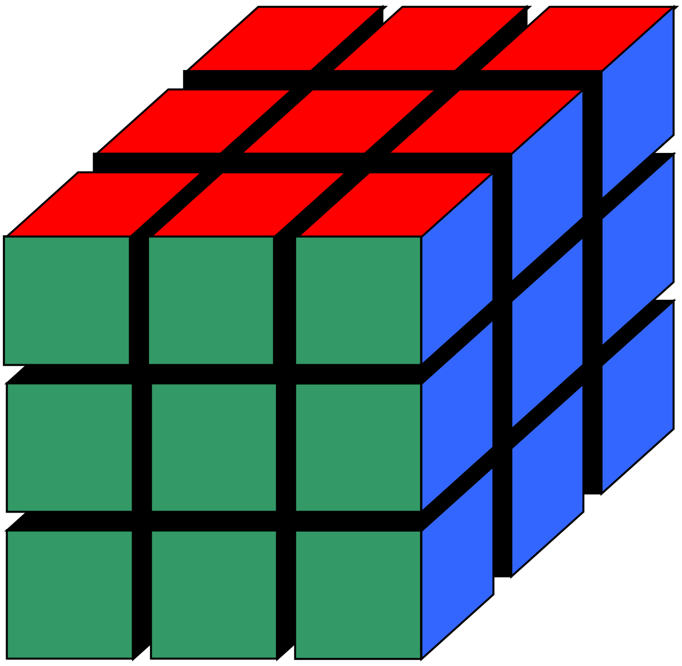
Rubik's Cube



Présentation :

Le Rubik's Cube est composé de 20 cubes mobiles (8 cubes sommet et 12 cubes arête) et 6 cubes immobiles (1 au centre de chaque face).
Le cube au centre d'une face peut en fait pivoter sur lui-même, mais cela n'affecte en rien le Rubik's Cube classique (certains cubes possèdent des motifs dessinés sur chaque face, et l'orientation du centre prend alors de l'importance).

Chaque cube sommet porte 3 facettes (dites facettes sommet), chaque cube arête 2 (dites facettes arête), chaque centre 1.
Il y a donc $8 \times 3 + 12 \times 2 = 48$ facettes mobiles sur le Rubik's Cube.

Voici une représentation possible du Rubik's Cube :

						1	2	3			
						4	U	5			
						6	7	8			
9	10	11	12	13	14	15	16	17	18	19	20
21	B	22	23	L	24	25	F	26	27	R	28
29	30	31	32	33	34	35	36	37	38	39	40
						41	42	43			
						44	D	45			
						46	47	48			

Le choix de la numérotation des facettes n'est pas important, il ne sert qu'à illustrer la modélisation mathématique que l'on va effectuer.
Le nom des faces est en anglais car c'est la notation la plus utilisée dans les publications concernant le Rubik's Cube.

U : up	haut
D : down	bas
L : left	gauche
R : right	droite
F : front	avant
B : back	arrière

Cette notation est justifiée si l'on considère que les centres de chaque face ne bougent pas, c'est à dire que le Rubik's Cube ne change jamais d'orientation.
Pour des raisons de pratique, c'est rarement vrai lorsque l'on manipule le cube, mais il est indispensable de l'imposer pour ébaucher la théorie.

Toutes les manipulations du Rubik's Cube peuvent être réalisées à partir de 6 mouvements simples : un quart de tour de chaque face dans le sens des aiguilles d'une montre (en regardant cette face).
U, D, L, R, F, B représentent les mouvements simples des faces correspondantes.

Modélisation mathématique :

Appelons G l'ensemble des mouvements ou manœuvres possibles sur le Rubik's Cube, une manœuvre étant la succession d'un nombre fini de mouvements simples. Dotons G de la loi interne "suivi de". (G, "suivi de") est clairement un magma. Par exemple : (U suivi de D) est bien une manœuvre sur le Rubik's Cube et donc un élément de G. La loi "suivi de" est associative (mais non commutative), il existe un élément neutre que l'on appellera Identité (Id) qui consiste à ne rien faire, et chaque élément de G admet un symétrique dans G (par exemple, le symétrique de U est la manœuvre qui consiste à faire un quart de tour dans le sens inverse des aiguilles d'une montre, qui est aussi (U suivi de U suivi de U). L'associativité de la loi permet évidemment de supprimer les parenthèses sans créer d'ambiguïté.).
Il apparaît alors que (G, "suivi de") est un groupe (non abélien).

Les symétriques de U, D, L, R, F, B seront notés respectivement U', D', L', R', F', B'. L'associativité de la loi permet aussi sans ambiguïté la notation x^n pour désigner l'itéré n-ième de tout élément x de G.

Une autre approche consiste à considérer que chaque manœuvre sur le Rubik's Cube est en fait une permutation sur l'ensemble des 48 facettes mobiles du Rubik's Cube. On peut alors considérer G comme le sous-groupe du groupe symétrique S_{48} engendré par les 6 éléments U, D, L, R, F et B, soit G = < U, D, L, R, F, B >. La loi "suivi de" est remplacée ici par la loi de composition classique de deux fonctions (attention : U suivi de D $\Leftrightarrow$ U D $\Leftrightarrow$ D o U). S_{48} est un groupe fini d'ordre 48!, donc G est un groupe fini dont l'ordre divise 48!.

C'est évidemment cette approche qui sera la plus productive car elle permet notamment d'envisager des permutations n'appartenant pas à G et d'expliquer ainsi certaines propriétés que les amateurs du Rubik's Cube connaissent bien comme l'impossibilité de permuter deux cubes arête sans toucher au reste.

Remarque :

L’ensemble des cubes sommet et l’ensemble des cubes arête étant stables par tout élément de G, il sera également possible de considérer G comme un sous-groupe de $S_{24} \times S_{24}$. L’ordre de G divise donc $(24\ !)^2$.

Abréviations :

CA : cube arête
CS : cube sommet
On pourra désigner un cube sommet par les trois faces auxquelles il appartient (ULF est le cube sommet appartenant aux faces U, L et F).
Les huit cubes sommets sont donc : ULF, URF, URB, ULB, DLF, DRF, DRB, DLB.
De même, on pourra désigner un cube arête par les deux faces auxquelles il appartient (RF est le cube arête appartenant aux faces R et F).
Les douze cubes arête sont donc : FD, FR, FU, FL, LD, LU, RU, RD, BD, BL, BU, BR.

Définitions :

F_A = ensemble des facettes arête
F_S = ensemble des facette sommet
Card (F_A) = Card (F_S) = 24

$H_A = \{ g \in G / \forall x \in F_S, g(x) = x \} = \text{Stab} (F_S)$ = ensemble des manœuvres qui n'affectent que les facettes arêtes
$H_S = \{ g \in G / \forall x \in F_A, g(x) = x \} = \text{Stab} (F_A)$ = ensemble des manœuvres qui n'affectent que les facettes sommet

Remarque : H_A et H_S sont clairement des sous-groupes de G.

$$\varphi_S : \begin{array}{l} G \rightarrow S_8 \\ g \rightarrow g_s \end{array}$$

g_s étant la permutation des CS induite par g.

De même :

$$\varphi_A : G \rightarrow S_{12}$$
$$g \rightarrow g_a$$

g_a étant la permutation des CA induite par g.

Il faut noter que g_s et g_a ne concernent que les cubes mobiles et non les facettes de ces cubes. Il est donc important que g soit un élément de G et non de S_{48} (un élément quelconque de S_{48} pouvant disperser les facettes d'un cube ce qui est évidemment impossible pour un élément de G). De plus ces définition ne sont acceptables que dans la mesure où tout élément de G transforme un cube sommet (resp. arête) en un autre cube sommet (resp. arête).
φ_S et φ_A sont des homomorphismes de groupe (trivial).

$$\varphi_{SA} : \quad G \rightarrow S_8 \times S_{12}$$
$$g \rightarrow (\varphi_S(g), \varphi_A(g))$$

Si l'on munit $S_8 \times S_{12}$ de la loi $\bullet$ telle que pour $f = (f_1, f_2)$ et $h = (h_1, h_2)$ deux éléments de $S_8 \times S_{12}$, $f \bullet h = (f1 \circ h1, f2 \circ h2)$, alors $(S_8 \times S_{12},\bullet)$ est un groupe et φ_{SA} est un homomorphisme de groupe.

Ces trois homomorphismes de groupe ont un intérêt évident. En déterminant leur image, on détermine en même temps les permutations des cubes mobiles permises par les éléments de G (c'est à dire les manœuvres réalisables sur le Rubik's Cube, en ne tenant compte que des cubes mobiles et pas de leur orientation).

Détermination des images de φ_S, φ_A et φ_{SA} :

Im(φ_S) = S_8

De par la définition même de φ_S, il est évident que Im(φ_S) $\subset S_8$.
Il suffit donc de montrer que tout élément de S_8 est l'image d'un élément de G par φ_S. Comme S_8 est engendré par les transpositions, il suffit même de montrer que toute transposition de S_8 est l'image d'un élément de G par φ_S.

Considérons tout d'abord la manœuvre M = R F' R' F D F D' F' D'.
Un calcul pénible ou une simple manipulation du Rubik's Cube permet de constater que φ_S(M) est une transposition des cubes sommet DLF et DRF.
Les différentes symétries du Rubik's Cube permettent d'obtenir à partir de M toutes les transpositions de deux cubes sommet adjacents (c'est à dire deux cubes sommet ayant exactement deux faces en commun).
Les transpositions entre deux cubes sommet ayant une seule face en commun (comme DLF et URF) peuvent être obtenues par composition de deux transpositions de cubes adjacents ((DLF, DRF) et (DRF, URF)).
Les transpositions entre deux cubes sommet n'ayant aucune face en commun (comme DLF et URB) peuvent être obtenues par composition de trois transpositions de cubes adjacents ((DLF, DRF), (DRF, URF) et (URF, URB)).

Il est évidemment possible de donner une démonstration mathématique rigoureuse de ce résultat (notamment en utilisant les symétries), mais cela est relativement pénible compte tenu de l'évidence du résultat.

Le fait que Im(φ_S) contiennent toutes les transpositions de S_8 et les propriétés d'homomorphisme de groupe de φ_S amènent alors naturellement la conclusion : $S_8 \subset$ Im(φ_S). CQFD

$\underline{\mathrm{Im}(\varphi_A) = S_{12}}$

La démarche est totalement similaire à la démonstration précédente.
On a clairement $\mathrm{Im}(\varphi_A) \subset S_{12}$ et on veut montrer que toute transposition de S_{12} est l'image d'un élément de G par φ_A.
Considérons la manœuvre M de la démonstration précédente. $\varphi_A(M)$ est une transposition des cubes arête DR et DB.
On obtient de même toutes les autres transpositions avec des considérations de symétrie.

$\underline{\mathrm{Im}(\varphi_{SA}) = \{ (x, y) \in S_8 \times S_{12} / \varepsilon(x) = \varepsilon(y) \}}$

Posons $E = \{ (x, y) \in S_8 \times S_{12} / \varepsilon(x) = \varepsilon(y) \}$
On a aussi $E = \{ (x, y) \in S_8 \times S_{12} / \varepsilon(x) \times \varepsilon(y) = 1 \}$
(ε désigne la signature d'une permutation et $\varepsilon(x) \in \{-1 ; 1\}$)

Montrons que $\mathrm{Im}(\varphi_{SA}) = E$
$\mathrm{Im}(\varphi_{SA}) = \{ f \in S_8 \times S_{12} / \exists\, g \in G \text{ tel que } f = \varphi_{SA}(g) \}$

♦ $\mathrm{Im}(\varphi_{SA}) \subset E$

$$\begin{aligned} s : \quad & S_8 \times S_{12} \to \{-1 ; 1\} \\ & (x, y) \to \varepsilon(x) \times \varepsilon(y) \end{aligned}$$

s est un homomorphisme de groupe.

Il faut donc montrer : $\forall g \in G,\ s(\varphi_{SA}(g)) = 1$

Soit $h \in \{U ; U' ; D ; D' ; L ; L' ; R ; R' ; F ; F' ; B ; B'\} \subset G$
$\varphi_S(h)$ est un 4-cycle donc $\varepsilon(\varphi_S(h)) = (-1)^3 = -1$
$\varphi_A(h)$ est un 4-cycle donc $\varepsilon(\varphi_A(h)) = (-1)^3 = -1$
d'où $s(\varphi_{SA}(h)) = 1$

Or $g \in G = \langle U, D, L, R, F, B \rangle$ donc $s(\varphi_{SA}(g)) = 1$ (on utilise le fait que φ_S, φ_A et φ_{SA} sont des homomorphismes de groupe et le fait que G est l'ensemble des composés finis des éléments U, D, L, R, F, B et de leurs symétriques). CQFD

♦ $E \subset Im(\varphi_{SA})$

Il faut montrer : $\forall (x, y) \in E, \exists g \in G$ tel que $\varphi_{SA}(g) = (x, y)$

<u>1[er] cas :</u> $\varepsilon(x) = \varepsilon(y) = 1$

On a donc $(x, y) \in A_8 \times A_{12}$
A_n étant le groupe alterné d'ordre n.
$A_n = \{ x \in S_n / \varepsilon(x) = 1 \}$
Rappelons le résultat général suivant : pour $n \geq 3$, A_n est engendré par les 3-cycles (pour le montrer, il suffit de rappeler que tout élément de A_n est le produit d'un nombre pair de transpositions distinctes 2 à 2, et de montrer que tout produit de 2 transpositions distinctes est un 3-cycle ou le produit de 2 3-cycles).

Montrons alors que $\forall x \in A_8, \exists g \in G$ tel que $\varphi_S(g) = x$
Nous avons dit que $x = \Pi_i x_i$ où $\forall i$, x_i est un 3-cycle de A_8.

Soit $C_1 \in G$ tel que $\varphi_S(C_1)$ soit un 3-cycle de S_8 et $C_1 \in H_S = Stab(F_A)$.
Un tel élément existe, par exemple L U' L' D L U L' D'.
φ_S(L U' L' D L U L' D') = (URB, LBD, RBD).
On prendra donc pour simplifier C_1 = L U' L' D L U L' D'

$\forall i$, $x_i = (CS_1, CS_2, CS_3)$ où CS_1, CS_2 et CS_3 désignent les 3 CS non invariants par x_i.
Comme $Im(\varphi_S) = S_8$, on peut assurer que :
$\exists a_i \in G$ tel que :
♦ $(\varphi_S(a_i))(CS_1)$ = URB
♦ $(\varphi_S(a_i))(CS_2)$ = LBD
♦ $(\varphi_S(a_i))(CS_3)$ = RBD

On voit donc que $x_i = \varphi_S(a_i^{-1} \circ C_1 \circ a_i)$ et que $\varphi_A(a_i^{-1} \circ C_1 \circ a_i) = Id$

D'où $x = \varphi_S(\Pi_i (a_i^{-1} \circ C_1 \circ a_i))$ et $\varphi_A(\Pi_i (a_i^{-1} \circ C_1 \circ a_i)) = Id$

De même, montrons que $\forall y \in A_{12}, \exists g \in G$ tel que $\varphi_A(g) = y$
Nous avons dit que $y = \Pi_i y_i$ où $\forall i$, y_i est un 3-cycle de A_{12}.

soit $C_2 \in G$ tel que $\varphi_A(C_2)$ soit un 3-cycle de S_{12} et $C_2 \in H_A = Stab(F_S)$.
Un tel élément existe, par exemple B' R' B2 D2 F2 L' F2 D2 B'.
φ_A(B' R' B2 D2 F2 L' F2 D2 B') = (UL, UB, UR).
On prendra donc pour simplifier C_2 = B' R' B2 D2 F2 L' F2 D2 B'

$\forall i$, $y_i = (CA_1, CA_2, CA_3)$ où CA_1, CA_2 et CA_3 désignent les 3 CA non invariants par y_i.
Comme $Im(\varphi_A) = S_{12}$, on peut assurer que :
$\exists b_i \in G$ tel que :
- $(\varphi_A(b_i))(CA_1) = UL$
- $(\varphi_A(b_i))(CA_2) = UB$
- $(\varphi_A(b_i))(CA_3) = UR$

On voit donc que $y_i = \varphi_A(b_i^{-1} \circ C_2 \circ b_i)$ et que $\varphi_S(b_i^{-1} \circ C_2 \circ b_i) = Id$
D'où $y = \varphi_A(\Pi_i (b_i^{-1} \circ C_2 \circ b_i))$ et $\varphi_S(\Pi_i (b_i^{-1} \circ C_2 \circ b_i)) = Id$

D'où la conclusion que pour $g = \Pi_i (a_i^{-1} \circ C_1 \circ a_i) \circ \Pi_i (b_i^{-1} \circ C_2 \circ b_i)$,
$\varphi_S(g) = x$ et $\varphi_A(g) = y$, soit $\varphi_{SA}(g) = (x, y)$. CQFD

<u>2ème cas :</u> $\varepsilon(x) = \varepsilon(y) = -1$

$\varepsilon(\varphi_S(U)) = \varepsilon(\varphi_A(U)) = -1$, donc $\varepsilon(\varphi_S(U)x) = \varepsilon(\varphi_A(U)y) = 1$
D'après le cas précédent :
$\exists h \in G$ tel que $\varphi_{SA}(h) = (\varphi_S(U)x, \varphi_A(U)y)$.
$\varphi_{SA}(U'h) = ((\varphi_S(U')\varphi_S(U)x, \varphi_A(U')\varphi_A(U)y) = (x, y)$
D'où la conclusion que pour $g = U'h$,

$\varphi_S(g) = x$ et $\varphi_A(g) = y$, soit $\varphi_{SA}(g) = (x, y)$. CQFD

<u>Conclusion</u>

Cette petite étude permet de montrer que, si l'on ne tient pas compte de l'orientation des cubes mobiles mais seulement de leur position, toutes les configuration sont possibles pour les cubes sommet, ainsi que pour les cubes arête. Cependant, toutes les configurations de cubes mobiles ne sont pas pour autant possibles, les cubes sommet (resp. arête) ne pouvant prendre la place de cubes arête (resp. sommet) et les permutations induites sur les cubes sommet et celles sur les cubes arête devant avoir la même signature.

Applications :

- On ne peut transposer deux cubes sommet sans modifier l'agencement des cubes arête,
- On ne peut transposer deux cubes arête sans modifier l'agencement des cubes sommet.

∀∃≅≤↔←→≥×≠≡∩∪⊃⊇⊄⊂⊆∈∉⇔⇐⇒φψ∅•εΠ