv 0[2], y = (y_1, \dots, y_{12}) \end{array} \right. \quad (*)$$

$$(*) \Leftrightarrow (r, s, x, y) \in H \Leftrightarrow G \subset H$$

**Proposition 5.**  $(H, \star)$  est un groupe non-abélien.

Preuve :

Soit  $((r, s, x, y), (r', s', x', y'), (r'', s'', x'', y'')) \in H^3$ .

$$(r, s, x, y) \star (r', s', x', y') = (r' \circ r, s' \circ s, x + S(r^{-1}, x'), y + A(s^{-1}, y'))$$

On a  $r \circ r' \in \mathfrak{G}_8$  car  $(r, r') \in \mathfrak{G}_8^2$ ,  $s' \circ s \in \mathfrak{G}_{12}$  car  $(s, s') \in \mathfrak{G}_{12}^2$ .

De plus,  $x + S(r^{-1}, x') = (x_1, \dots, x_8) + (x_{r^{-1}(1)}, \dots, x_{r^{-1}(8)})$ . Donc :  $\sum_{i=1}^8 x_i + x_{r^{-1}(i)} \equiv 0[3]$ , d'après la définition de la loi  $\star$ .

De même,  $y + A(s^{-1}, y') = (y_1, \dots, y_{12}) + (y_{s^{-1}(1)}, \dots, y_{s^{-1}(12)})$ . Donc :  $\sum_{i=1}^{12} y_i + y_{r^{-1}(i)} \equiv 0[2]$ , d'après la définition de la loi  $\star$ .

Finalement,  $(r, s, x, y) \star (r', s', x', y') \in H$ .

$(r, s, x, y) \star (id, id, 0, 0) = (r, s, x + S(0), y + A(0)) = (r, s, x, y)$ ,  $(id, id, 0, 0)$  est l'élément neutre et il appartient à  $H$ .

$r$  et  $s$  sont, par définition, des applications bijectives. Il existe donc leurs applications réciproques,  $r^{-1}$  et  $s^{-1}$ , respectivement dans  $\mathfrak{G}_8$  et  $\mathfrak{G}_{12}$ . On sait aussi que  $\forall x \in \{-1, 0, 1\}, -x \in \{-1, 0, 1\}$  et  $\forall y \in \{-1, 1\}, -y \in \{-1, 1\}$ . Notons  $X = (r^{-1}, s^{-1}, -A(r, x), -S(s, y))$

$$\begin{aligned} (r, s, x, y) \star X &= (r^{-1} \circ r, s^{-1} \circ s, x - A(r^{-1}, A(r, x)), y - S(s^{-1}, S(s, y))) \\ &= (id, id, 0, 0) \end{aligned} \quad \text{avec } X \in H.$$

En effet, on a :

$$S(s^{-1}, S(s, y)) = S(s^{-1}, (y_{s(1)}, \dots, y_{s(12)})) = y \text{ et } A(r^{-1}, A(r, x)) = A(r^{-1}, (x_{r(1)}, \dots, x_{r(8)})) = x.$$

$(r, s, x, y) \star ((r', s', x', y') \star (r'', s'', x'', y'')) = ((r, s, x, y) \star (r', s', x', y')) \star (r'', s'', x'', y'')$  parce que  $(r \circ r') \circ r'' = r \circ (r' \circ r'')$  et  $(\mathbb{Z}, +)$  est un groupe.

Cependant, en général  $r \circ r' \neq r' \circ r$ .

$(H, \star)$  est donc un groupe non-abélien.

**Proposition 6.**  $(G, \star)$  est un sous-groupe de  $(H, \star)$ .

Preuve :

–  $G \subset H$  (proposition précédente)

–  $(id, id, 0, 0) \in G$

– Soit  $((r, s, x, y), (r', s', x', y')) \in G^2$   $(r', s', x', y')^{-1} = (r'^{-1}, s'^{-1}, -A(r', x'), -S(s', y')) \in G$

En effet,  $\varepsilon(r') = \varepsilon(r'^{-1}) = \varepsilon(s') = \varepsilon(s'^{-1})$  et par définition,  $-A(r', x') \equiv 0[3]$ ,  $-S(s', y') \equiv 0[2]$

Donc  $(r, s, x, y) \star (r'^{-1}, s'^{-1}, -A(r', x'), -S(s', y')) \in H$  et

$$\begin{aligned} \varepsilon(r'^{-1} \circ r) &= \varepsilon(r'^{-1})\varepsilon(r) = \varepsilon(s'^{-1})\varepsilon(s) \\ &= \varepsilon(s'^{-1} \circ s) \end{aligned}$$

D'où  $(r, s, x, y) \star (r'^{-1}, s'^{-1}, -A(r', x'), -S(s', y')) \in G$

Alors :  $(G, \star)$  est un sous-groupe de  $(H, \star)$ .

$G$  est appelé **groupe du Rubik's Cube**.

**Proposition 7** (utile pour les algorithmes). *Deux permutations commutent si elles agissent sur des ensembles disjoints.*

## 2 Les algorithmes du cube

### 2.1 L'intérêt des mathématiques

Les mathématiques jouent un rôle important dans l'élaboration d'algorithmes.

En effet, grâce à la loi  $\star$ , nous allons pouvoir prévoir l'ensemble des positions à partir des mouvements qui les ont engendrées. Ainsi, avec certitude, nous saurons ce qu'une suite de mouvement entraînera comme changements. Le but étant ainsi de pouvoir montrer qu'il existe des algorithmes, et que ceux-ci se terminent. C'est un bien vaste programme.

Avant de se lancer dans la découverte des quelques manipulations de base, nous allons préciser les notations utilisées. Pour les indices de rotation, les notations restent les mêmes qu'en table 1, pour mémoire, nous la réécrivons également. La table 3 nous informera quant à elle des permutations engendrées par les mouvements élémentaires.

Avant de se lancer dans la résolution du cube, une question se pose. **Le cube peut-il se résoudre à partir de n'importe quelle position ?**

Pour pouvoir répondre à cette question, il est important de savoir ce qu'est une position. Elle peut se décrire comme une permutation des sommets et des arêtes avec leurs indices de

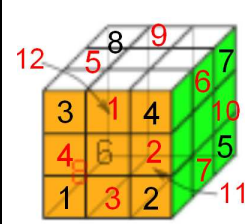
	Q	Indice de rotation des sommets	Indice de rotation des arêtes
		(1,2,3,4,5,6,7,8)	(1,2,3,4,5,6,7,8,9,10,11,12)
F		(0,0,0,0,0,0,0,0)	(1,1,1,1,1,1,1,1,1,1,1,1)
B		(0,0,0,0,0,0,0,0)	(1,1,1,1,1,1,1,1,1,1,1,1)
R		(0,-1,0,1,1,0,-1,0)	(1,-1,1,1,-1,-1,1,1,-1,1,1)
L		(1,0,-1,0,0,-1,0,1)	(1,1,1,-1,-1,1,1,-1,1,1,-1)
T		(0,0,1,-1,0,0,1,-1)	(1,1,1,1,1,1,1,1,1,1,1,1)
D		(1,1,0,0,-1,-1,0,0)	(1,1,1,1,1,1,1,1,1,1,1,1)

TABLE 2 – Récapitulatif des indices de rotation

Q	Permutation des arêtes	Permutation des sommets
F	(1 2 3 4)	(1 3 4 2)
B	(9 10 11 12)	(5 6 8 7)
R	(6 10 7 2)	(2 4 7 5)
L	(4 5 12 8)	(1 3 8 6)
T	(1 6 9 5)	(3 4 7 8)
D	(7 11 8 3)	(1 2 5 6)

TABLE 3 – Récapitulatif des permutations

rotation respectifs. Une position se note alors  $[\sigma, \mathcal{M}_A, \mathcal{M}_S] \in G$  et comme  $G$  est un groupe, chaque élément possède un inverse. Finalement, si on applique cet inverse, nous retrouverons le cube fait. Ainsi, le cube **peut être résolu** depuis n'importe quelle position ! C'est pourquoi nous allons pouvoir tenter de trouver un algorithme pour le résoudre dans n'importe quel cas.

## 2.2 Algorithmes de bases et conséquences

Cette section s'articulera autour de deux axes, dans un premier temps, il conviendra de prouver que l'on peut faire une face du cube et ensuite nous nous attarderons à trouver un mouvement générateur du reste du cube.

### Faire une face

Posons que la face que nous choisissons de faire est de couleur **C**. Nous la positionnons alors vers le haut. Ensuite nous choisissons une face du cube possédant un cube arête (**A**) mal positionné. Par une rotation de cette dernière, nous plaçons le cube secondaire avec la couleur **C** sur la dernière couronne. Il nous faut alors tourner la face **D** pour positionner **A** sur la face dont le cube central est de la même couleur que lui (en effet, le cube a deux faces, une de couleur **C** et une autre). Puis nous retournons la face d'origine de **A**. Ensuite une rotation de  $180^\circ$  suffit à faire passer **A** sur la première couronne.

Maintenant, nous répétons cette opération trois nouvelles fois, et nous avons quatre cubes arêtes aux bons endroits. Le passage à prouver dans cet algorithme est le fait qu'un cube placé reste au bon endroit après une série de mouvement. Le seul mouvement qui pourrait déplacer un cube déjà en place serait la rotation d'une des quatre faces sur le côté du cube. Cependant, si un cube (**A**) est bien placé et que l'on doit tourner cette face, c'est qu'elle possède un autre cube de couleur **C**. Ce cube (**B**) ne peut occuper la même place que le premier, un mouvement de  $45^\circ$  direct ou indirect suffira alors à placer le cube sur la dernière couronne. Il s'ensuit une rotation de la face **D** sur lequel notre cube **A** n'est pas. Le mouvement qui consiste alors à faire tourner la face d'origine du cube permet de replacer notre cube **A** et le cube **B** retrouve le même emplacement qu'auparavant.

Une fois les cubes arêtes correctement placés, il suffit de corriger leur indice de rotation pour

qu'ils soient alors dans la bonne position. Pour cela, nous devons choisir un cube avec un indice de rotation non nul. Nous allons le faire passer sur la dernière couronne en faisant tourner de  $180^\circ$  la face frontale<sup>5</sup>. Il est donc sur la dernière couronne. Ensuite, nous devons faire une rotation de la face **D** de  $90^\circ$  horaire. Il suffit alors de faire une rotation de la couronne entre la face gauche et droite de  $90^\circ$  dans le sens anti-horaire suivi à nouveau d'un quart de tour anti-horaire de la face **D** qui remet le cube secondaire sur la face frontale. Enfin, il suffit de tourner la couronne centrale de  $90^\circ$  dans le sens horaire pour finir l'inversion. Cet algorithme est représenté en figure 1, sans tenir compte des couleurs, le cube est simplement inversé.

Pour faire la preuve de cet algorithme, nous allons changer de méthode. Il suffit de prouver qu'un seul cube secondaire sur la face du dessus a pu se déplacer ou pivoter. Les mouvements effectués ne pourraient modifier que le cube opposé à celui que l'on souhaite déplacer. Cependant, les seules opérations susceptibles de le changer sont les rotations de la couronne centrale, lesquelles le laisse sur la face du dessus. Cette face n'étant pas modifiée entre ces deux rotations, le cube revient alors à sa place.

De façon empirique, nous constatons que le cube que nous souhaitons inverser s'est effectivement inversé. La rotation de la face frontale de  $180^\circ$  n'entraîne aucun changement d'indice<sup>6</sup>, notre cube a donc toujours un indice de rotation de 1. La rotation **D** dans le sens horaire ou anti-horaire ne modifie pas non plus l'indice de rotation de ce cube. Ce sont alors les rotations des couronnes centrales qui permettent ce changement. En effet, ces rotations ont pour indice de rotation des arêtes :  $(-1, 1, -1, 1, 1, 1, 1, 1, -1, -1)$ <sup>7</sup>. Comme notre cube ne subit qu'une fois cette rotation, son indice sera modifié de 1. Parfait, l'indice devient nul, le cube est alors inversé. Notre

5. On considère dorénavant que le cube secondaire était sur la face frontale. Si tel n'était pas le cas, il suffit de faire tourner le cube entre ses mains.

6. Confère table 2

7. On constate que cela est possible, la somme modulo 2 donne bien 0.

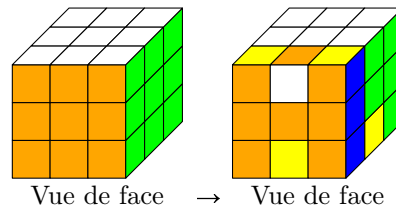


FIGURE 1 – Représentation du cube après l'algorithme 2.



rotation de la couronne centrale est représentée par la permutation des arêtes :  $\begin{pmatrix} 9 & 11 & 3 & 1 \end{pmatrix}$ . Ainsi, pour nous assurer que notre cube est revenu à sa place, regardons  $\sigma$ , la permutation de l'algorithme.

$$\sigma = \begin{pmatrix} 9 & 11 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 7 & 11 & 8 & 3 \end{pmatrix}^{-1} \circ \begin{pmatrix} 9 & 11 & 3 & 1 \end{pmatrix}^{-1} \circ \begin{pmatrix} 7 & 11 & 8 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}^2$$

Ainsi :  $\sigma(1) = 1$ . C'est ce que nous souhaitons.

Au bout de quatre fois au plus, le cube dispose d'une croix, quatre cubes sont bien placés. Nous procédons de même pour les cubes sommets, aucune explication de plus n'est nécessaire. Ainsi, nous pouvons nous retrouver avec une face complète.

### Une formule pour le finir...

Maintenant que nous avons notre première face, nous pouvons nous consacrer à un tout autre mouvement. Notre objectif est de pouvoir tourner une pièce sur elle-même ou d'en échanger deux. Comme nous l'avons déjà signalé, la théorie mathématique nous indique qu'il n'est pas possible de faire ses mouvements sans sacrifier d'autres pièces. C'est un problème que nous tenterons de résoudre après avoir trouver nos algorithmes. La formule que nous obtiendrons à la fin sera appelée formule d'Arnaud Maes.

Notons  $X$  une suite de mouvements qui stabilise tous les éléments de la face supérieure et change l'indice de rotation d'un cube. Pour cela, nous pouvons utiliser un algorithme semblable au 2.  $X^{-1}$  représentera les manipulations telles que  $X \star X^{-1} = (id, id, \mathcal{M}_0, \mathcal{M}_0)$ . Finalement  $X = (\sigma_S, \sigma_A, (a, b, 1, 1, c, d, 1, 1), (-1, e, f, g, 1, 1, h, i, 1, j, k, l))$ , avec  $(a, b, c, d, e, f, g, h, i, j, k, l) \in \{-1; 1\}^{12}$  tels que  $X \in G$ . Soit  $T$ , la rotation de la face supérieure d'un quart de tour.  $X$  peut se décomposer en deux mouvements,  $X = Y \star Z$  avec  $Y$  une transformation des éléments autres que ceux de la première face et  $Z$  l'inversion du cube de la première face. Ainsi  $Y$  et  $Z$  agissent sur des supports disjoints. L'algorithme que nous cherchons à faire est alors :  $X \star T \star X^{-1} \star T^{-1}$ . Comme le groupe n'est pas abélien, nous ne pouvons dire que cette transformation est l'application identique. En effet, nous avons une transformation  $M = X \star T \star X^{-1} \star T^{-1} = Y \star Z \star T \star Z^{-1} \star Y^{-1} \star T^{-1}$ . Comme  $Y$  travaille sur un ensemble disjoint à  $T$  ou à  $Z$ , elle commute avec

ces derniers (**Proposition 6**). Ainsi :

$$M = Z \star T \star Z^{-1} \star T^{-1}$$

Cela signifie que  $M$  **retourne deux cubes arêtes de la face supérieure et conserve le reste du cube.**

Avec le même raisonnement, on prouve que si  $X$  échange deux sommets, deux arêtes ou tourne un sommet, alors il est possible de tourner deux coins ou d'échanger trois (voire quatre) cubes de la face supérieure sans détruire le reste du cube.

### 2.3 Algorithme de résolution

La résolution du cube est maintenant proche. Nous pouvons faire une face et échanger les cubes que nous souhaitons à l'aide d'une séquence bien choisie. Cependant, le cube n'est pas encore résolu. Les deux premiers algorithmes proposés permettent de faire une face. Procédons par ordre. Dans un premier temps, nous allons mettre les cubes arêtes de la seconde couronne en place. Pour cela, il suffit d'utiliser la séquence convenable donnée par l'algorithme d'Arnaud Maes.

Après avoir positionné les cubes arêtes aux bons endroits (ce qui est faisable, aucune preuve n'est nécessaire), nous réglons un problème. En effet, si ces cubes sont à la bonne place, il ne reste plus que 8 cubes à placer correctement, et ils sont sur la même face ! Ainsi, nous pouvons placer correctement les sommets puis les arêtes. Si les sommets ne peuvent pas être mis à la bonne place, c'est qu'un cube secondaire de cette face doit être inversé. Une séquence du type :  $M \star M \star B \star B \star M \star M$  avec  $M$  la rotation d'une couronne du milieu permet la transposition entre deux cubes arêtes et règle alors le problème que nous avons avec les cubes sommets<sup>8</sup>. Il suffit alors de remettre ces cubes dans la bonne position en faisant uniquement changer leurs indices de rotation. Et pour la même raison que précédemment, cette manipulation se termine car le cube est sensé être soluble depuis n'importe quelle position. Comme il existe un algorithme ne changeant que les indices de rotation **le cube peut alors se finir.**

---

8. Il s'agissait en fait d'un problème de parité. Faire la transformation proposée permet de rajouter une inversion.

## Conclusion

Pour conclure, nous pouvons dire qu'en effet le cube est un objet mathématique, peut-être un des seuls représentants concrets de la théorie des groupes. Ainsi, grâce à ses nombreuses propriétés, nous avons pu proposer des algorithmes permettant la résolution du cube par étape. Le cube jusqu'alors extrêmement difficile à résoudre sans techniques particulières perd toute sa complexité. Cependant, des recherches se poursuivent encore aujourd'hui et certains défis ne sont pas encore résolus. Par exemple, le nombre de mouvements minimum nécessaire a été trouvé, cependant l'algorithme de « Dieu » permettant sa résolution en un minimum de mouvements n'a pas encore été trouvé...

Quoi qu'il en soit, le Rubik's Cube reste encore un objet rempli de mystères....

## Bibliographie

Pour réaliser ce document, je me suis principalement appuyé sur des données disponibles sur internet vu le faible nombre de documents papier. La première partie mathématique est le fruit de lecture sur de nombreux sites tels Wikipedia[5], ou encore des sites de passionnés ou enseignants[1][3]. Les preuves ont toutes été refaites sauf celle sur les indices de rotation des sommets[6]. La seconde partie est le fruit d'une lecture attentive d'un document sur la création d'algorithmes « maisons »[2][4].

## Références

- [1] Pierre Colmez. Le rubik's cube, groupe de poche, Mai 2010.
- [2] Arnaud Maes. Comment résoudre n'importe quel puzzle de type rubik, Mai 2007.
- [3] Philippe Picart. Théorie des groupes et rubik's cube, 2001.
- [4] Jaap Scherphuis. Jaap's puzzle, 1999-2011.
- [5] Wikipedia. Rubik's cube, 2004-2011.
- [6] Wikipedia. Théorie mathématique sur le rubik's cube, 2006-2011.