

Les mathématiques du cube de Rubik
Club mathématique, Université de Montréal
Le 6 avril 2011
Matilde N. Lalín–Université de Montréal¹

1 Le cube de Rubik



Le cube de Rubik est un casse-tête inventé en 1974 par le hongrois Ernő Rubik. Il s'agit d'un cube dont chaque face est divisée en neuf petits cubes ou pièces qui peuvent tourner de façon indépendante. Le cube est composé d'un axe central portant les centres des 6 faces, de 8 pièces coins et de 12 pièces arêtes. Il y a 54 petits carrés colorés qui correspondent aux faces extérieures des pièces. À l'état initial, chaque face du cube de Rubik est d'une couleur homogène et différente des autres, mais la rotation indépendante de chaque face provoque un mélange des pièces coins et arêtes.

Le but du jeu est, après avoir mélangé les six faces, de manipuler le cube pour tenter de lui rendre son apparence d'origine, avec les six faces de couleurs unies.

2 Le groupe de mouvements

2.1 Les mouvements fondamentaux

Les mouvements fondamentaux sont les rotations des faces [S81]. On les décrit de la façon suivante:

- D = rotation d'un quart de tour dans les sens direct (ou sens horaire) de la face droite.
- H = rotation d'un quart de tour dans les sens direct de la face haute.
- G = ... face gauche.
- A = ... face avant.
- P = ... face postérieure.
- B = ... face basse.

2.2 La combinaison de mouvements

Soient X et Y deux mouvements. Alors XY dénote «faire X , puis faire Y ». Par exemple, $X^2 = XX$ «faire X deux fois consécutives ». On dénote avec 1 le mouvement «ne rien faire ». Deux mouvements sont égaux s'ils ont le même effet sur le cube, par exemple, $H^4 = 1$.

¹mlalin@dms.umontreal.ca – <http://www.dms.umontreal.ca/~mlalin>

3 Groupes

Un groupe est un ensemble \mathcal{G} avec une opération $*$

$$\mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}$$

telle que

- $(a * b) * c = a * (b * c)$ (associativité).
- Il y a un élément $e \in \mathcal{G}$ tel que $\forall a \in \mathcal{G}, e * a = a * e = a$ (identité).
- $\forall a \in \mathcal{G}, \exists a^{-1} \in \mathcal{G}$ tel que $a * a^{-1} = a^{-1} * a = e$ (inverse).

Un groupe \mathcal{G} est dit abélien si

$$a * b = b * a \quad \forall a, b \in \mathcal{G}.$$

Par exemple, les entiers \mathbb{Z} , avec la somme, sont un groupe (la identité est 0 et l'inverse de x est $-x$). Les nombres réels sans zéro $\mathbb{R} \setminus \{0\}$, avec la multiplication, sont un groupe. L'ensemble de matrices non-singulières avec la multiplication est un groupe non-abélien.

Les mouvements du cube de Rubik, avec l'opération qu'on a décrit, forment un groupe qu'on appelle \mathcal{R} .

4 Propriétés de \mathcal{R}

Soit X un mouvement de \mathcal{R} . Alors, X^{-1} est le mouvement qui défait X . Si on a une suite de mouvements, pour trouver l'inverse il faut défaire chaque mouvement en ordre inverse:

$$(X_1 X_2 \dots X_n)^{-1} = X_n^{-1} \dots X_2^{-1} X_1^{-1}.$$

«L'inverse de vous mettre vos chaussettes et ensuite vous mettre vos chaussures est d'abord enlever vos chaussures et ensuite enlever vos chaussettes. »[H11].

On observe aussi que la opération n'est pas commutative. Par exemple,

$$AH \neq HA.$$

Alors, \mathcal{R} n'est pas abélien. Il y a des mouvements qui commutent, comme $HB = BH$. Si X et Y affectent des pièces différentes, ils commutent. D'abord on fait X . Ensuite, on fait Y . On ne change aucune de pièces qui ont été changées par X . Quand on fait X^{-1} , ça retourne sur place toutes les pièces que X avait changées sans affecter les pièces qui ont été changées par Y . Enfin, on fait Y et ça retourne toutes les pièces sur place.

«Se mettre sa chaussure gauche commute avec se mettre sa chaussure droite.»[H11]

5 Sous-groupes

Étant donné un groupe \mathcal{G} , un sous-groupe \mathcal{H} est un sous-ensemble qui est encore un groupe avec l'opération de \mathcal{G} . C'est-à-dire que

- $e \in \mathcal{H}$,

- $a, b \in \mathcal{H} \Rightarrow a * b \in \mathcal{H}$,
- $a \in \mathcal{H} \Rightarrow a^{-1} \in \mathcal{H}$.

\mathcal{R} a plusieurs sous-groupes, par exemple

$$\mathcal{H}_A = \{A, A^2, A^3, A^4 = 1\}.$$

On peut définir un sous-groupe en donnant un sous-ensemble S de \mathcal{G} et on dit que \mathcal{H} est le sous-groupe engendré par S si \mathcal{H} est le plus petit sous-groupe de \mathcal{G} qui contient S . Par exemple, \mathcal{H}_A est le sous-groupe engendré par A .

Une caractéristique importante des groupes et sous-groupes est l'ordre, qui est le nombre des éléments du groupe. L'ordre maximum d'un élément sur \mathcal{R} est $2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 = 1260$. Un exemple est $DH^2B^{-1}PB^{-1}$ ([B82]).

Voici une table avec quelques sous-groupes et son ordre (voir [B82, D06, FS82])

Générateurs	Ordre
D^2	2
D	$4 = 2^2$
D^2, G^2	$4 = 2^2$
D^2, G	$8 = 2^3$
D, G	$16 = 2^4$
D^2, H^2 (les deux carrés, $\simeq D_{12}$)	$12 = 2^2 \cdot 3$
D^2, H	$14400 = 2^6 \cdot 3^2 \cdot 5^2$
D, H (lié à $PGL(2, \mathbb{F}_5)$)	$73483200 = 2^6 \cdot 3^8 \cdot 5^2 \cdot 7$
D^2, G^2, H^2	$96 = 2^5 \cdot 3$
D, G, H	$159993501696000 = 2^{14} \cdot 3^{13} \cdot 5^3 \cdot 7^2$
D^2, A^2, H^2	$2592 = 2^5 \cdot 3^4$
D, A, H	$170659735142400 = 2^{18} \cdot 3^{12} \cdot 5^2 \cdot 7^2$
D^2, G^2, H^2, B^2	$192 = 2^6 \cdot 3$
D^2, G^2, H^2, A^2	$165888 = 2^{11} \cdot 3^4$
D^2, G^2, A^2, P^2, H^2 (les carrés)	$663552 = 2^{13} \cdot 3^4$
D^2, G^2, A^2, P^2, H	$19508428800 = 2^{16} \cdot 3^5 \cdot 5^2 \cdot 7^2$
D^2, G^2, A, P, H	$21119142223872000 = 2^{16} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$
D, G, A, P, H	$43252003274489856000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11$
$AP^{-1}, DG^{-1}, HB^{-1}$ (sandwich)	$768 = 2^8 \cdot 3$
AP, DG, HB (anti-sandwich)	$6144 = 2^{11} \cdot 3$

Noter que

$$B = D^2G^2H^2D^2P^2D^2G^2A^2G^2H^{-1}D^2G^2H^2D^2P^2D^2G^2A^2G^2H^2,$$

$$B^2 = D^2A^2P^2G^2H^2D^2A^2P^2G^2.$$

Alors il suffit avec 5 mouvements fondamentaux pour engendrer \mathcal{R} .

Théorème 1 ([B82]) *Le groupe \mathcal{R} contient tous les sous-groupes d'ordre < 13 , et tous les sous-groupes non-abéliens d'ordre < 26 . Le plus petit groupe qui n'est pas sous-groupe de \mathcal{R} est $\mathbb{Z}/13\mathbb{Z}$ et le plus petit groupe non-abélien qui n'est pas sous-groupe de \mathcal{R} est D_{26} .*

5.1 Superflip

Il y a un mouvement très spécial qui s'appelle superflip:

$$S = HD^2APDP^2DH^2GP^2DH^{-1}B^{-1}D^2AD^{-1}GP^2H^2A^2.$$

Superflip tourne chaque pièce arête sur elle-même.



Le centralisateur $\mathcal{Z}(\mathcal{G})$ d'un groupe \mathcal{G} est l'ensemble d'éléments qui commutent avec tous les éléments du groupe.

$$\mathcal{Z}(\mathcal{G}) = \{f \in \mathcal{G} \mid fg = gf \quad \forall g \in \mathcal{G}\}.$$

$\mathcal{Z}(\mathcal{G})$ est toujours un sous-groupe de \mathcal{G} (et il est égal à \mathcal{G} si et seulement si \mathcal{G} est abélien).

Le centralisateur de \mathcal{R} est donné par

$$\mathcal{Z}(\mathcal{R}) = \{1, S\},$$

un sous-groupe d'ordre 2.

6 Permutations

On peut penser aux mouvements du cube comme permutations des pièces. Si on a un ensemble fini $\{1, 2, \dots, n\}$, on utilise la notation des cycles pour décrire les permutations de cet ensemble. Par exemple,

$$(12)(345)$$

Ici, tous les nombres sont différents. Ça veut dire qu'on fait $1 \leftrightarrow 2$, et $3 \rightarrow 4$, $4 \rightarrow 5$, et $5 \rightarrow 3$.

On peut faire la multiplication

$$(612)(34) * (124)(35) = (16)(2354)$$

Le groupe de permutations de l'ensemble X est noté comme \mathbb{S}_X (groupe symétrique).

L'ordre d'une permutation est le plus petit entier positif k tel que si on répète la permutation k fois, tout reste invariant. Par exemple, (123) a ordre 3. Les cycles d'ordre 2 s'appellent transpositions. Une permutation est paire (impaire) si elle se décompose en un nombre pair (impair) de transpositions:

$$\text{impaires} \quad (12), (1234) = (14)(13)(12)$$

$$\text{paires} \quad (123) = (13)(12)$$

Les permutations paires forment un sous-groupe noté \mathbb{A}_X (groupe alterné).

\mathbb{A}_X est engendré par les 3-cycles.

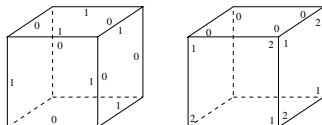
Pour être plus précis, on fait la distinction entre les permutations des pièces, et leur orientations. Alors, on suit la notation de [B00, B82]. Soient

$$\Pi_A = \{a_1, \dots, a_{12}\}$$

l'ensemble des 12 pièces arêtes et

$$\Pi_C = \{c_1, \dots, c_8\}.$$

l'ensemble des 8 pièces coins. Alors $\Pi = \Pi_A \cup \Pi_C$ est l'ensemble des pièces. Chaque pièce arête peut avoir deux orientations qu'on dénote $\{0, 1\}$. Pour les pièces coins, les orientations sont $\{0, 1, 2\}$. On suit la notation de la figure suivante.



Alors, on peut décrire les positions du cube comme

$$(\sigma, \tau, x, y) \quad \sigma \in \mathbb{S}_{\Pi_A}, \tau \in \mathbb{S}_{\Pi_C}, x \in \{0, 1\}^{12}, y \in \{0, 1, 2\}^8.$$

Théorème 2 ([B82]): (σ, τ, x, y) est possible ssi

- σ et τ sont toutes les deux paires ou toutes les deux impaires.
- 2 divise $x_1 + \dots + x_{12}$.
- 3 divise $y_1 + \dots + y_8$.

Chaque mouvement fondamental est un 4-cycle sur les pièces arêtes et un 4-cycle sur les pièces coins.

Corollaire 3

$$\mathcal{R} \simeq ((\mathbb{S}_{12} \times \mathbb{S}_8) \cap \mathbb{A}_{20}) \times ((\mathbb{Z}/2\mathbb{Z})^{11} \times (\mathbb{Z}/3\mathbb{Z})^7).$$

Théorème 4 Le nombre des positions est

$$\frac{1}{2} 12! \cdot 8! \cdot 2^{11} \cdot 3^7 = 43252003274489856000 \sim 4.3 \times 10^{19}$$

Les pièces arêtes peuvent s'interchanger entre elles avec 12! possibilités et le même pour les pièces coins avec 8! possibilités, mais la permutation finale doit être paire, alors il faut diviser par 2. Chaque pièce arête a deux orientations, mais il est impossible de changer l'orientation d'une pièce arête seule, alors, ça donne 2^{11} possibilités. Chaque pièce coin a 3 orientations possibles et de même on ne peut changer une pièce coin seule, alors 3^7 possibilités.

Si on fait un mouvement par seconde, on a besoin de 1.37×10^{12} ans pour faire toutes les permutations, c'est-à-dire, 100 fois l'âge de l'univers.

Corollaire 5 Si on démonte le cube de Rubik et on le remonte au hasard, on a une chance sur douze de pouvoir le résoudre.

7 Quelques sous-groupes naturels de la théorie de groupes

7.1 Supergroupe

Si les faces centrales ont des dessins non-symétriques, il faut tenir en considération les rotations des pièces et on obtient un groupe plus grande qui s'appelle le Supergroupe $\widehat{\mathcal{R}}$. Le supergroupe est plus grande que \mathcal{R} . On a [FS82]

$$2^{11}|\mathcal{R}| = 88580102706155225088000 \sim 8.9 \times 10^{22}$$

7.2 Stabilisateurs

Le stabilisateur d'un ensemble X est le sous-groupe de mouvements que laisse l'objet fixé.

$$\text{Stab}(X) = \{g \in \mathcal{G} \mid g \cdot x = x\}.$$

On a

- Le stabilisateur d'une face a ordre $8! \cdot 4 \cdot 3 \cdot 2^7 \cdot 3^3 = 1672151040$.
- Le stabilisateur des pièces arêtes a ordre $\frac{8!}{2} \cdot 3^7 = 44089920$.
- Le stabilisateur des pièces coins a ordre $\frac{12!}{2} \cdot 2^{11} = 490497638400$.

8 Commutateurs

Étant donnés deux éléments a et b d'un groupe \mathcal{G} , on peut former le commutateur

$$[a, b] = aba^{-1}b^{-1}.$$

On trouve que $[a, b] = 1$ si et seulement si a et b commutent.

Le sous-groupe commutateur $\mathcal{K}(\mathcal{G})$ est le sous-groupe engendré par les $[a, b]$.

On a que

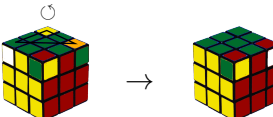
$$\mathcal{K}(\mathcal{R}) = \{(\sigma, \tau, x, y) \in \mathcal{R} \mid \sigma, \tau \text{ paires}\}.$$

Si X et Y sont des mouvements du cube qui n'affectent pas les mêmes pièces alors $[X, Y] = 1$

Propriété 6 [H11] *S'il y a une seule pièce qui est permuté par X et Y à la fois, alors $[X, Y]$ donne un 3-cycle, $[X, Y]^3 = 1$.*

On peut contrôler le nombre de pièces affectées par $[X, Y]$ de cette façon.

Exemple:

$$[HDH^{-1}, G^{-1}] = HDH^{-1}G^{-1}HD^{-1}H^{-1}G \text{ fait}$$


9 Conjugaison

Étant donnés deux mouvements X et Y , on peut faire la conjugaison de X par Y :

$$XYX^{-1}.$$

XYX^{-1} et X sont dits conjugués.

Mouvements conjugués ont le même effet sur le cube, mais sur endroits différents.

10 Nombre de mouvements pour résoudre le cube

Les algorithmes de résolution les plus populaires ont besoin environ de 60-70 mouvements pour résoudre le cube quelle que soit la position de départ. En janvier 1995, Michael Reid a prouvé que superflip a besoin de au moins 20 mouvements [S95]. En juillet 2010, Morley Davidson, John Dethridge, Herbert Kociemba et Tomas Rokicki ont annoncé qu'il suffit avec 20 mouvements [DDKR10]. Ce nombre s'appelle «nombre de Dieu».

11 Les méthodes de résolution

11.1 La méthode couche par couche

- Compléter une face, par exemple la face basse, en prenant bien soin de placer correctement la couronne (placer les pièces entourant cette face) et les pièces centrales.

- Faire premièrement une croix.



- Compléter les coins.



- Faire la deuxième couche (la rangée horizontale à mi-hauteur).

- $HDH^{-1}D^{-1}AD^{-1}A^{-1}D$



→



- $H^{-1}A^{-1}HAHDH^{-1}D^{-1}$



→



- Placer les pièces arêtes de la face supérieure à leur place et les orienter correctement.

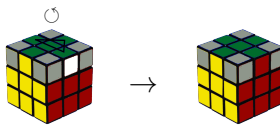
- $PGHG^{-1}H^{-1}P^{-1}$



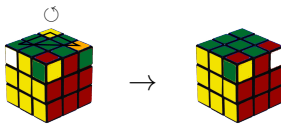
→




(plusieurs fois)

$$- DHD^{-1}HDH^2D^{-1}$$


- Placer les pièces coins à leur place et les orienter correctement.

$$- [HDH^{-1}, G^{-1}] = HDH^{-1}G^{-1}HD^{-1}H^{-1}G$$


$$- [D^{-1}BDABA^{-1}, H] = D^{-1}BDABA^{-1}HAB^{-1}A^{-1}D^{-1}B^{-1}DH^{-1}$$




11.2 Méthodes Corners First (Guimond, Ortega, Waterman)

- Placer et orienter les pièces coins.
- Placer et orienter les pièces arêtes de deux faces opposées.
- Résoudre la couche intermédiaire.

11.3 Méthode d'Ofapel

- Compléter une face.
- Compléter la face opposée à celle déjà correcte. Il faut d'abord placer correctement toutes les pièces coins, puis les orienter correctement, et enfin mettre les pièces arêtes.
- Par échanges, amener chaque pièce arête restante à sa place.
- Enfin orienter les 4 bords correctement.

11.4 La méthode de Lars Petrus

Moins intuitif. La résolution prend en moyenne 60 mouvements.

- Faire un «petit cube» de $2 \times 2 \times 2$ de 3 couleurs.
- Étendre le «petit cube» à un parallélépipède de $2 \times 2 \times 3$ sans jamais détruire le petit cube.
- Orienter les arêtes restantes.
- Étendre l'objet $2 \times 2 \times 3$ à un objet $2 \times 3 \times 3$ (c'est-à-dire deux couches du cube complet), sans jamais détruire ce qui a été fait auparavant.
- Placer et orienter les 4 pièces coins restantes.
- Et enfin, placer et orienter les 4 pièces arêtes restantes.

11.5 La méthode de Jessica Fridrich

Systematique. Utilisée en speedcubing.

- Réaliser une croix sur une face.
 - Créer les quatre paires constituées d'un arête et d'un coin qui lui correspond afin de les insérer une à une sur la face de départ, le but étant de finir les deux premiers étages.
 - Réaliser l'OLL (orientate last layer), c'est-à-dire orienter les cubes de la dernière face.
 - Réaliser la PLL (permute last layer), c'est-à-dire remplacer les cubes de la dernière face.
- Il faut apprendre de nombreuses séquences (57 pour l'OLL et 21 pour la PLL)

11.6 Les méthodes de Thistlethwaite, Kociemba, Korf

Se fondent sur des sous-groupes, d'utilisation théorique. Soient $\mathcal{G}_0 = \langle G, D, A, P, H, B \rangle$, $\mathcal{G}_1 = \langle G, D, A, P, H^2, B^2 \rangle$, $\mathcal{G}_2 = \langle G, D, A^2, P^2, H^2, B^2 \rangle$, $\mathcal{G}_3 = \langle G^2, D^2, A^2, P^2, H^2, B^2 \rangle$, $\mathcal{G}_4 = I$. L'idée est qu'on commence avec \mathcal{G}_0 . On étudie les quotients droites $\mathcal{G}_{i+1} \setminus \mathcal{G}_i$ et détermine une suite de mouvements qui envoie chaque co-ensemble sur \mathcal{G}_{i+1} . Alors, on combine les mouvements pour aller de \mathcal{G}_0 à \mathcal{G}_1 , de \mathcal{G}_1 à \mathcal{G}_2 , etc., jusqu'à \mathcal{G}_4 . Les quotients $\mathcal{G}_{i+1} \setminus \mathcal{G}_i$ sont assez petits, le plus grande est $\mathcal{G}_2 \setminus \mathcal{G}_1$ qui a 1082565 éléments. La version originale du algorithme a au plus 52 mouvements.

11.7 La méthode du tournevis

References

- [B82] Christoph Bandelow, Inside Rubik's Cube and Beyond, Birkhäuser Boston, 1982.
- [B00] Ed Blakey, The Group Theory Behind Rubik's Cube. Bachelor monograph, Oxford, 2000.
- [D06] Tom Davis, Group Theory via Rubik's Cube, 2006.
- [FS82] Alexander Frey, Jr and David Singmaster, Handbook of Cubik Math, Enslow, 1982
- [H11] Michael Hutchings. The Mathematics of Rubik's cube, presentation at the Julia Robinson Mathematics Festival, UC Berkeley, 2011.
- [DDKR10] <http://www.cube20.org>
- [S81] David Singmaster, Notes on Rubik's Magic Cube, Enslow, 1981.
- [S95] http://www.math.rwth-aachen.de/~Martin.Schoenert/Cube-Lovers/michael_reid_superflip_requires_20_face_turns.html