Le groupe du Rubik's Cube
(Tome II)

La connaissance est le patrimoine de l'humanité, donc chaque être humain peut l'utiliser librement mais il a aussi le devoir de le protéger, partager, améliorer.

Morphocode CODE

Titre: Le groupe du Rubik's Cube (Tome II)

Auteur: Morphocode CODE

Site web: https://fan2cube.fr

Version: 17.3-24.6.14

ISBN **:** 979-8-4488-4544-4

Préface

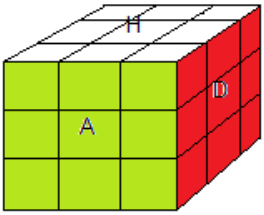
Ce livre est la suite du livre “Le groupe du Rubik’s Cube (Tome I)” du même auteur.

1 L'ORBITE

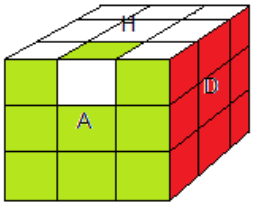
Si vous jouez l'Helicopter ou récemment Curvy Copter vous savez en gros ce que c'est une "orbite". Dans l'Helicopter, il y a 4 orbites pour les centres, chaque' orbite contient 6 centres et les rotations de l'Helicopter déplacent ces centres dans leur orbite.

En Rubik's Cube vous avez aussi les orbites !! mais il est assez rare et peu d'articles en parlent sur ce sujet.

Commençons par quelques observations
Voici deux états du Cube: l'état e_{000} = e (formule I) c'est l'état résolu , l'état e_{100} (rotation étendue Γ) on a enlevé (HA), pivotée puis la remet.



l'état e_{000} = résolu

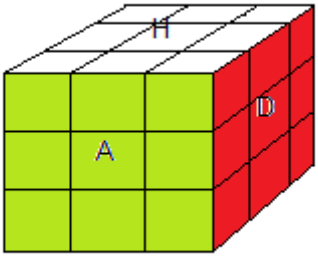


l'état e_{100}

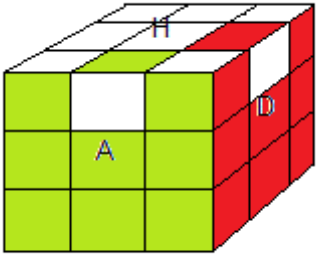
Prenons l'état e_{000}, à partir de cette état on mélange le Cube avec les 6 rotations de base {H,B,A,P,G,D} on obtient un nouveau état disons μ, l'ensemble de tous les états formés à partir de e_{000}, forme ce qu'on appelle l' orbite G_{000} (il y a 43252003... états dans cette orbite).

On fait de même pour état e_{100}, à partir de cette état on mélange le Cube avec les 6 rotations de base {H,B,A,P,G,D} on obtient un nouveau état disons ν, l'ensemble de tous les états formés à partir de e_{100}, forme ce qu'on appelle l' orbite G_{100} (il y a aussi 43252003... états dans cette orbite).

On peut toujours passer d'un état à un autre dans la même orbite (par des rotations de base) , mais on ne peut pas passer 2 états dans des orbites différentes , on peut passer de μ à e_{000} et de ν à e_{100} mais pas de μ à ν .
Par ex l'état γ est dans l' orbite G_{000} car on peut passer de γ à e_{000}



l'état e_{000}

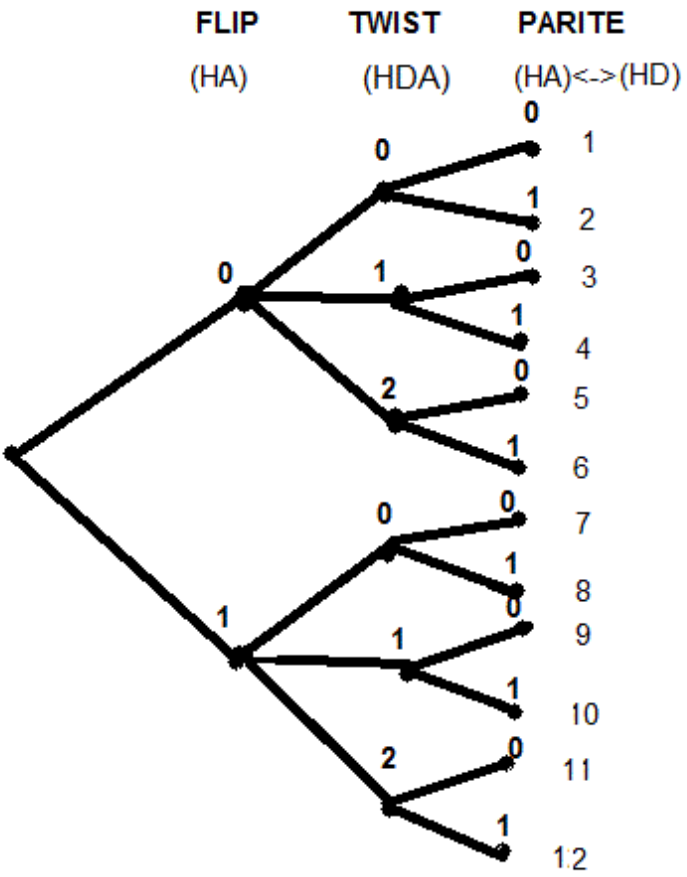


l'état γ est dans l' orbite G_{00}

La question vient naturellement à l'esprit c'est combien d' orbites en a -t- on ?
La réponse se trouve dans les 3 lois fondamentales du Rubik's Cube, on sait qu'on ne peut pas passer d'une orbite à une autre comme par ex on ne peut pas passer l'état e_{100} à l'état e_{000}, donc il suffit de violer les lois du Rubik's Cube pour trouver les orbites !!

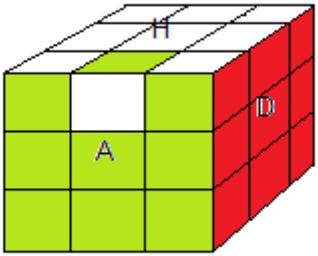
On note e_{ftp} l'état ou l' orbite (ftp) f=flip, t=twist, p=parité e_{111} signifie:

1. On enlève l'arête (HA), renverse puis la remet ; (f=1)
2. On enlève le sommet (HDA), pivote 1/3 tour dans le sens horaire puis le remet ; (t=1)
3. On enlève (HA) et (HD), permute puis les remet ; (p=1)



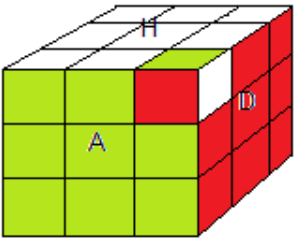
l'arbre des orbites G_{ftp}

1. Violer la loi des flips: Somme des flips = impair

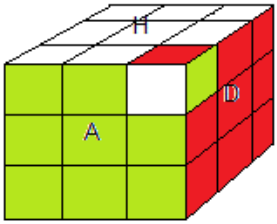


l'état e_{100} (rotation étendue Γ)

2. Violer la loi des twists: Somme des twists = 1,2 (mod 3)

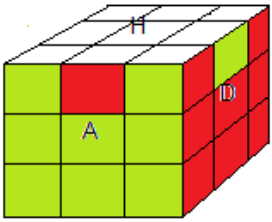


l'état e_{010} (rotation étendue ψ)



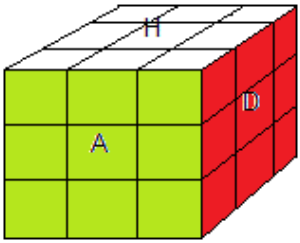
l'état e_{020} (rotation étendue ψ^2)

3. Violer la loi de parité: signature(sommets) ≠ signature(arêtes)

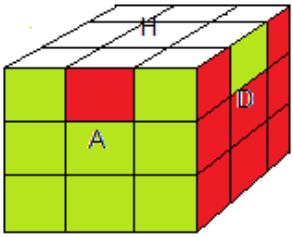


l'état e_{001} (rotation étendue Ω)

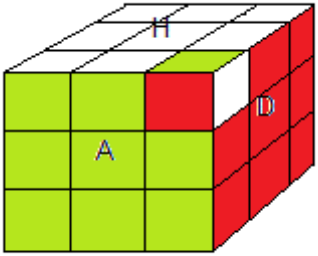
A partir de ces états on fait des combinaisons et on trouve exactement 12 orbites pour le Rubik's Cube.



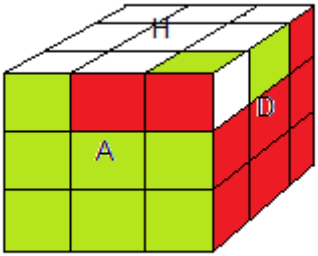
l'état e_{000} = e = résolu
l'orbite G_{000} = G



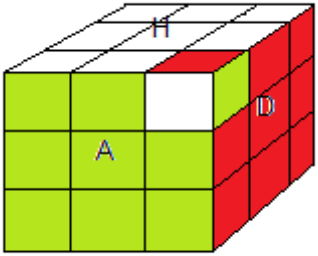
l'état e_{001}
l'orbite G_{001}



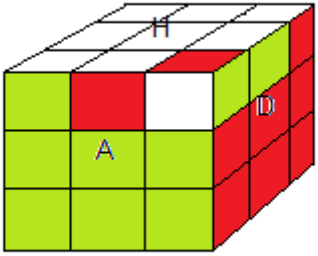
l'état e_{010}
l'orbite G_{010}



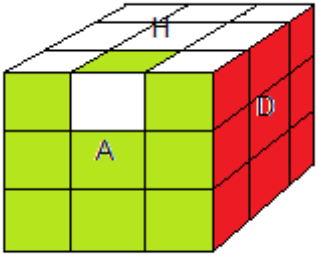
l'état e_{011}
l'orbite G_{011}



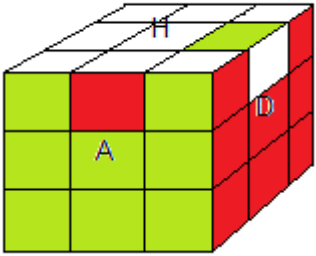
l'état e_{020}
l'orbite G_{020}



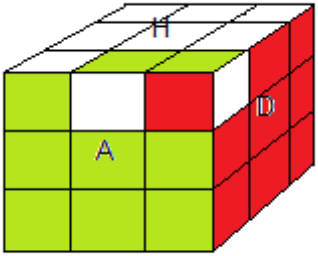
l'état e_{021}
l'orbite G_{021}



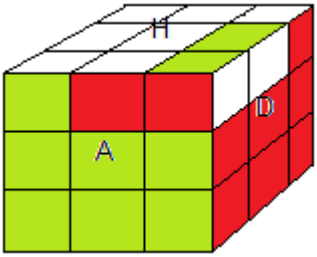
l'état e_{100}
l'orbite G_{100}



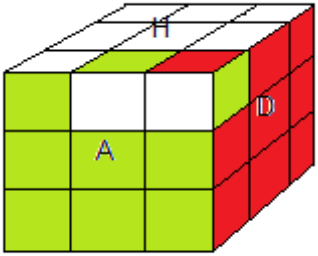
l'état e_{101}
l'orbite G_{101}



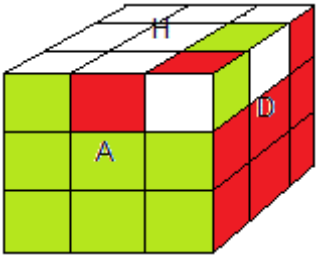
l'état e_{110}
l'orbite G_{110}



l'état e_{111}
l'orbite G_{111}



l'état e_{120}
l'orbite G_{120}



l'état e_{121}
l'orbite G_{121}

Il y a 12 orbites.

On peut retrouver ces 12 orbites par la formule de Burside.

On sait que M agit sur G^+ ($G^+ \bullet M$) et la formule de Burside donne:

$$\mathcal{N} = \frac{1}{|M|}\sum_{V\in M} |F_v|$$

$F_V = \{\mu\in G^+ \mid \mu\bullet V=\mu\}$ = l'ensemble des points fixes de $V\in M$

$\mathcal{N}$ = le nombre d'orbites (on dit aussi le nombre de contraintes, le nombre de choix)

Pour calculer $\mathcal{N}$ on examine les 3 lois du Rubik's Cube.

<u>Théorème fondamentale de la Cubologie</u> :

$\mu = (u,x,v,y)\in G^+$ est un élément de G ssi:

(F) $\sum_{i=1}^{12} x_i = 0 \pmod 2$; abrégé $x = 0 \pmod 2$

(T) $\sum_{i=1}^{8} y_i = 0 \pmod 3$; abrégé $y = 0 \pmod 3$

(P) sig(u) = sig(v)

*La condition (F) montre qu'il y 2 choix (x=0 (mod 2), x=1 (mod 2))
*La condition (T) montre qu'il y 3 choix (y=0 (mod 3), y=1 (mod 3) et y=2 (mod 3))
* La condition (P) : u (2 choix et 1 famille), v (2 choix et 1 famille), et u, v en phase d'où $2^1.2^1/2$ choix .
donc le nombre d'orbites est:

$\mathcal{N}$ = 2 .3 .2 = 12

1.1 UN RAPPEL SUR L'ACTION LIBRE ET COMPATIBLE D'UN GROUPE

¤ $G^+ \bullet M^+$: M^+ agit (à droite) sur G^+
$e \in G^+$ (e = état résolu)

$|G^+| = |M_e^+ \backslash M^+| = |M^+| / |M_e^+|$
$M_e^+ = \{V \in M^+ \text{ tels que } e \bullet V = e\} = \{I\}$; car librement
$|G^+| = |M^+|$

$$\mathcal{N} = \frac{1}{|M^+|} \sum_{V \in M^+} |F_v|$$

$F_v = \emptyset$ si $V \neq I$
$F_I = \{\mu \in G^+ \mid \mu \bullet I = \mu\} = G^+$

tous les autres V n'ont pas de points fixes (car l'action est libre)

$$\mathcal{N} = \frac{|G^+|}{|M^+|}$$

$\mathcal{N} = 1$, on a une seule orbite.

¤ $G \bullet M$: On peut prendre M agit sur G

$e \in G$ (e = état résolu)

$|G| = |M_e \backslash M| = |M| / |M_e|$
$M_e = \{V \in M \text{ tels que } e \bullet V = e\} = \{I\}$
et on trouve
$|G| = |M|$

$$\mathcal{N} = \frac{1}{|M|} \sum_{V \in M} |F_v|$$

$F_I = \{\mu \in G \mid \mu \bullet I = \mu\} = G$

tous les autres V n'ont pas de points fixes

$$\mathcal{N} = \frac{|G|}{|M|}$$

$\mathcal{N} = 1$, on a une seule orbite .

¤ $G^+ \bullet M$: On peut prendre M agit sur G^+

$$\mathcal{N} = \frac{1}{|M|} \sum_{V \in M} |F_v|$$

$F_I = \{\mu \in G^+ \mid \mu \bullet I = \mu\} = G^+$

tous les autres V n'ont pas de points fixes, $V \neq I$, $F_v = \emptyset$

$$\mathcal{N} = \frac{|G^+|}{|M|}$$

Pour trouver $\mathcal{N}$, on regarde les trois lois (F), (T), (P) du Rubik's Cube et on trouve $\mathcal{N}$=2.3.2=12

$$12 = \frac{|G^+|}{|M|}$$

Pour montrer que |M|=|G| on considère l'application suivante :

$\zeta: M \to G$

$V \to \zeta(V) = e \bullet V$

* ζ est surjective car on sait résoudre le Rubik's Cube

$\mu \bullet Q = e$

$\mu = e \bullet Q'$

$\mu = \zeta(Q')$; surjectif

* ζ est injective

$\zeta(V) = \zeta(T)$

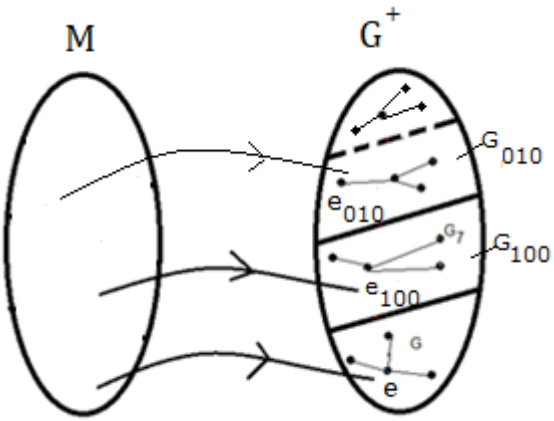
$e \bullet V = e \bullet T \Rightarrow V=T$; axiome3

ζ est bijectif donc $|M| = |G|$

Et finalement

$|G^+| = 12|G|$

NOTE: Suivant l'action on trouve le nombre des orbites est différents:
M^+ agit sur $G^+ \Rightarrow$ 1 orbite
M agit sur $G \Rightarrow$ 1 orbite
M agit sur $G^+ \Rightarrow$ 12 orbites



G⁺•M : G⁺ possède 12 orbites de même taille

on a

$M^+ = < H,B,A,P,G,D,\Gamma,\psi,\Omega >$

$M = < H,B,A,P,G,D >$

$|M^+| = |G^+|$

$|M^+| = 12|M|$

$|M| = |G|$

$|G^+| = 12|G|$

2 L'ALGORITHME THÉORIQUE

La question ... Il y a bien longtemps que je me pose la question suivante:
"Quel est le nombre minimum de formules doit-on mémoriser pour pouvoir restaurer le Cube ?" .
Il est clair que l'algorithme utilisant le moindre formule n'est pas fait pour le SpeedCubing, en SpeedCubing pour allez plus vite on mémorise le maximum de formules possible (environ 119 formules !) ! mais ici la question n'est pas d'économiser le temps mais plutôt d'espace, la mémoire ... par ex on stocke ces formules dans la mémoire d'un ROBOT et c'est lui qui restaurera le Cube avec des algorithmes adéquates.

Mais avant voyons un peu ce que c'est un algorithme

Définition d'un algorithme :

Un algorithme de résolution d'entrée $\mathcal{A}$ est une suite finie d'actions (placer, orienter, ranger, glisser, pivoter, ...) :

À chaque étape de la résolution on peut:

- Tenir le Cube comme on veut

- Utiliser les conjugaisons

- Les formules V utilisées provenant de $\mathcal{A}$

- Des opérations : V', V^n, ${}^tZ$, ${}^tZ^2$, ... (Z=rotation de base)

exemple : $\mathcal{A}$ ={V,C}

A_1: Placer les centres : ($^tD^tH$) V ($^tD^tH$) V' ($^tH'^tD'$) V ($^tH'^tD'$)
A_2: Placer les arêtes : C .G'VG
A_3: Pivoter les sommets : V^4 C'

.....

Autrement dit à chaque étape de la résolution on peut utiliser la conjugaison, l'inverse, la puissance, et on peut tenir le Cube comme on veut.

Posons-nous la question suivante: Combien de formules qu'utilise un algorithme ?

Donc il est raisonnable de dire que le nombre de formules qu'utilise l'algorithme c'est le nombre de formules dans l'entrée pour faire fonctionner l'algorithme.

Certaine partie de la résolution n'a pas besoin de formules , c'est intuitif et on convient de noter cette partie "0" ça signifie "pas besoin de formules, c'est intuitif"

On dit que le Cube est restauré par $\mathcal{A}$, ou résolu par $\mathcal{A}$.

<u>BUT</u> : Trouver $\mathcal{A}$ ayant le moindre formules possibles.

Le groupe des états G du Rubik's Cube est
$G \subset G^+ = (S_{12} \times \mathbb{Z}_2^{12}) \times (S_8 \times \mathbb{Z}_3^8)$

Ceci montre que G comporte 4 composants (4 morceaux) divisant en deux clans: le clan des arêtes ($S_{12} \times \mathbb{Z}_2^{12}$) et le clan des sommets ($S_8 \times \mathbb{Z}_3^8$), chaque clan comporte 2

morceaux: permutations représentées par S, orientations représentées par $\mathbb{Z}$.

Ceci suggère qu'on a 4 étapes de résolution :

1. Placer les arêtes

2. Orienter les arêtes

3. Placer les sommets

4. Orienter les sommets

2.1 LES 4 FORMULES

L'idée c'est d' avoir 4 formules pour les 4 étapes de la résolutions. Avec le programme Cube Explorer (cube514qtm.exe) on trouve les 4 formules suivantes, qui permettent de restaurer le Cube . L'ensemble $\mathcal{A}$ contient donc 4 formules

Alg0(4) :
1. (HA)↔(HD) = DH'DH AB'ABA^2 DAD'A' D'
2. (HA)°(HG)° = ADPGHG'HP'D'A'G'H'GH'
3. (HAG)→(HPD)→(HGP) = DHP'B'PHP'BPH^{2}D'
4. (HAG)$^-$(HGP)$^+$ = G'HD'H'P'D'PGP'DPHDH'

Quand on arrive à l'étape (3), les arêtes sont bien rangées donc bien placées (sig(u)=1), donc sig(v)=1, on peut ainsi placer toutes les sommets avec le 3-cycle (sous entendu et avec la conjugaison).
On a donc un algorithme à 4 formules.

Ces formules sont minimales mais n'ont aucune structure !! on ne comprend rien ce que fait la formule !!!
Donc on peut restaurer le Cube avec 4 formules.
Rappel : le mot "restaurer" est dans le sens que nous avions défini : "il existe un algorithme tel que ..."

Première réduction

On peut réduire $\mathcal{A}$ à 3 éléments, en utilisant W

$W = G'HD'H^2\ GH'G'H^2\ GDH' = (HAG,HDA)(HA,HD)$

On place les arêtes par W, puis on utilise ce même W pour placer les sommets, ce qui est possible parce qu'une fois les arêtes sont bien placées , on aura un nombre pair de couples de sommets à placer (loi de parité) donc on ne dérange pas les arêtes qui sont déjà bien placées.

Alg1(3) :

1. $(HA)\leftrightarrow(HD) = W$
2. $(HAG)\leftrightarrow(HDA) = W$
3. $(HA)^{\circ}(HG)^{\circ} = ADPGHG'HP'D'A'G'H'GH'$
4. $(HAG)^{-}(HGP)^{+} = G'HD'H'P'D'PGP'DPHDH'$

Algorithme à 3 formules .

Deuxième réduction

On voit que les deux dernières lignes (3),(4) pivotent les pièces, on se demande si on peut les remplacer par une seule formule ? la réponse est affirmative, en effet si on renverse 2 fois une arêtes on revient à son état initial, par contre il faut pivoter 3 fois un sommets pour revenir à son

état initial, donc si on trouve une formule qui renverse 2 arêtes et 2 sommet on aura gagné, en voici une :

S = GP'D'PH'AHP'A'DPD'HG'H'D

= $(HA)°(HG)°(HAG)^{-}(HPD)^{+}$

Alg2(2) :
1. $(HA)\leftrightarrow(HD) = W$
2. $(HAG)\leftrightarrow(HDA) = W$
3. $(HA)^{+}(HG)^{+} = S$
4. $(HAG)^{+}(HPD)^{-} = S^2$

On réduit ainsi $\mathcal{A}$ à 2 éléments, on a un algorithme à 2 formules !! C'est vraiment pas mal mais on se demande si on peut faire mieux ? càd d'avoir un algorithme à un élément !!?? et puis si on peut rendre les formules plus compréhensives ? plus structurées ?? la réponse est "oui" .

2.2 LE CROCHET [DH]

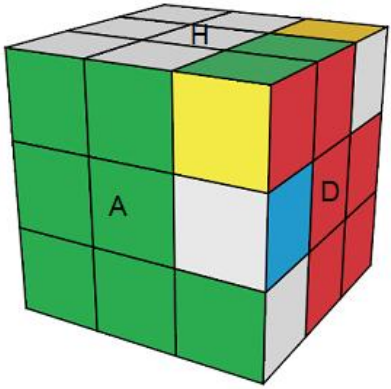
Le problème de ces formules c'est qu'elles n'ont aucune structure, on ne voit rien ce qu'elles font et elles ne sont pas faciles à se retenir !! .

On voudrait donc avoir des formules structurées pour comprendre ce qui se passe, ce que fait la formule et facile à se mémoriser ...

Si on sait restaurer le Cube quand les arêtes en état pair, alors on peut restaurer le Cube à partir de n'importe quel

état (en ajoutant H).
Les états pairs sont gérés par les 3-cycles et comme les commutateurs produisent des 3-cycles c'est pourquoi on va examiner le commutateur [DH], on veut construire un algorithme autour de [DH] c'est-à-dire à chaque étape de résolution il doit apparaître le crochet [DH].

Observons bien ce que fait ce commutateur. [DH] agit sur le Cube comme une sorte de **'Z'** et nous le notons Z = [DH]



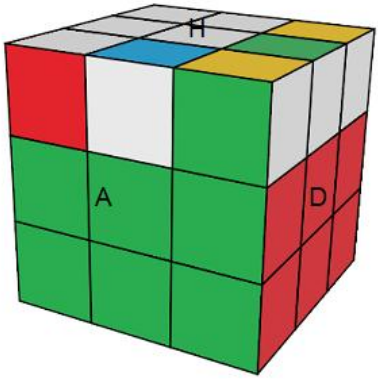
[DH]=(AD,HD,HP)(HDA,BAD)(HGP,HPD)

[DH] agit sur le Cube:
Arêtes : (AD)→(HD)→(HP) = (AD,HD,HP) notation moins lourde !
Sommets : (HDA)↔(BAD).(HGP)↔(HPD) = (HDA,BAD)(HGP,HPD)

[DH]= (AD,HD,HP)(HDA,BAD)(HGP,HPD)

Nous allons construire un algorithme autour du commutateur [DH]. L'idée c'est d'avoir 4 formules "structurées" qui correspondent aux 4 étapes de la résolution :
Et voilà, si on observe bien on a tout ce qui faut!!!

A partir de [DH] si on veut que tout se passe sur la face Haut il suffit de faire A[DH]A' , c'est plus clair et plus propre. A[DH]A' déplace donc 3 arêtes de face Haut



(HA)→(HD)→(HP) = A[DH]A'

Pour orienter les arêtes il suffit de bien observer O=A[DH]A', O laisse une seule bonne arête, on ramène la 2ème bonne arête par H, car on veut seulement avoir 2 mauvaises arêtes c'est-à-dire on prend A[DH]A'.H = J .

J permute 2 arêtes on peut donc utiliser J pour placer toutes les arêtes.

Pour renverser les arêtes on va examiner J de près.

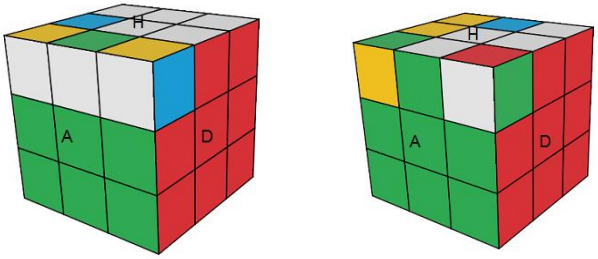
J permute 2 arêtes en effet soient x_1, x_2 , x_3 de la façon suivante:

$$x_1, x_2, x_3 \xrightarrow{J} x_2^+ , x_1, x_3^+$$

x_1, x_2 permutés et x_2^+ pivoté donc il suffit de faire J^2 et on renversera les arêtes :

$$x_1, x_2, x_3 \xrightarrow{J} x_2^+ , x_1, x_3^+ \xrightarrow{J} x_1^+ , x_2^+, x_3^{++} = x_3$$

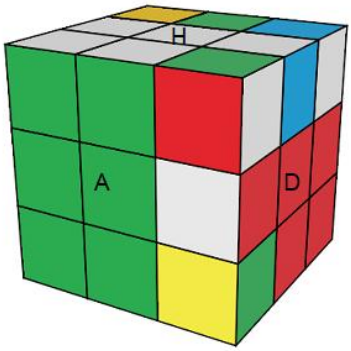
x_1 et x_2 sont donc pivotés
J^2 renverse bien 2 arêtes.



$J = A[DH]A'.H$ $\qquad (HG)^-(HP)^- = (A[DH]A'.H)^2$

Voyons maintenant pour les sommets:

[DH] modifie une seule pièce de la face G, il échange le sommet (HGP) de la face G, avec (HPD) un autre sommet du Cube, on peut facilement fabriquer un 3-cycle-sommets comme ceci:
[[DH],G] = [DH] .G'[HD]G = (HGP)→(HAG)→(HPD)
Q = [DH] .G'[HD]G
Pour orienter les sommets , observons $[DH]^2$:



$[DH]^2$

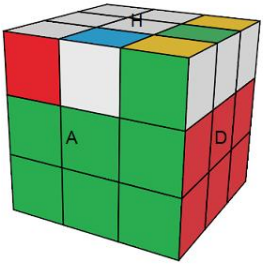
$[DH]^2$ modifie une seule pièce de la face G, il pivote le sommet (HGP) de la face G, il suffit de placer le sommet (HAG) en (HGP) et appliquer l'inverse de $([DH]^2)'=[HD]^2$ pour pivoter 2 sommets :
$[[DH]^2,G] = [DH]^2 .G'[HD]^2G = (HGP)°(HAG)°$
$T= [DH]^2 .G'[HD]^2G$

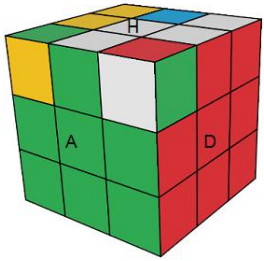
On a donc $\mathcal{A}$ = {J, Q, T}
Et l'algorithme Alg3(3) associé:

1. $(HG)\leftrightarrow(HP) = J$
2. $(HG)^-(HP)^- = J^2$
3. $(HGP)\rightarrow(HAG)\rightarrow(HPD) = Q$
4. $(HGP)^+(HAG)^- = T$

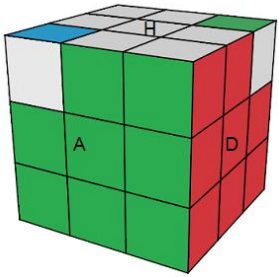
l'étape (3) est possible car les arêtes sont bien placées donc l' état des sommets est pair, donc on peut tous les placer par un 3-cycle.

Ici les formules sont beaucoup plus claires et structurées donc facile à mémoriser et on voit ce que fait une formule; de plus elles sont construites autour de [DH].

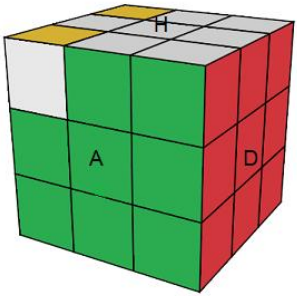




$(HP)\rightarrow(HA)\rightarrow(HD) = A[DH]A'$ $(HG)\cdot(HP)^{-} = (A[DH]A'.H)^{2}$



$(HGP)\rightarrow(HAG)\rightarrow(HPD) = [DH]\ .G'[HD]G$



$(HAG)^{+}(HGP)^{-} = [DH]^2 .G'[HD]^2G$

Remarque : A partir de O, J, Q, T on peut adapter pour avoir un algorithme de résolution tout à fait raisonnable, c'est ce que j'ai fait:

1. Placer les arêtes :
    * Bas: $(HA) \dashrightarrow (BA) = A^2$
    * Équateur: $(HP) \dashrightarrow (AD) = [DH]$
    * Haut: $(HP) \rightarrow (HA) \rightarrow (HD) = A[DH]A' = O$

→ Si on a 2 arêtes adjacentes : tenir le cube (HG), (HA) adjacentes et appliquer HO.
→ Si on a 2 arêtes opposées : tenir le cube (HP), (HA) opposées et appliquer O ⇒ on revient au cas adjacente.

2. Renverser les arêtes: $(HG)°(HP)° = (A[DH]A'.H)^2$
3. Placer les sommets:
    $(HGP) \rightarrow (HAG) \rightarrow (HPD) = [DH] .G'[HD]G$
4. Pivoter les sommets:
    $(HAG)^{+}(HGP)^{-} = [DH]^2 .G'[HD]^2G$

2.3 QUATRE ÉQUATIONS DE LA RÉSOLUTION

1. $(HG)\leftrightarrow(HP) = J$
2. $(HG)^{-}(HP)^{-} = J^2$
3. $(HGP)\rightarrow(HAG)\rightarrow(HPD) = Q$
4. $(HGP)°(HAG)° = T$

On dira aussi les 4 équations de la restauration.
Voilà, on remonte le Cube avec un algorithme construit autour du commutateur [DH], chaque étape on voit apparaître [DH].
a) L'algorithme est simple à comprendre: On place les arêtes puis les oriente. On place des sommets puis les oriente.
b) 3 formules seulement.
c) Les formules sont structurées donc facile à comprendre et mémoriser.

2.4 L'ALGORITHME THÉORIQUE

On a trouvé un algorithme "structuré" à 3 formules, récemment j'ai aperçu qu'on peut encore aller plus loin ...
La formule J = A[DH]A'H est vraiment intéressante, on effet :

1. J permute 2 arêtes et 2 sommets
2. J^2 (ou J^6) renverse 2 arêtes
3. J^4 pivote 3 sommets

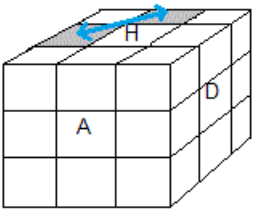
Comme J permute aussi 2 sommets on peut donc l'utiliser pour placer les sommets (après avoir placé les arêtes), et J^4 pivote 3 sommets ce qui permet d'orienter tous les sommets. et voilà c'est merveilleux , on peut tout faire avec J !!...

* On commence par placer toutes les arêtes par J
* Après avoir placer toutes les arêtes, on place alors les sommets grâce à J aussi ! on place (HGP)↔(HDA) (avec la conjugaison) en veillant de ne pas toucher les arêtes (HG) et (HP) c'est-à-dire ne pas utiliser les rotations H, G et P, c'est possible parce que les sommets sont maintenant en état pair (sig(u)=1=sig(v)).
* On renverse les arêtes par J^2 (ou J^6),
* On pivote les sommets par J^4

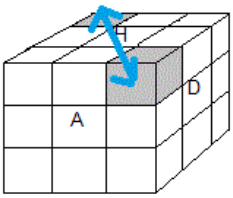
Alléluia !! une seule formule pour restaurer le Cube !!! ...

$\mathcal{A}$ = {J = A[DH]A'.H}
Et l'algorithme théorique associé :

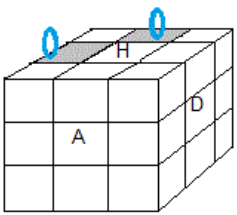
- (HG)↔(HP) = J
- (HGP)↔(HDA) = J
- $(HG)^-(HP)^- = J^2$ (ou J^6)
- $(HGP)^+(HAG)^+(HD)^+ = J^4$



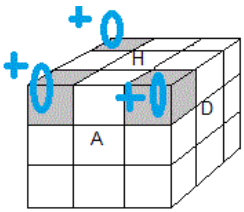
(HG)↔(HP) = A[DH]A'.H



(HGP)↔(HDA) = A[DH]A'.H



$(HG)^{-}(HP)^{-} = (A[DH]A'.H)^{2}$



$(HGP)^{+}(HAG)^{+}(HDA)^{+} = (A[DH]A'.H)^{4}$

Et voilà, il est vraiment extraordinaire qu'on puisse restaurer le Cube avec seulement une formule construite autour d'un seul commutateur [DH] !! C'est incroyable n'est ce pas ?
Cet algorithme en pratique n'est pas vraiment utilisable mais en théorie il peut être très utile, par ex on peut programmer un Robot pour résoudre le Cube, à part l'algorithme, il faut stocker les formules en mémoire, donc si la mémoire coûte chère on peut faire des économies en

utilisant l'algorithme théorique avec une seule formule à stocker.
Remarque : J^4 et J^6 sont propres donc indépendants (l'ordre d'exécution n'intervient pas)
On a 4 équations pour restaurer le Cube , ces équations n'utilise qu'une seule formule J

- (HG,HP) = J
- (HGP,HDA) = J
- $(HG)^-(HP)^- = J^2$
- $(HGP)^+(HAG)^+(HDA)^+ = J^4$

Il est vraiment frappant qu'il y a une analogie avec les 4 équations de Maxwell en électromagnétique

- div(B) = 0
- $\mathrm{rot}(E) = -\frac{\partial B}{\partial t}$
- $\mathrm{div}(E) = \frac{\rho}{\varepsilon}$
- $\mathrm{rot}(B) = \mu j + \varepsilon\mu \frac{\partial E}{\partial t}$

NOTE : On pourrait dire que J et Z=[DH] sont les deux constantes de la structures M, et elles sont reliées par $J = Z^A H$

Finalement l'algorithme théorique est par définition :

- Placer les arêtes : V
- Placer les sommets : V
- Renverser les arêtes : V^2
- Pivoter les sommets : V^4

où V est une formule, la formule V dans l'algorithme théorique est nommé formule première

Application : Suivons la scénario suivante :

Une équipe d'explorateurs se trouve sur Mars, suite à une explosion tout le système de communication est hors circuit, il ne reste plus que le canal SMS pour communiquer avec la Terre. Le système d'oxygène est endommagé et il n'y a plus que 45 minutes pour respirer . Heureusement l'équipage a découvert un système d'oxygène installé par des extra-terrestres mais pour le déclencher il faut résoudre un Rubik's Cube !!! aucun membre de l'équipe sait le résoudre, sauf le Robot R18, bien que le programme de résolution est intact mais le Robot a perdu une partie mémoire de ses données , plus précisément l'entrée d'une formule du Rubik's Cube ...

-Allo! Allo ! la Terre .... Au secours ....

OK, il faut envoyer au Robot une formule ? mais quelle formule ? et puis la communication coûte chère un caractère envoyé coûte 100.000€ !!!

Alors comment faire pour sauver l'équipage en minimum de coût ?

Solution: On envoie au Robot par SMS la formule A[DH]A'H !!!

8 caractères ...

ou Z^AH , seulement 3 caractères si le Robot est équipé la dernière version de l'algorithme de résolution !!

Remarque importante : En Août 2014 Tomas Rokicki et Morley Davidson démontrent le théorème suivant:

$\forall \mu$ état $\exists V$ formule, avec $|V| \leq 26$ telle que $\mu \bullet V = e$

Le problème c'est qu'on ne trouve pas V facilement pour un μ quelconque !!.

C'est donc un problème différent avec l'algorithme théorique. Dans le problème l'algorithme théorique on cherche le nombre minimum de formules à mémoriser pour s'en sortir. Dans le SpeedCubing, pour aller plus vite on mémorise environs 60 à120 formules !!!

Ce nombre 26 est le diamètre du Rubik's Cube (il se nomme aussi le nombre de Dieu) car on peut restaurer le Cube à partir de n'importe quel état au maximum 26 rotations . Il fallait 33 ans pour trouver ce nombre !!

On se demande quels sont des états (les plus loin) qui demandent 26 rotations pour s'en sortir ? Michael Reid a trouvé la formule ci-dessous par ordinateur

$\Pi = H^2B^2G\ A^2\ .H'BD^2\ PH'B'D.\ GA^2D\ HB'\ D'GHA'P'$

et a prouvé que c'est la plus courte formule $|\Pi| = 26$, l'état $e \bullet \Pi = \pi$ est nommé le SuperFlip4Spot, c'est donc l'un des états les plus loin du Rubik's Cube.

Pourquoi on l'appelle SuperFlip4Spot parce que c'est le produit de SuperFlip et 4Spot .

SuperFlip4Spot = SuperFlip . 4Spot = 4Spot . SuperFlip

On ne connaît pas d'autres états de longueur 26, à part ce SuperFlip4Spot !!

On se souvient déjà en Juillet 2010, Tomas Rokicki, Herbert Kociemba, Morley Davidson, et John Dethridge ont démontré que diamètre du Rubik's Cube est 20f ($|A|^2=1$) (30 ans de galère) , ça signifie :

$\forall \mu$ état $\exists V$ formule, avec $|V| \leq 20f$ telle que $\mu \bullet V = e$

Là aussi on cherche des formules les plus loin V avec $|V| = 20f$

* Le SuperFlip φ (12 arêtes retournées) est l'un des états les plus loin en f-rotation, en effet en 1992 Dik .T. WINTER a trouvé une formule du SuperFlip
$\Phi = APH^2DA^2.D^2P^2H'BA.H^2D'G'HP^2.BD^2HP^2H$
de longueur $|\Phi| = 20f$ il fallait attendre jusqu'au 1995 pour que Michael REID démontre que c'est la plus courte formule en f-rotation. En résumé , le SuperFlip est l'un des états les plus loin en f-rotation
Michael REID a trouvé cette formule :

$\Phi = D'H^2PG' .AH'PBA .HB'GB^2 .A'DP'BA' .H'P'HB'$

en 1995 (par ordinateur) pour le SuperFlip (e•Φ=φ) et c'est Jerry BRYAN qui démontre (1995) que c'est la plus courte formule |Φ| = 24 .

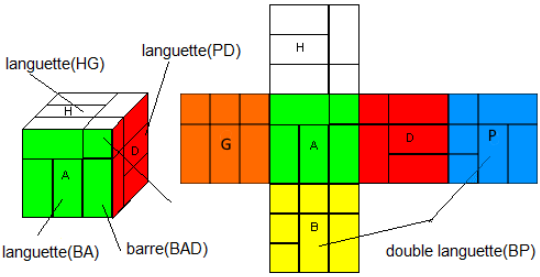
* Le SuperFlip φ joue un rôle important, il est le seul (à part l'identité e) dans le centre de G (le groupe du Rubik's Cube) pour une formule donnée, il est toujours intéressant d' avoir une des plus courte écriture.

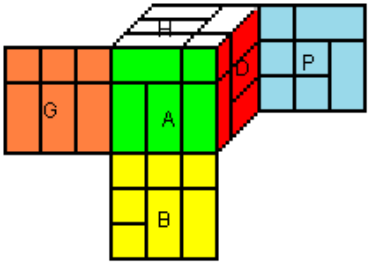
2.5 AUTRES EXEMPLES DE L'ALGORITHME THÉORIQUE

Ici on peut donner 2 exemples de l'algorithme théorique.

Le Bandage Cube

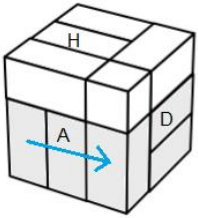
Le Bandage Cube est un bandage du Rubik's Cube inventé par Meffert vers les années 1981.



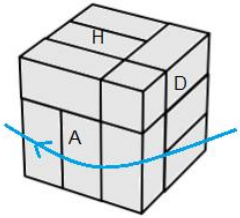


Bandage Cube

Les rotations



B*



^{t}H

Il est étonnant que le Bandage Cube possède un algorithme théorique à 2 formules.

On commence par se placer en position de START.

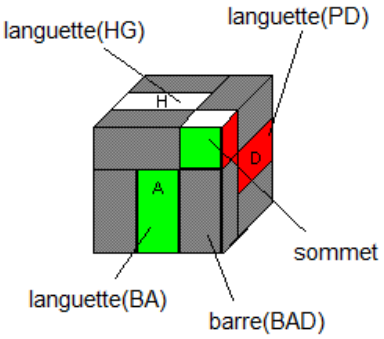
Position START :

1. Le double arête ⌋ doit se trouver dans leur emplacement (BP).

2. Le petit sommet doit se trouver en position (HDA) (même mal orienté, mais il sera bien orienté automatiquement)

3. Les autres arêtes doivent être bien rangées (BG), (PD), (BA), (HG).

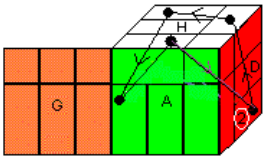
4. Qu'on puisse faire les rotations H,D,A



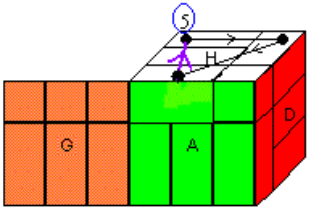
Position START

L'algorithme théorique $\mathcal{A}$ = {Q, T}

On a deux formules:

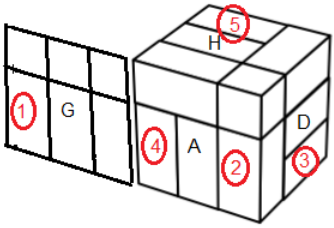


$Q = ADHA\ .D'A^2H'$



$T = A'H .GA'G'A^2.DH'D'$

On range les barres dans l'ordre suivant : (BPG), (BAD), (BDP), (BGA), (HGP)



Range dans cet ordre

1) <u>Placer la barre (BPG)</u> :

Trouver la barre (BPG) (reconnaissable par ses 3 couleurs). Il faut amener cette barre en position (HGP) en utilisant Q ou (${}^tD{}^tH$) Q (${}^tH'{}^tD'$) (quand cette barre se trouve en (BAD))

puis une fois en (HGP) on la place avec : (DB*D') Q (DB*'D')

Explication : La formule Q recouvre le cube sauf 2 zones: (BAD) et (BPG), mais grâce à la conjugaison on arrive bien à placer (BPG)

2) Placer la barre (BAD) :

Trouver la barre (BAD) (reconnaissable par ses 3 couleurs). Il faut amener cette barre en position (BGA) en utilisant Q

puis une fois en (BGA) on la place avec : $({}^{t}H'{}^{t}D')$ Q $({}^{t}D{}^{t}H)$

Remarque : $({}^{t}H'{}^{t}D')$ signifie "tenir le cube comme il faut" avant d'appliquer Q .

3) Placer la barre (BDP) :

Trouver la barre (BDP) (reconnaissable par ses 3 couleurs), rien de compliquer, on la place avec : Q

Remarque : Aucun problème pour déplacer la barre (BDP) à sa place car la barre est dans la zone couverte par Q

4) Placer la barre (BGA) :

Trouver la barre (BGA) (reconnaissable par ses 3 couleurs). Il faut amener cette barre en position (HGP) en utilisant : T

puis une fois en (HGP) on la place avec :

$({}^{t}D{}^{t}H)$ Q $({}^{t}D{}^{t}H)$ Q' $({}^{t}H'{}^{t}D')$ Q $({}^{t}H'{}^{t}D')$

Remarque : Cette formule compliquée permute (BGA,HGP)(HAG,HPD)

5) Placer la barre (HGP) :

Trouver la barre (HGP) (reconnaissable par ses 3 couleurs). On la place avec T (on applique T plusieurs fois s'il le faut) .

Remarque:

- La barre (HGP) est forcement en Haut et T (génère un 3-cycle sommets) couvre tout le Haut donc aucun problème de la déplacer en (HGP).

- Parfois on utilise la formule inverse pour déplacer plus vite, cela dépend où se trouve la barre et où qu'on veut le déplacer. Par ex si on veut

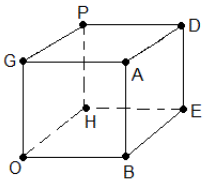
déplacer (HAG) en (BGA) il vaut mieux utiliser Q' que Q.

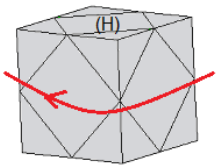
Le Skewb

Le Skewb est un twist assez bien connu, lui aussi possède un algorithme théorique à une formule !

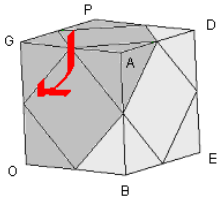
Skewb

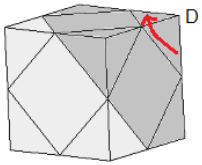
Les rotations :





Rotations ^{t}H





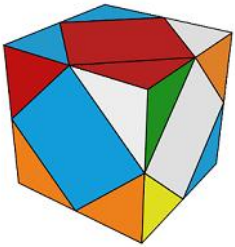
G =120° D=120°

On a choisi Haut=blanc, Avant=vert, Droite=rouge , ...

On se place en position de START

Position START (isoler les sommets)

Les 4 sommets blancs sont en Haut .

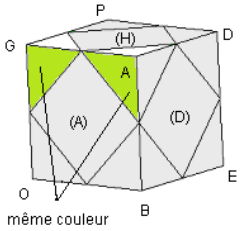


Position START

L'algorithme théorique $\mathcal{A}$ = {[DG']}

A- Placer les sommets Haut

On place correctement les sommets Haut avec [DG']:
A↔P = [DG']



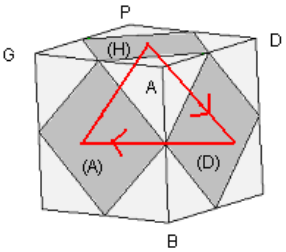
Remarque : Une fois les sommets Haut sont bien placés, les sommets Bas sont automatiquement bien placés.

B- Placer des centres

On déplace les centres (repérés par les sommets) par la formule suivante :

Permutation circulaire de 3 centres :

$(H)\rightarrow(D)\rightarrow(A) = [DG']^2$



$$(H)\rightarrow(D)\rightarrow(A) = [DG']^2$$

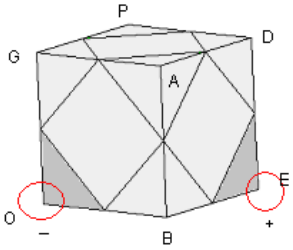
On essaie d'abord de placer le centre Haut (blanc) puis d'avoir 2 centres adjacents à (H). On tient le cube comme il le faut pour appliquer la formule.

<u>C- Pivoter les sommets</u>

Pour cela on utilise la formule suivante:

Pivoter 2 sommets:

$O^{-}E^{+} = [DG']^3\ {}^{t}H^2\ [DG']^3$



$$O^{-}E^{+} = [DG']^{3}\ {}^{t}H^{2}\ [DG']^{3}$$

Ici aussi, on tient le cube comme il le faut pour appliquer la formule.

Le Skewb possède un algorithme théorique à une seule formule comme le Rubik's Cube !

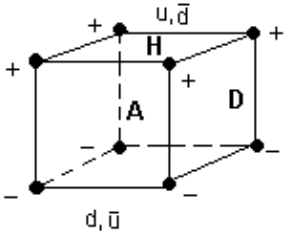
3 LE RUBIK'S CUBE ET LES PARTICULES

Un quark est une particule élémentaire ayant une charge fractionnaire, par ex:
le quark u = 2/3 (up) et
le quark d = -1/3 (down)
les antiquarks ont les charges opposées, par ex
$\overline{u}$ = -2/3 antiquark up et
$\overline{d}$= 1/3 antiquark down.
Une des propriétés étranges des quarks c'est qu'ils ne peuvent exister tout seul! mais toujours en couple ou en triple ! Un couple de quarks se nomme méson et un triplet de quarks se nomme baryon.
Avec les quarks et antiquarks on fabrique les particules, par ex un proton p est composé de deux quarks up et un quark down p = uud, un neutron n, d'un quark up et deux quarks down n = udd.

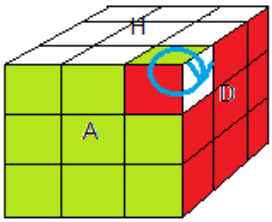
On vérifie aisément que, pour un proton p sa charge vaut 1, en effet:
p = uud ⇒ 2/3 + 2/3 - 1/3 = 1 de même pour un neutron n
n = udd ⇒ 2/3 - 1/3 - 1/3 = 0 sa charge vaut bien 0

Un baryon est une particule à 3 quarks , le proton et le neutron sont des baryons. Un méson est une particule formée par une paire de (quarks, antiquark) comme
$\pi^+ = u\overline{d}$ = (pion+)

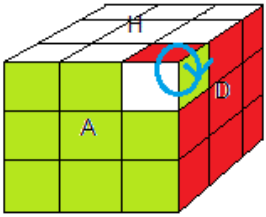
Avant tout on va convenir (convention "B-") que les rotations des sommets Haut (up) seront comptés toujours positive, et celle du Bas (down) toujours négative, ça signifie que les rotations par exemple (HDA) comptent 1/3 ou 2/3 (toujours dans le sens horaire) par contre les rotations par ex (BAD) comptent -1/3 ou -2/3 (dans le sens contraire).



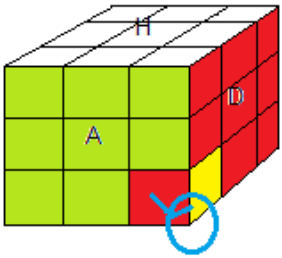
Sommet Haut: compté 1/3 ou 2/3 , Bas -1/3 ou -2/3



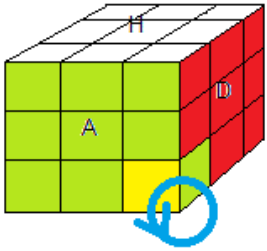
Rotation 1/3



Rotation 2/3



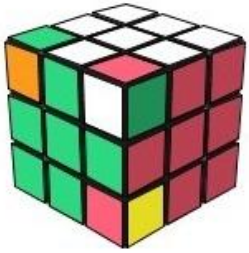
Rotation -1/3



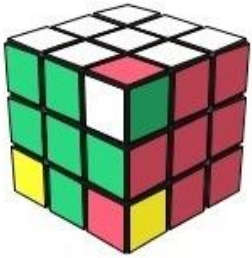
Rotation -2/3

On voit donc que le Haut produit les quarks u et $\overline{d}$ et le Bas les quarks d et $\overline{u}$, en effect les sommets Haut pivote 1/3 ou 2/3 de tour, et les sommet Bas pivote -1/3 ou -2/3 de tour d'après notre convention "B-" .

Il n'est pas difficile de fabriquer des particules avec le Rubik's Cube !!
Voyons par ex pour un proton p, on sait que p = uud il suffit donc (par ex) de pivoter (HDA) 2/3 de tour, (HAG) 2/3 de tour, et (BAD) -1/3 de tour c'est-à-dire
(HDA) = 2/3 , (HAG) = 2/3 et (BAD) = -1/3
De même pour un neutron n = udd
(HDA) = 2/3 , (BGA) = -1/3 , (BAD) = -1/3



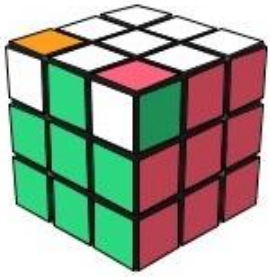
Un proton: p = uud
proton = B'GBD'BD'BG'B^2 D^2HA^2H'



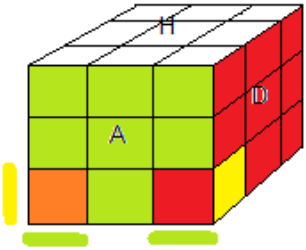
Un neutron: n = udd
neutron = $D(HG')^2HD'H^2G^2B$ $A^2B'H'$

Il est vraiment mystérieux que ces états représentent un proton et un neutron !!! Voici une formule V = $[DH]^2.G'[HD]^2G$ qui donne le pion $\pi^+=u\overline{d}$ composé d'une paire de quarks-antiquark $(u,\overline{d})$ et avec les rotations Cube $^tH,^tD$ ... (notation anglais CU,CR...), vous pouvez obtenir tous les autres pions !! (quark de première génération u,d)

$(u, \overline{d})$
$(d, \overline{u})$



Un méson: pion $\pi^+ = u\overline{d}$
(HDA) = u, (HAG) =$\overline{d}$



Un méson: pion $\pi^- = \overline{u}d$
(BGA) =$\overline{u}$, (BAD) = d

On a:

- Soit 2 sommets à pivoter dans le sens contraire .
- Soit 3 sommets à pivoter dans le même sens.

Méson
¤ (-1/3, 1/3)
⇒ (2/3 , 1/3) = u$\overline{d}$ = π^+
⇒ (-1/3, - 2/3) = d$\overline{u}$ = π^-

Baryon
¤ (-1/3, -1/3, -1/3) = ddd = Δ^-
⇒(2/3, -1/3, -1/3) = udd neutron
⇒(2/3, 2/3, -1/3) = uud proton
⇒(2/3, 2/3, 2/3) = uuu = Δ^{++}
¤ (1/3, 1/3, 1/3) = $\overline{d}\,\overline{d}\,\overline{d}$ (hypotétique)
(-2/3, 1/3, 1/3) = $\overline{u}\,\overline{d}\,\overline{d}$ (hypotétique)
(-2/3, -2/3, 1/3) = $\overline{u}\,\overline{u}\,\overline{d}$ (hypotétique)
(-2/3, -2/3, -2/3) = $\overline{u}\,\overline{u}\,\overline{u}$ (hypotétique)

REMARQUE : La rotation cube $^tD'$ transforme $\overline{d}$ en $\overline{u}$ et u en d: $^tD'$: $\overline{d} \rightarrow \overline{u}$ et u → d, de même on peut tourner le Cube pour obtenir le neutron à partir du proton et vis-versa, $^tA^2$: proton→neutron. Les rotations cube jouent donc le rôle l'interaction faible !!

<u>En résumé</u> : Un sommet pivoté représente un quark, comme un quark ne peut exister tout seul, on ne peut pas pivoter un sommet tout seul !!! Finalement notre cher Rubik's Cube contient des Pions, des protons, neutrons, l'interaction faible ... et le nombre complexe i^2=-1 ,... incroyable non ?

Si on supprime la convention "B-" un sommet a donc deux rotations (dans le sens horaire) : soit 1/3 de tour, soit 2/3

de tour . Dans ce cas, votre Rubik's Cube ne produit que 3 particules :
Un méson (quark-antiquark) = $\pi^+ = u\overline{d} = 2/3 + 1/3 = 1$
un baryon (3 quarks) = $\Delta^{++} = uuu = 2/3 + 2/3 + 2/3 = 2$
un antibaryon = $\overline{\Delta}^{--} = \overline{d}\,\overline{d}\,\overline{d} = 1/3 + 1/3 + 1/3 = 1$
(hypotétique)

Avec un Rubik's Cube dans votre poche:
-à 2 sommets pivotés.
ou
-à 3 sommets pivotés.
nul ne peut imaginer que vous baladez avec une particule élémentaire dans la poche !!!
(+1,-1) ⇒ méson π^+
(-1,-1,-1) ⇒ baryon Δ^{++}
(+1,+1,+1) ⇒ ?? pas encore découvert !!!

4 LE GROUPE SIMPLE MATHIEU M_{12}

Ce qui est vraiment remarquable c'est que le Rubik's Cube contient un objet mathématique extrêmement rare : le groupe simple sporadique de Mathieu M_{12} !!!

Un groupe simple c'est un groupe qui ne contient pas de sous groupes normaux (à par 1 et G bien sûr) , par exemple $\mathbb{Z}_p$ avec p = premier, et les A_n avec $n \geq 5$
La classification des groupes finis simples s'est terminée en 1983 (légère correction en 2004) , il y a 18 familles et 26 groupes non classables nommés sporadiques . Le groupe M_{12} est l'un des sporadiques découvert par Mathieu dans les années 1860 (Mathieu en a découvert cinq)

Le groupe M_{12} est assez simple à construire
Soit: E = {1,2,3,4,5,6,7,8,9,10,11,12}
Soient p et q, deux fonctions suivantes:

$p(x) = 13 - x$

et

$q(x) = \min(2x - 1, 26 - 2x)$

ce qui donne comme permutations :

p = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)

q = (2,3,5,9,8,10,6,11,4,7,12)

et M_{12} c'est l'ensemble des permutations de E engendrées par p et q
$M_{12} = < p, q > \subset S_E$
On a: $|M_{12}| = 12!/7! = 95040$
Remarque : les permutations p et q sont paires donc M_{12} est un sous groupe de $M_{12} \subset A_{12}$

GAP nous donne bien $|M_{12}| = 95040$

gap_mathieu12.txt

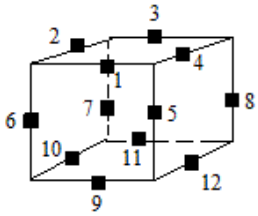
```
p := (1,12)(2,11)(3,10)(4,9)(5,8)(6,7) ;
q := (2,3,5,9,8,10,6,11,4,7,12) ;
mathieu12 :=  Group( p,q );
Smathieu12 := Size( mathieu12 );
```

Remarque : M_{12} est 5-transitif

4.1 LE RUBIK'S CUBE ET M_{12}

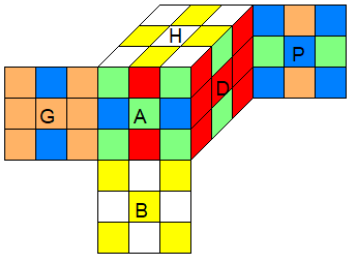
On va noter les arêtes comme indique la fig ci-dessous
(HA)=1,(HG)=2,(HP)=3,(HD)=4

(AD)=5,(AG)=6,(PG)=7,(PD)=8
(BA)=9,(BG)=10,(BP)=11,(BD)=12

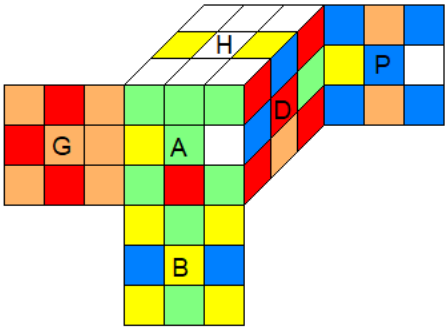


1,2,3,4
5,6,7,8
9,10,11,12

Posons
$C = HP^2H^2G^2D^2H^2A^2H'$ (14*)
$S = BH'G^2H' .P^2BG^2 .ADHGH'.A'D'BA'B .H'DBD'$ (24)
d'où
$M_{12} = < C,S >$



e•C = c = (p,0,id,0)



e•S = s = (q,0,id,0)

Les formules C et S engendrent exactement M_{12}, il est remarquable que le Rubik's Cube contient M_{12} car c'est un groupe simple sporadique, les groups simples sporadiques il n'y en a que 26.

4.2 RÉSOUDRE LE PUZZLE M_{12}

Voici une question intéressante: Si on mélange le Cube uniquement avec C et S comment le restaurer avec seulement C et S ?
Il est clair qu'on ne peut pas le faire manuellement car les formules C et S sont trop longues .... mais imaginez qu'il y a une machine, ou un programme qui fait C et S pour vous alors comment s'en sortir ?
La solution provient d'une propriété mathématique du

groupe M_{12} il est 5-transitif c'est à dire s'il y a 5 nombres bien placés alors les autres seront automatiquement bien placés !!
La stratégie est donc de placer les nombres 1,2,3,4,5

Rappel :
$C = HP^2H^2G^2D^2H^2A^2H' = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7)$
$S = BH'G^2H' .P^2BG^2 .ADHGH'.A'D'BA'B .H'DBD' = (2,3,5,9,8,10,6,11,4,7,12)$

Considérons les 6 formules suivantes:

$F_3 = CS^2CS^5CS^4 = (3,10,4,5)(6,7,11,12)$
$G_3 = CSCS^3CS^2 = (4,9)(3,11,10,5,8,7,12,6)$

$F_4 = CSCS^3CS^2CS^9CS^7CS^8 = (4,7,6,12)(5,10,8,9)$
$G_4 = CS^3CS^6CSCS^9CS^7CS^8 = (4,7)(5,6)(8,12)(9,11)$

$F_5 = CS^9CS^7CS^8CS^7CSCS^5 = (5,10,12,7)(6,8,11,9)$
$G_5 = CSCS^3CS^2CS^7CSCS^5\ CS^7CSCS^5 = (5,11,12,6)(7,9,10,8)$

Placer 1, 2
- Si 1 est en bonne place, alors rien à faire sinon on le déplace avec S en 12 puis le place avec C
- Pour 2: on le place avec S .

Placer 3
- Si 3 en 4: utilisez F_3
- Sinon: utilisez G_3

Placer 4
- Si 4 en 6,7,12: utilisez F_4
- Si 4 en 5,9,10: utilisez F_4 pour le mettre en 8

- Si 4 en 8,11: utilisez G_4 pour le mettre en 12 ou 9

<u>Placer 5</u>

- Si 5 en 7,10,12: utilisez F_5
- Si 5 en 8,9,11: utilisez F_5 pour le mettre en 6
- Si 5 en 6: utilisez G_5

5 ACTION, OPÈRER, AGIR

Rappel :

$G^+ = S_{12} \times Z_2^{12} \times S_8 \times Z_3^8$

$\mu=(u,x,v,y)\in G^+$, $u\in S_{12}$, $x\in Z_2^{12}$, $v\in S_8$, $y\in Z_3^8$

$\mu=(u,x,v,y)$, $\mu'=(u',x',v',y')$

$\mu\mu' = (u,x,v,y)\ (u',x',v',y') = (uu',x+u(x'),vv',y+v(y'))$

$uu' = u' \circ u$

$u(x) = (x_{u(1)} , x_{u(2)} , \dots , x_{u(12)})$

G^+ c'est l'ensemble des configurations.

et

$M = < H,B,A,P,G,D >$

$(M, .)$ où '.' est le concatération , $V,T \Rightarrow VT$

Il est vraiment important de distinguer deux choses: formule (mouvement, manœuvre, mélange, ...) et configuration (motif, ...)

- Une formule transforme une configuration en une autre

configuration.
- Les configurations décrivent le Cube

On va définir une action libre et compatible '•' de M sur G^+ de façon suivante:

$G^+ \times M \to G^+$

$(\mu,V) \to \mu \bullet V = \nu \in G^+$

$A_1)$ $\forall \mu$; $\mu \bullet I = \mu$;élément neutre

$A_2)$ $\forall \mu,V,T$; $(\mu \bullet V) \bullet T = \mu \bullet (VT)$;associative

$$A_3) \begin{cases} a \in G^+ \text{ donné, fixé} \\ \forall V \in M\ ;\ a \bullet V = a \Rightarrow V = I\ ; \text{librement} \end{cases}$$

Quelqu'un qui laisse fixe un point est forcement I, I est la seule formule ayant des points fixes.

(5.1.1) $A_4)$ $\forall \mu,V,T$; $\mu \bullet (VT) = (\mu \bullet V)(\mu \bullet T)$;compatibilité les lois de M et G^+

On pose

$G \overset{\text{def}}{=} \{\mu \in G^+ \mid \exists V \in M\ ,\ e \bullet V = \mu\} \subset G^+$; e = l'état résolu.

G c'est l'ensemble des états, ce sont des configurations provenant de M (à partir de e) , c'est l'orbite de e.

5.2 BIJECTION ENTRE M ET G

Il y a une bijection entre M et G , voyons ...
Soit

f: M $\dashrightarrow$ G
V $\dashrightarrow$ f(V) = e•V

Le but est donc de montrer que f est bijective.

1. f est injective

f(V) = f(T)
e•V = e•T
(e•V)•T' = (e•T)•T'
e•(VT') = e•(TT') ;propriété (A_2)
e•(VT') = e•I = e ; axiome A_1
La propriété (A_3) donne

VT' = I d'où
V = T
f est donc injective

2. f est surjective

Il n'y a rien à démontrer , la surjectivité de f provient de la définition de G, ce sont des configurationss qui proviennent de M .

$\forall \mu \in G \Rightarrow \exists V$ tel que $\mu = e \bullet V = f(V)$
f est surjective.

Finalement on a une bijection entre M et G (on note $M \leftrightarrow G$)
Une formule $\leftrightarrow$ un état , une formule génère un état et un seul, un état provient d'une formule unique .

Il y a donc une seule formule pour un état donné mais cette formule a des différentes écritures, par ex:

$(H^2D^2)^3(B^2D^2)^3 = (H^2G^2)^3(B^2G^2)^3$
$D' = D^3$

De même à l'état résolu e:
il y a une seule formule I pour l'état e mais il y a plusieurs l'écriture de cette formule
$A^4 = [HD]^6 = I$

C'est exactement quand vous écrivez:
* 1/2 = 0,5 = 3/6
l'inverse de 2 est unique mais il y a plusieurs l'écriture.

- Les rôles de M et G sont très différents, un éléments de M possède plusieurs l'écriture, alors que ce n'est pas le cas pour un élément de G. M agit sur G et non à l'inverse, et M agit sur X mais pas G .
- Beaucoup de gens pensent que la rotation A par exemple fait bouger les sommets (parce que visuellement c'est ça). MAIS NON !!! la rotation A "ordonne", à la permutation de bouger les sommets, c'est la permutation qui bouge les sommets (elle exécute l'ordre de A). Mais pourquoi ça ? c'est simple c'est dans l'écriture de la permutation !!! Nommons les sommets par exemple a, b, c quand on écrit:

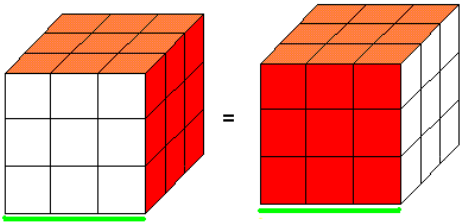
p = (a,b,c) c'est bien
p(a)=b, p(b)=c et p(c)=a ⇒ p déplace a en b , b en c etc ...
mais jamais
A(a)=b, A(b)=c et A(c)=a !!!
On voit donc bien que p bouge a en b (p(a)=b)

6 INDICATRICE DU RUBIK'S CUBE

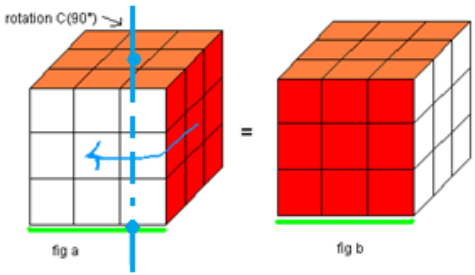
Prenons le Rubik's Cube et posons nous 2 questions suivantes:
- Combien de Cubes différents si on le peint avec seulement 3 couleurs, ou 6 couleurs (une couleur par face et une couleur peut être utilisée plusieurs fois) ?
- Combien de Cubes différents si on le peint avec 1 face jaune, 2 faces rouges, et 3 faces kleins ?

6.1 ANALYSER LE PROBLÈME

Voyons comment on dit 2 Cubes sont identiques ...



Ces 2 Cubes sont identiques



On passe de a à b par la rotation C(90°)

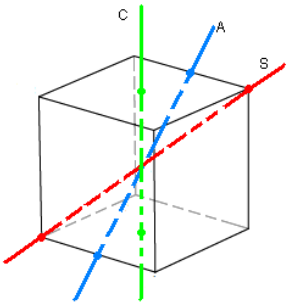
En effet si on le tient dans la main , on ne verra pas la différence, pour nous c'est un Cube à 4 couleurs orange-rouge-vert et blanc. Il n'y a pas de Haut, ni de Bas, ni Gauche, ni Droite ,... c'est un Cube "mobile" on peut le bouger, tourner, pivoter .... contrairement à un Cube fixe il y a un Haut, un Bas ....

Un Cube fixe c'est comme votre chambre: il y a le plafond, le plancher, ...

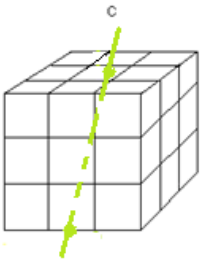
Pour un Cube mobile, on le tient dans la main comme on veut ça ne change rien, mais on passe d'une position à une autre par des rotations
Exemple on passe de fig(a) à fig(b) par la rotation C(90°)=d'axe centre-centre à 90°:

La question se pose donc quelles sont les rotations qui laissent invariant le Cube ?

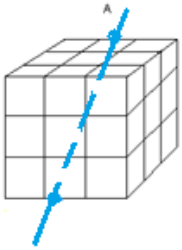
6.2 LE GROUPE DES DÉPLACEMENTS DU RUBIK'S CUBE $\mathfrak{D}(R)$



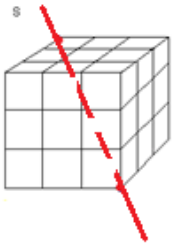
3 types de rotations



Rotation C: Axe centre-centre



Rotation A: Axe arête-arête



Rotation S: Axe sommet-sommet

Il y a trois types de rotations sur le Cube: les rotations d'axe centre-centre, les rotations d'axe arête-arête (axe passe par les milieux d'arêtes), les rotations d'axe sommet-sommet , mais avant tout on va introduire une notation: T_k^n , signifie on a: n orbites à k éléments

<u>Rotation C: Axe centre-centre</u>
- il y a 3 rotations C(90°) ⇒ 2 orbites à 1 élément, 1 orbites à 4 éléments ce qui donne
$3T_1^2T_4$
- il y a 3 rotations C(-90°) ⇒ 2 orbites à 1 élément, 1

orbites à 4 éléments ce qui donne
$3T_1^2T_4$
- il y a 3 rotations C(180°) ⇒ 2 orbites à 1 élément, 2 orbites à 2 éléments ce qui donne
$3T_1^2\ T_2^2$

Rotation A: Axe arête-arête
- il y a 6 rotations A(180°) ⇒ 3 orbites à 2 éléments ce qui donne
$6T_2^3$

Rotation S: Axe sommet-sommet
- il y a 4 rotations S(120°) ⇒ 2 orbites à 3 éléments ce qui donne
$4T_3^2$
- il y a 4 rotations S(-120°) ⇒ 2 orbites à 3 éléments ce qui donne
$4T_3^2$

Et bien sûr
L'identité id
- il y a un id ⇒ 6 orbites à 1 élément, ce qui donne
T_1^6
Soit au total: 9+6+8+1(identité) = 24 rotations, ces rotations forment un groupe $\mathfrak{D}(R)$ (identique à $S_4 = \mathfrak{D}(R)$) ce qu'on appelle le groupe de déplacement (isométrie positive) du Cube. il laisse invariant le Cube.

La fonction définie par:
$K = (6T_1^2T_4 + 3T_1^2T_2^2 + 6T_2^3 + 8T_3^2 + T_1^6)/24$
se nomme l'indicatrice du Rubik ou l'indicateur des cycles de $\mathfrak{D}(R)$. Pourquoi des 'cycles' ??

En fait on peut voir les choses autrement, on peut dire: T_k^n, signifie on a: n cycles de longueur k
voyons pour:

<u>Rotation C: Axe centre-centre</u>
- il y a 3 rotations C(90°) ⇒ les faces bougent ⇒ (H)(B)(D,A,G,P) ⇒ deux 1-cycle, un 4-cycle ce qui donne $3T_1^2T_4$
- il y a 3 rotations C(-90°) ⇒ les faces bougent ⇒ (H)(B)(D,P,G,A) ⇒ deux 1-cycle, un 4-cycle ce qui donne $3T_1^2T_4$
- il y a 3 rotations C(180°) ⇒ les faces bougent ⇒ (H)(B)(A,P)(G,D) ⇒ deux 1-cycle et deux 2-cycle ce qui donne $3T_1^2\ T_2^2$

<u>Rotation A: Axe arête-arête</u>
- il y a 6 rotations A(180°) ⇒ trois 2-cycles ⇒ (H,P)(A,B)(G,D) ce qui donne $6T_2^3$

<u>Rotation S: Axe sommet-sommet</u>
- il y a 4 rotations S(120°) ⇒ deux 3-cycles ⇒ (H,G,P)(A,B,D), ce qui donne $4T_3^2$
- il y a 4 rotations S(-120°) ⇒ deux 3-cycles ⇒ (P,G,H)(D,B,A), ce qui donne $4T_3^2$

Et bien sûr
<u>L'identité id</u>

- il y a un id ⇒ six 1-cycles ⇒ (H)(B)(A)(P)(G)(D), ce qui donne
T_1^6

6.3 L'INDICATRICE DU RUBIK

On rappelle que ça vaut:

$K = (6T_1^2T_4 + 3T_1^2T_2^2 + 6T_2^3 + 8T_3^2 + T_1^6)/24$

T_k^n , signifie on a: n orbites à k éléments
ou encore
T_k^n , signifie on a: n cycles de longueur k, n (k-cycle)

6.4 FONCTION COLORIAGE μ, μ*

On a 2 fonctions de coloriage du cube
La fonction μ définie par:
μ = dans K, on remplace T_k = c où c=le nombre de couleurs
$\mu = (6c^2c + 3c^2c^2 + 6c^3 + 8c^2 + c^6)/24$
$\mu = (12c^3 + 3c^4 + 8c^2 + c^6)/24$

Pour simplifier on ne prend que 3 couleurs X_1, X_2, X_3
La fonction définie par:
μ* = Dans K , on remplace $T_k = (X_1^k+X_2^k+X_3^k)$

6.5 RÉPONSE À NOS QUESTIONS

- Combien de Cubes différents si on le peint avec seulement 3 couleurs ? (une couleur peut être utilisée plusieurs fois).
$\mu = (12c^3 + 3c^4 + 8c^2 + c^6)/24$
pour c=3
$\mu = (12.3^3 + 3.3^4 + 8.3^2 + 3^6)/24$
$\mu = 57$!!!!

- Combien de Cubes différents si on le peint avec a couleurs X_1, b couleurs X_2, et c couleurs X_3, ?
Il suffit de développer μ^* et trouver le coefficient de $X_1^a X_2^b X_3^c$, bien sûr on ne développe pas μ^* à la main il y a des programmes, des calculatrices qui le font pour nous.

Commentaire

Pour trouver l'indicatrice du Cube on est obligé de passer par le groupe de déplacement, une fois trouvé l'indicatrice K elle nous fournit 2 fonctions de coloriages μ et μ^* mais seulement μ qu'on peut le calculer manuellement, quant à μ^* il faut des machines pour calculer. Retenons donc simplement μ

$\mu = (12c^3 + 3c^4 + 8c^2 + c^6)/24$

N'oubliez pas qu'on peut utiliser une couleur plusieurs fois. Par ex si on prend c=6 $\Rightarrow$ μ =2226 et non μ=30 (une couleur utilisée une seule fois)

7 LA CONJUGAISON

En manipulant votre Rubik's Cube, vous utilisez peut-être sans le savoir le principe de conjugaison.

7.1 LE TECHNIQUE DE LA CONJUGAISON

La technique de la conjugaison (TC) permet de réaliser un projet en tout point si on peut le faire un un point ! On va prendre un ex pour bien comprendre. Voici une formule

$T = AH^2A^2.B'[H'G']B.A^2H'A'H'$

qui renverse deux arêtes (HA) et (HD) et laisse intactes les autres pièces du Cube (on dira que le reste du Cube est invariant) donc d'après la TC on peut renverser toutes les arêtes ! par ex si on veut renverser (AD) et (HP) comment faire ?
Eh bien c'est très simple, il suffit d'amener (AD) en (HA) et (HP) en (HD) puis appliquer la formule ensuite remettre les arêtes (AD) et (HD) dans leur emplacement initial c'est tout !!
voyons de plus prés:

1. (AD,HA)(HP,HD) = A'P'D'

2. Appliquer la formule: T
3. Remettre les pièces (AD) et (HP) dans leur emplacement initial: DPA

Autrement dit pour renverser (AD) et (HP) on fait:
$(AD)^{+}(HP)^{+}$ = (A'P'D') .(AH^2A^2.B'[H'G']B.A^2H'A'H') .(DPA)
Ainsi on peut renverser toutes les arêtes.

T = AH^2A^2.B'[H'G']B.A^2H'A'H'

$(AD)^{+}(HP)^{+}$ = (A'P'D')T(DPA)

La TC s'écrit toujours dans le format : XYX' comme vous avez remarqué sur l'exemple ci-dessus (A'P'D').T.(A'P'D')'. C'est pourquoi l'écriture XYX' s'appelle conjugaison. par ex : ABA' c'est une conjugaison
Rappel l'inverse d'une formule
X = ABH'GD'P^2G'H
X' = H'GP^2'DG'HB'A' (lire à envers et prime↔non-prime)

Parfois on trouve dans la littérature les notations Y^X=XYX' ou $\frac{Y}{X}$ = XYX' , pour la simple raison que ces notations conserve une propriété de la conjugaison , en effet :
* $(Y^X)^Z$ = $(XYX')^Z$ = Z(XYX')Z'
= (ZX)Y(X'Z') = (ZX)Y(ZX)' = Y^{ZX} autrement dit on a la relation
$(Y^X)^Z$ = Y^{ZX} ce qui correspond bien une propriété des puissances, comme pour les nombres :

$(5^2)^3$ = 5^{3x2}
de même pour la notation $\frac{Y}{X}$
* $\frac{\left(\frac{Y}{X}\right)}{Z} = \frac{XYX'}{Z} = Z(XYX')Z' = (ZX)Y(X'Z') = (ZX)Y(ZX)' =$

$\frac{Y}{ZX}$ ce qui correspond bien une propriété de la division:

$$\frac{\left(\frac{Y}{X}\right)}{Z} = \frac{Y}{ZX}$$

comme pour les nombres:

$$\frac{\left(\frac{5}{2}\right)}{3} = \frac{5}{3x2}$$

7.2 LES K-FORMULES

Une K-formule c'est une formule qui modifie une seule pièce de la face K laissant ainsi intactes les autres pièces de la face K, elle peut bien sûr modifier les autres faces. Par ex:

→ C = D'BDABA' est une H-formule car elle modifie une seule pièce (HDA) de la face Haut.
→ Z = [DH] est une B-formule car elle modifie une seule pièce (BAD) de la face Bas, mais c'est aussi une G-formule car elle modifie une seule pièce (HGP) de la face Gauche.

→ V = AHB'$G^2H^2B^2$DH est une H-formule car elle modifie une seule pièce (HA) de la face Haut.

7.3 FORMULES PROPRES

Rappel: Une formule propre (ou indépendante) est une formule qui réalise un travail visé et laisse le reste du Cube invariant.

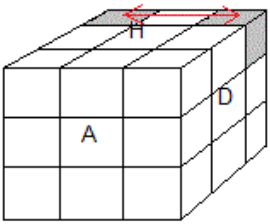
La formule T est propre. Les formules propres sont très recherchées car elles permettent d'appliquer le Principe de Conjugaison sans aucune précaution à prendre.

Mais comment trouve-t-on les formules propres ?

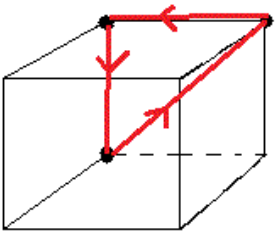
comment fabrique-t-on les formules propres ??. Eh ! bien, on les fabrique à partir des K-formule !!

Supposons qu'on aie une G-formule qui modifie un sommet-Gauche et laisse autres pièces de la face Gauche invariantes (elle peut modifier les autres faces bien sûr) alors on peut construire une formule propre. Voyons sur un ex

Voici une G-formule Z = [DH] qui modifie le sommet (HGP) et laisse la face G invariante, on va construire une formule propre à partir de Z
Il suffit de prendre S = [ZG] = ZGZ'G'
Explication
1. On applique Z : le sommet (HGP) est échangé, mais le reste du Cube est perturbé
2. On amène le sommet (BPG) -sommet cobaye- en (HGP): G
3. On applique Z' : qui échange le sommet (BPG) et répare le reste du Cube en même temps .
4. On remet le sommet (BPG) dans son emplacement initial: G'
La formule S = ZGZ'G' déplace 3 sommets (HGP)→(BPG)→(HPD) et laisse le reste du Cube invariant.



Z = [DH]



S = [ZG] = ZGZ'G'

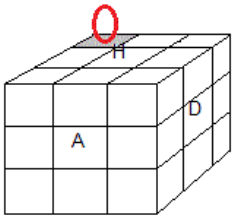
[DH].G[HD]G' = (HGP)→(BPG)→(HPD)

Dans le même ordre idée

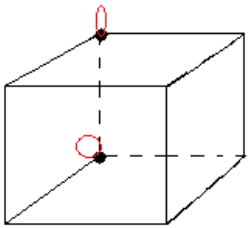
Soit $Z^2 = [DH]^2$ qui pivote le sommet (HGP) et laisse la face G invariante, on va construire une formule propre à partir de Z^2.
Comme dans l'exemple précédant on prend $S = [Z^2G] = Z^2GZ^{2'}G'$
Explication

1. On applique Z^2 : le sommet (HGP) est pivoté, mais le reste du Cube est perturbé
2. On amène le sommet (BPG) -sommet cobaye- en (HGP): G
3. On applique $Z^{2'}$: qui pivote (BPG) à l'inverse et répare le reste du Cube en même temps.
4. On remet le sommet (BPG) dans son emplacement initial: G'

La formule $S = Z^2GZ^{2'}G'$ pivote ainsi 2 sommets (HGP), (BPG) et laisse le reste du Cube invariant.



$Z^2 = [DH]^2$



$S = [Z^2G] = Z^2GZ^{2'}G'$

De même on peut construire une formule propre à partir de V, il suffit de prendre S = [VH] = VHV'H' qui pivote deux arêtes (HA) et (HD) .

La façon de construire une formule propre comme ci-dessus s'appelle Principe de Commutation. Le Principe de Commutation s'écrit toujours dans le format: XYX'Y' en abrégeant [XY], c'est pourquoi l'écriture XYX'Y' s'appelle commutation

En Rubik's Cube on utilise 2 principes:
La Conjugaison: XYX' = Y^X et
La Commutation: XYX'Y' = [XY]
XYX' s'appelle un conjugué de Y

[XY] = Y^X Y' .

8 L'ORDRE MAXIMAL D'UN ÉLÉMENT DE G

Le but de ce paragraphe c'est démontrer mathématiquement l'ordre maximal d_{max} d'un élément de G (ou l'ordre maximal d'une formule) est 1260, c'est-à-dire trouver une formule mathématique donnant d_{max} .
Beaucoup de gens en parlent , mais souvent c'est vague, pas de démonstration et on ne sait toujours pas pourquoi ça vaut 1260.
Il existe des algorithmes qui calculent tous les ordres de G, et on trouve évidemment le plus grand c'est 1260.
Mais ce qu'on veut c'est une démonstration mathématique ...

8.1 DÉFINITIONS ET NOTATIONS

Rappel
$G^+ = S_{12} \times \mathbb{Z}_2^{12} \times S_8 \times \mathbb{Z}_3^8$ le groupe des configurations ,
le groupe du Rubik's Cube G est l'ensemble des éléments (u,x,v,y) de G^+ vérifiant (th fondamentale):

1. $\sum x_i = 0 \pmod 2$ où $x = (x_1,x_2,...,x_{12})$
2. $\sum y_i = 0 \pmod 3$ où $y = (y_1,y_2,...,y_8)$
3. sig(u) = sig(v)

L'ordre
L'ordre d'une permutation v , c'est le plus petit entier positif d tel que $v^d = id$ et on le note $|v| = d$
NOTE : Si v est composé de cycles disjoints son ordre vaut le ppcm des cycles
v = (a-cycle)(b-cycle)(c-cycle)
alors
$|v| = d = ppcm(a,b,c)$

Théorème central :
On pose: m=ppcm(a,b) et
$A = \{ m'=ppcm(a',b') \text{ où } a' \mid a \text{ et } b' \mid b \}$
$B = \{ x \mid x \mid m \}$
alors on a: A=B

L'ensemble des diviseurs de ppcm est égal à l'ensemble des ppcm des diviseurs.
Div(ppcm(a,b))={ppcm(Div(a),Div(b)) }
où Div(a)=l'ensemble des diviseurs de a, ces deux ensemble sont égaux.

Démonstration
La démonstration se fait par la décomposition de ces nombre en facteurs premiers, et la façon de calculer le ppcm. Pour bien voir le déroulement de la démonstration on va raisonner sur un exemple.

$a = p^3q^2$

$b = p^2r^3$

$Div(a) = \{(1+p+p^2+p^3)\ (1+q+q^2)\}$
$= \{1,q,q^2,\ p,pq,pq^2,\ p^2,p^2q,p^2\ q^2,\ p^3,p^3q,p^3q^2\ \}$
$= \{a'=p^iq^j \text{ avec } 0\leq i\leq 3,\ 0\leq j\leq 2\}$

$Div(b) = \{(1+p+p^2)\ (1+r+r^2+r^3)\}$
$= \{1,r,r^2,r^3,\ p,pr,pr^2,pr^3,\ p^2,p^2r,p^2r^2,p^2r^3\ \}$
$= \{b'=p^kr^t \text{ avec } 0\leq k\leq 2,\ 0\leq t\leq 3\}$

$m=ppcm(a,b)=p^3q^2r^3$ (tout et plus grande puissance)

$Div(m) = \{(1+p+p^2+p^3)\ (1+q+q^2)\ (1+r+r^2+r^3)\}$
$= \{x=p^fq^gr^h, \text{ avec } 0\leq f\leq 3,\ 0\leq g\leq 2,\ 0\leq h\leq 3\ \}$

* $a'\in Div(a)$ $a'=p^iq^j$ avec $0\leq i\leq 3,\ 0\leq j\leq 2$

* $b'\in Div(b)$ $b'=p^kr^t$ avec $0\leq k\leq 2,\ 0\leq t\leq 3$

$m'=ppcm(a',b')= p^iq^jr^t$ en supposant que i absorbe k (i>k)

On voit donc que $m'=p^iq^jr^t$ et $x= p^fq^gr^h$ un diviseur de m $x\in Div(m)$ ont exactement la même forme et les puissances (i,j,t) et (f,g,h) varient de la même façon (c'est la même écriture) donc ces deux ensemble sont égaux A=B

$m'\in A \Rightarrow m'=p^iq^jr^t \Rightarrow m'\in Div(m) \Rightarrow m'\in B \Rightarrow A\subset B$

$x\in B \Rightarrow x=p^fq^gr^h \Rightarrow x=ppcm(a',b') \Rightarrow x\in A \Rightarrow B\subset A$

finalement A=B .

Un sommet est représenté par $(v,y) \in S_8 \times \mathbb{Z}_3^8$ et la loi de composition donne
$(v,y)(v',y') = (vv', y + v(y'))$
donc pour
$(v,y)^2 = (v^2, y + v(y))$
$(v,y)^3 = (v^3, y + v(y) + v^2(y))$
....
$(v,y)^b = (v^b, y + v(y) + v^2(y) + ... + v^{b-1}(y))$

par définition on note
$y + v(y) + v^2(y) + ... + v^{b-1}(y) = y^b$
d'où
$(v,y)^b = (v^b, y^b)$
On appelle l'ordre du vecteur y, c'est le plus petit entier positif b tel que
$y + v(y) + v^2(y) + ... + v^{b-1}(y) = 0$
et on le note $|y| = b$

Big théorème.

On a le théorème suivant

<u>Théorème</u>
L'ordre du vecteur d'orientation y est un diviseur de 3|v| .
$|y| \mid 3|v|$
de même pour les arêtes
L'ordre du vecteur d'orientation x est un diviseur de 2|u| .
$|x| \mid 2|u|$

Remarque
$3|v| \Rightarrow$ '3' parce qu' un sommet a 3 orientations

$2|u| \Rightarrow$ '2' parce qu' une arête a 2 orientations
L'ordre de l'orientation ne dépend que de l'ordre de la permutation.

On va faire la démonstration pour les sommets $(v,y) \in S_8 \times \mathbb{Z}_3^8$, pour les arrêtes c'est pareil. Mais avant on va étudier un polynôme nécessaire à la démonstration.

Posons: $P_d(v) = 1 + v + v^2 + ... + v^{d-1}$ un polynôme en v et $P_0(v) = 0$ (c'est un polynôme "formel" on va l'appliquer sur le vecteur y, on aura une somme de vecteurs donc pas de problème avec le signe '+').
Commençons par avoir quelques propriétés de ce polynôme
P1. $P_{ab}(v) = P_a(v^b)\, P_b(v)$
P2. $P_{ab+r}(v) = v^r P_{ab}(v) + P_r(v)$
P3. $P_{3|v|}(v) = 3P_{|v|}(v)$

<u>Démonstration P1</u>
Posons $w = v^b$
$P_a(w) = 1 + w + w^2 + ... + w^{a-1}$
$P_b(v) = 1 + v + v^2 + ... + v^{b-1}$

$$P_a(w)P_b(v) = \sum_{j=0}^{j=a-1} \sum_{i=0}^{i=b-1} w^j v^i$$

$$= \sum_{j=0}^{j=a-1} \sum_{i=0}^{i=b-1} v^{jb} v^i = \sum_{j=0}^{j=a-1} \sum_{i=0}^{i=b-1} v^{jb+i}$$

$1 + v + v^2 + ...+ v^{b-1}$
$+v^b + v^{b+1} +...+ v^{2b-1}$
$+v^{2b} + v^{2b+1} +...+ v^{3b-1}$
$+v^{3b} + v^{3b+1} +...+ v^{4b-1}$
...
$+v^{(a-1)b} + v^{(a-1)b+1} +...+ v^{ab-1}$
$= P_{ab}(v)$

Démonstration P2
$P_{ab+r}(v) - P_r(v) = v^r + v^{r+1} + v^{r+2}...+ v^{ab+r-1}$
$= v^r(1 + v + v^2...+ v^{ab-1})$
$= v^r(P_{ab}(v))$

Démonstration P3
$P_{3|v|}(v) = P_3(v^{|v|}) P_{|v|}(v)$; d'après P1
$= P_3(1) P_{|v|}(v)$; car $|v|$ est l'ordre de v
$= 3P_{|v|}(v)$

Démonstration de théorème
L'ordre du vecteur y est un diviseur de $3|v|$
donc soit d = l'ordre de y c'est-à-dire le plus petit entier tel que
$[P_d(v)](y) = y + v(y) + v^2(y) + ...+v^{d-1}(y) = 0$ (*)
il faut donc démontrer que d divise $3|v|$

on divise $3|v|$ par d donc $3|v|=kd+r$ avec $0 \leq r < d$
$P_{3|v|}(v) = P_{kd+r}(v)$
$3P_{|v|}(v) = v^r P_{kd}(v) + P_r(v)$
$3P_{|v|}(v) = v^r(P_k(v^d) P_d(v)) + P_r(v)$

appliquons à y
$[3P_{|v|}(v)](y) = [v^r(P_k(v^d) P_d(v)(y)) + P_r(v)](y)$

$[3P_{|v|}(v)](y) = [P_{|v|}(v)](3y) = 0$ car $y \in \mathbb{Z}_3^8$
$[P_d(v)](y) = 0$ car d est l'ordre de y
d'où
$[P_r(v)](y) = 0$
mails alors comme d est le plus petit entier qui vérifie (*)
donc ça force r=0
finalement on a donc
$P_{3|v|}(v) = P_{kd+0}(v)$ d'où $3|v|=kd$ ca signifie que d divise $3|v|$

8.2 L'ORDRE DANS G^+

Le but est de montrer que l'ordre maximal dans G^+ est 1260 , puis trouver un élément de G^+ ayant l'ordre maximal et ensuite montrer qu'il appartient à G

$(u,x,v,y) \in G^+$
$|(u,x,v,y)| = d$ = ordre de $(u,x,v,y) \Rightarrow (u,x,v,y)^d = (id,0,id,0)$
$|(u,x)| = p$ = ordre de $(u,x) \Rightarrow (u,x)^p = (id,0)$
$|u| = t$ = ordre de $u \Rightarrow u^t = id$
$|x| = a$ = ordre de $x \Rightarrow x^a = x + u(x) + u^2(x) + ...+u^{a-1}(x) = 0$

Relation sur les ordres
$|(u,x,v,y)| = ppcm(|(u,x)|,|(v,y)|)$
$|(u,x)| = ppcm(|u|,|x|)$
$|(v,y)| = ppcm(|v|,|y|)$

On a la chaine
$(u,x,v,y)^d \Rightarrow (u,x)^p(v,y)^q \Rightarrow (u^{|u|},x^{|x|})(v^{|v|},y^{|y|})$
avec
$d = ppcm(p,q)$
$p = ppcm(|u|,|x|)$
$q = ppcm(|v|,|y|)$

on pose: $|x|=a$, $|y|=b$.
on note $O_{u,v}$ les ordres "provenant" de u,v
$O_{u,v} = \{ d\in\mathbb{N} , d = ppcm(ppcm(|u|,a),ppcm(|v|,b))$ où $a \mid 2|u|$ et $b \mid 3|v| \}$
et tous les ordres de G^+ c'est la réunion des $O_{u,v}$

$$O = \bigcup_{(u,v)} O_{u,v}$$

avec $u\in S_{12}$ et $v\in S_8$

Pour avoir un ordre d de G^+ on fixe u et v puis on fait varier a et b
ensuite on fait varier u et v

NOTE: Les ordres ne dépendent que les permutations pas d'orientation

On fixe |u| et |v|, et l'ordre d provenant de u,v est:

$T^+ =\{d=ppcm(ppcm(|u|,a),ppcm(|v|,b))$ où $a \mid 2|u|$ et $b \mid 3|v|\}$

on pose

$A=\{p=ppcm(|u|,a)$, $|u| \mid 2|u|$ et $a \mid 2|u|\}$

$B=\{k \mid k \mid m\}=\{k \mid k \mid 2|u|\}$

avec $m=ppcm(2|u|,2|u|)=2|u|$

$A'=\{p'= ppcm(|v|,b)\ ,\ |v| \mid 3|v| \text{ et } b \mid 3|v|\}$

$B'=\{k' \mid k' \mid m'\}=\{k' \mid k' \mid 3|v|\}$

avec $m'=ppcm(3|v|,3|v|)=3|v|$

Le théorème central nous dit que A=B et A'=B' on peut donc remplacer:

$ppcm(|u|,a) \dashrightarrow k \mid 2|u|$

$ppcm(|v|,b) \dashrightarrow k' \mid 3|v|$

d'où:

$T^+ = \{d=ppcm(k,k')\ ,\ k \mid 2|u| \text{ et } k' \mid 3|v|\}$

Puis on recommence le même raisonnement

$A=\{d=ppcm(k,k')\ ,\ k \mid 2|u| \text{ et } k' \mid 3|v|\}$

$h=ppcm(2|u|,3|v|)$

$B=\{q \mid q \mid h\} = T^+$

$T^+ = \{d\ ;\ d \mid ppcm(2|u|, 3|v|)\ \}$

d'où le

Théorème

Les ordres de G^+ sont:

$T^+ =\{ d ;\ d \mid ppcm(2|u|, 3|v|) \}$

Donc l'ordre maximal d'un élément de G^+ est:

$max \{ d ;\ d \mid ppcm(2|u|, 3|v|) \}$

D'où les ordres de G sont:

$T = \{ d ;\ d \mid ppcm(2|u|, 3|v|)$ avec $sig(u)=sig(v) \}$

Donc l'ordre maximal d'un élément de G est:

$max \{ ppcm(2|u|, 3|v|)$ avec $sig(u)=sig(v) \} \Rightarrow$

$\Rightarrow d_{max} = \max_{sig(u)=sig(v)} \{ppcm(2|u|, 3|v|)\}$

Maintenant il faut trouver u et v avec sig(u)=sig(v) tels que ppcm(2|u|,3|v|) soit maximal.

Attention !! On a: $a \mid 2|u|$ et $b \mid 3|v|$, une erreur de raisonnement c'est remplacer directement

$a=2|u|$ et $b=3|v|$ (valeur maximale)

dans

$Max \{d = ppcm(ppcm(|u|,a),ppcm(|v|,b)) \} \Rightarrow$

$Max \{d = ppcm(ppcm(|u|,2|u|),ppcm(|v|,3|v|)) \} \Rightarrow$

$Max \{d = ppcm(2|u|, 3|v|) \}$

pour trouver le Maximal.

C'est une erreur car le ppcm(a,b) n'augmente pas forcement quand a ou b augmente !

$a=2.3^2=18$

$b=2.5=10$

$ppcm(18,10)=2.3^2.5=90$

$a=2.3^2=18$

$b=2^2.3=12$

$ppcm(18,12)=2^2.3^2=36$

$a=2.3^2=18$

$b=2^2.5=20$

$ppcm(18,20)=2^2.3^2.5=180$

8.3 PARTITION DE 12 ET 8

Soit $u \in S_{12}$ pour calculer l'ordre de u , $|u|=d$ il serait plus facile de décomposer u en cycles disjoints car dans ce cas l'ordre de u c'est le ppcm de l'ordre de ces cycles.
La décomposition de u en cycles disjoints revient à partitionner l'entier 12 , par ex la partition
12 = 5+4+2+1
revient à dire
u = (5-cycle)(4-cycle)(2-cycle)(1-cycle)

|u|=ppcm(5,4,2,1)=20

On va donc chercher les partitions de 12 (il y a p(12)=77) (une partition n = une liste de nombres décroissants dont la somme est n)

partition paire: le nombre de décompositions est pair (donc u est pair) .

a+b+c+d ⇒ ppcm(a,b,c,d) :

1. 11+1 ⇒11
2. 10+2 ⇒ 10
3. 9+3 ⇒ 9
4. 8+4 ⇒ 8
5. 7+5 ⇒ 35
6. 6+6 ⇒ 6
7. 9+1+1+1 ⇒ 9
8. 8+2+1+1 ⇒ 8
9. 7+3+1+1 ⇒ 21
10. 6+4+1+1 ⇒ 12
11. 5+5+1+1 ⇒ 5
12. 7+2+2+1 (*) ⇒ ppcm(7,2,2,1)=14
13. 6+3+2+1 ⇒ 6
14. 5+4+2+1 ⇒ 20
15. 5+3+3+1 ⇒ 15
16. 4+4+3+1 ⇒ 12
17. 6+2+2+2 ⇒ 6
18. 5+3+2+2 ⇒ 30
19. 4+4+2+2 ⇒ 4
20. 4+3+3+2 ⇒ 12
21. 3+3+3+3 ⇒ 3
22. 7+1+1+1+1+1 ⇒ 7
23. 6+2+1+1+1+1 ⇒ 6

24. 5+3+1+1+1+1 ⇒ 15
25. 4+4+1+1+1+1 ⇒ 4
26. 5+2+2+1+1+1 ⇒ 10
27. 4+3+2+1+1+1 ⇒ 12
28. 3+3+3+1+1+1 ⇒ 3
29. 4+2+2+2+1+1 ⇒ 4
30. 3+3+2+2+1+1 ⇒ 6
31. 3+2+2+2+2+1 ⇒ 6
32. 2+2+2+2+2+2 ⇒ 2
33. 5+1+1+1+1+1+1+1 ⇒ 5
34. 4+2+1+1+1+1+1+1 ⇒ 4
35. 3+3+1+1+1+1+1+1 ⇒ 3
36. 3+2+2+1+1+1+1+1 ⇒ 6
37. 2+2+2+2+1+1+1+1 ⇒ 2
38. 3+1+1+1+1+1+1+1+1+1 ⇒ 3
39. 2+2+1+1+1+1+1+1+1+1 ⇒ 2
40. 1+1+1+1+1+1+1+1+1+1+1+1 ⇒ 1

P_{12} = {11,10,9,8,35,6,21,12,5,14,20,15,30,4,3,7,2,1}

partition impaire: le nombre de décompositions est impair (donc u est impair).

a+b+c ⇒ ppcm(a,b,c) :

1. 12 ⇒ 12
2. 10+1+1 ⇒ 10
3. 9+2+1 ⇒ 18
4. 8+3+1 ⇒ 24
5. 7+4+1 ⇒ 28
6. 6+5+1 ⇒ 30
7. 8+2+2 ⇒ 8
8. 7+3+2 ⇒ 42
9. 6+4+2 ⇒ 12
10. 5+5+2 ⇒ 10

11. 6+3+3 ⇒ 6
12. 5+4+3 ⇒ 60
13. 4+4+4 ⇒ 4
14. 8+1+1+1+1 ⇒ 8
15. 7+2+1+1+1 ⇒ 14
16. 6+3+1+1+1 ⇒ 6
17. 5+4+1+1+1 ⇒ 20
18. 6+2+2+1+1 ⇒ 6
19. 5+3+2+1+1 ⇒ 30
20. 4+4+2+1+1 ⇒ 4
21. 4+3+3+1+1 ⇒ 12
22. 5+2+2+2+1 ⇒ 10
23. 4+3+2+2+1 ⇒ 12
24. 3+3+3+2+1 ⇒ 6
25. 4+2+2+2+2 ⇒ 4
26. 3+3+2+2+2 ⇒ 6
27. 6+1+1+1+1+1+1 ⇒ 6
28. 5+2+1+1+1+1+1 ⇒ 10
29. 4+3+1+1+1+1+1 ⇒ 12
30. 4+2+2+1+1+1+1 ⇒ 4
31. 3+3+2+1+1+1+1 ⇒ 6
32. 3+2+2+2+1+1+1 ⇒ 6
33. 2+2+2+2+2+1+1 ⇒ 2
34. 4+1+1+1+1+1+1+1+1 ⇒ 4
35. 3+2+1+1+1+1+1+1+1 ⇒ 6
36. 2+2+2+1+1+1+1+1+1 ⇒ 2
37. 2+1+1+1+1+1+1+1+1+1+1 ⇒ 2

I_{12} = {12,10,18,24,28,30,8,42,6,60,4,14,20,2}

De même cherchons les partitions de 8 (il y a p(8)=22)

<u>partition paire</u> (donc v est pair) .

a+b+c+d ⇒ ppcm(a,b,c,d) :

1. 7+1 ⇒ ppcm(7,1)=7
2. 6+2 ⇒ ppcm(6,2)=6
3. 5+3 (*) ⇒ ppcm(5,3)=15
4. 4+4 ⇒ ppcm(4,4)=4
5. 5+1+1+1 ⇒ ppcm(5,1,1,1)=5
6. 4+2+1+1 ⇒ ppcm(4,2,1,1)=4
7. 3+3+1+1 ⇒ 3
8. 3+2+2+1 ⇒ 6
9. 2+2+2+2 ⇒ 2
10. 3+1+1+1+1+1 ⇒ 3
11. 2+2+1+1+1+1 ⇒ 2
12. 1+1+1+1+1+1+1+1 ⇒ 1

P_8 = {7,6,15,4,5,3,2,1}

partition impaire (donc v est impair).

a+b+c ⇒ ppcm(a,b,c) :

1. 8 ⇒ 8
2. 6+1+1 ⇒ 6
3. 5+2+1 ⇒ 10
4. 4+3+1 ⇒ 12
5. 4+2+2 ⇒ 4
6. 3+3+2 ⇒ 6
7. 4+1+1+1+1 ⇒ 4
8. 3+2+1+1+1 ⇒ 6
9. 2+2+2+1+1 ⇒ 2
10. 2+1+1+1+1+1+1 ⇒ 2

I_8 = {8,6,10,12,4,2}

On va montrer que ces deux partitions (*) donneront la solution de notre problème

8.4 L'ORDRE MAXIMAL

On a vu que l'ordre d , d'un élément (u,x,v,y) de G est un diviseur de m=ppcm(2|u|,3|v|) :

d | m où m= ppcm(2|u|,3|v|) avec sig(u)=sig(v)

T = {d | ppcm(2|u|,3|v|) avec sig(u)=sig(v)}
Pour trouver d_{max} il suffit de calculer l'ensemble T puis regarde son élément maximal.

On trouve |T|=73 , il y a 73 ordres, et parmi ces ordres il y a un maximal=1260. Voici la liste de ces ordres d'après le javascripts

https://fan2cube.fr/javascript/ordre_tout.html

avec les formules associées, les longueurs sont minimales

N°) formule → ordre

1) H H' -> 1

2) H^2 -> 2

3) H D H' B' D B -> 3

4) H -> 4

5) H D H D' -> 5

6) H^2 D^2 -> 6

7) H D H' A -> 7

8) H D^2 B -> 8

9) H D A^2 -> 9

10) H' D H A -> 10

11) H D A^2 P B' H D A^2 P B' -> 11

12) H D A B' -> 12

13) H' D H D' A B -> 14

14) H D^2 H D^2 -> 15

15) H D H' A B -> 16

16) H D H' D' A -> 18

17) H D H' G^2 -> 20

18) H^2 D H^2 A -> 21

19) H D A^2 P B' -> 22

20) H D^2 B' -> 24

21) H D H' G -> 28

22) H D^2 -> 30

23) H D A' B' -> 33

24) H^2 D H^2 G' -> 35

25) H^2 D' A' -> 36

26) H D H^2 G -> 40

27) H D^2 H^2 D' -> 42

28) H' D A' B -> 44

29) H D H G -> 45

30) H^2 D H A -> 48

31) H D A' H' P' G -> 55

32) H^2 D A' B -> 56

33) H D' A' -> 60

34) H D' -> 63

35) H D H A^2 G' -> 66

36) H D H' D A P' -> 70

37) H D H A' -> 72

38) H D' A' G' -> 77

39) H' D' A' -> 80

40) H D A -> 84

41) H D B -> 90

42) H D^2 A G^2 -> 99

43) H D -> 105

44) H' D' H D A B' P' G' -> 110

45) H D' H A' D B -> 112

46) H D A G' -> 120

47) H' D A' G' -> 126

48) H D A' G -> 132

49) H D' H A' -> 140

50) H D' A' B^2 -> 144

51) H D H A G B' -> 154

52) H D' H A^2 G' -> 165

53) H D B^2 -> 168

54) H D B' -> 180

55) H^2 D A B^2 -> 198

56) H D' B G' -> 210

57) H D A' B -> 231

58) H' D A' G^2 -> 240

59) H D A G -> 252

60) H' D' H' A G' -> 280

61) H D B G -> 315

62) H^2 D A' B' G' -> 330

63) H D H A B^2 -> 336

64) H D A' -> 360

65) H D B G' -> 420

66) H' D A' B^2 G' -> 462

67) H D^2 H A' G' -> 495

68) H D^2 A G' -> 504

69) H' D' H' A' G^2 -> 630

70) H' D' H' A' B^2 -> 720

71) H^2 D' A' B -> 840

72) H' D' H' A' G B -> 990

73) H D' H A' B^2 -> 1260

Pour trouver l'ordre 11, il suffit de trouver les ordres 22, 33, 44, 55, 66, 77 , ect ... car on a :

$V^{11k} = (V^k)^{11}$

par ex :

V = H D A^2 P B' $\rightarrow$ ordre 22

V^2 = (H D A^2 P B')^2 ordre 11

$|V^2|$ = 12* = longueur minimale (ordre 11)

On peut aussi trouver d_{max} par :

$d_{max} = \max T = \max \{ppcm(2|u|,3|v|)\}$

$$d_{max} = \max_{sig(u)=sig(v)} \{ ppcm(2|u|, 3|v|) \}$$

on doit trouver u,v avec sig(u)=sig(v) tel que
ppcm(2|u|,3|v|) soit maximal.

Pour ça on calcule |u|,|v|, avec sig(u)=sig(v) et on regarde si ppcm(2|u|,3|v|) est maximal.

P_{12} = {11,10,9,8,35,6,21,12,5,14,20,15,30,4,3,7,2,1}
I_{12} = {12,10,18,24,28,30,8,42,6,60,4,14,20,2}

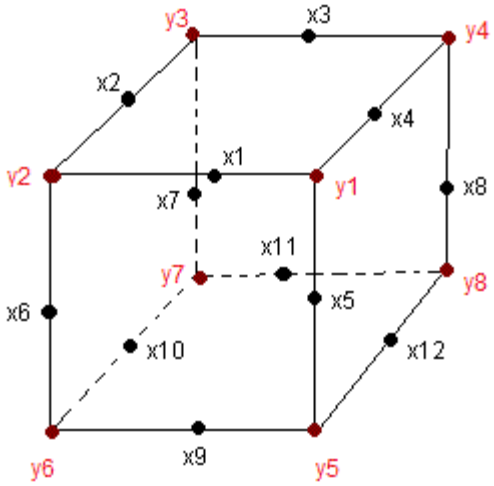
P_8 = {7,6,15,4,5,3,2,1}
I_8 = {8,6,10,12,4,2}

comme sig(u) = sig(v) on prend donc u,v toutes les deux paires ou impaires
voyons quelques valeurs
$u \in I_{12}$, $v \in I_8$
(30,12) ⇒ ppcm(2x30,3x12)=180
(18,10) ⇒ ppcm(2x18,3x10)=180
(12,8) ⇒ ppcm(2x12,3x8)=24
(42,10) ⇒ ppcm(2x42,3x10)=420
...
...

$u \in P_{12}$, $v \in P_8$
(7,15) ⇒ ppcm(2x7,3x15)=630
(14,15) ⇒ ppcm(2x14,3x15)=<u>1260</u>
(30,7) ⇒ ppcm(2x30,3x7)=420

(35,6) ⇒ ppcm(2x35,3x6)=630
...
...
Les calculs nous montre que le maximal 1260 est atteint par des permutations paires sig(u)=sig(v)=1 et que u et v valent
u = (7-cycle)(2-cycle)(2-cycle)(1-cycle)
v = (5-cycle)(3-cycle)
|u| = ppcm(7,2,2,1)=14
|v| = ppcm(5,3)=15
ppcm(2x14,3x15)=1260

8.5 L'ORDRE MAXIMAL DANS G



Sommets et arêtes

C'est pratiquement fini, il suffit de prendre un élément de G^+ d'ordre maximal et montrer qu'il est dans G
On prend
$(u,x,v,y)\in G^+$
u=(1,7,12,5,2,4,3)(8,10)(9,11)(6)
x=(1,0,0,1,0,0,1,0,0,1,0,0)
v=(4,6,5,8,7)(1,2,3)
y=(1,1,0,2,1,1,2,1)
x_1=(bv)=1, x_2=(bo)=0, ...
x_4=(br)=1, x_5=(vr)=0, ...
y_2=(bvo)=1, y_4=(bkr)=2, ...

(u,x,v,y) vérifie toutes les conditions pour être dans G, $(u,x,v,y)\in G$ et son ordre 1260

NOTE: On a la formule associée $DH^2B'PB'$, et $(DH^2B'PB')^{1260} = I$

On peut noter aussi que $(D\,{}^tH)^{1260} = I$ donne aussi l'ordre maximal , mais évidemment ce n'est pas un élément de G ni de G^+

<u>Résumons</u>

1. L'ordre ne dépend pas de l'orientation
2. Un ordre d, est donné par :

   $d \mid m$ où $m=ppcm(2|u|,3|v|)$ avec $sig(u)=sig(v)$

3. L'ordre maximal d_{max} est donné par

$$d_{max} = \max_{sig(u)=sig(v)} \{ppcm(2|u|, 3|v|)\}$$

4. L'ordre maximal est atteint par:
   u = (7-cycle)(2-cycle)(2-cycle)(1-cycle) ; permutation paire
   v = (5-cycle)(3-cycle) ; permutation paire

   d_{max}=ppcm[2.ppcm(7,2,2,1),3.ppcm(5,3)]

Rappelle la formule qui donne l'ordre 1260: $DH^2B'PB'$ (J. B. Butler)
Il est remarquable que l'ordre maximal du Rubik

est un quatrix[1] !! , $1260 = \frac{\left(\frac{4!+4}{4}\right)!}{4}$, il suffit de remarquer que 1260 = 35.36 = 7.5.6.6 = 7.6.5.3.2 = 7!/4

Voici un javascript pour calculer l'ordre maximal et l'ordre d'un élément.

https://fan2cube.fr/javascript/ordre_maxi.html

https://fan2cube.fr/javascript/ordre_calcul.html

[1] Un quatrix est un entier qui s'écrit avec quatre chiffres '4' et avec les 8 opérations suivantes : { +, -, x, /, $\sqrt{}$, !, a^b, 4^0 }

9 LE NOMBRE D'ÉLÉMENTS D'ORDRE DE 2

Il est intéressant de calculer le nombre d'éléments de G d'ordre 2, cela nous permet de voir comment ça marche dans G ....

Un élément s de G d'ordre 2 si $s^2=1$, voyons combien a-y-t-il ce genre d'états.

Soit O_2 l'ensemble d'éléments d'ordre 2 de G.

On peut partager cet ensemble en trois ensembles.

1. V_+ seulement les sommets bougent

2. E_+ seulement les arêtes bougent

3. T les deux, sommets et arêtes bougent.

Voyons sur V_+

$\mu \in V_+$ ça signifie que les arêtes sont invariantes ⇒ u=1 et x=0 il reste $\mu=(v,y) \in S_8 \times Z_3^8$, v bouge un certain nombre de sommets et peut-être laisse fixes certain d' autres.

Propriété1 : v ne modifie pas l'orientation des sommets fixes .

démonstration : supposons que v modifie l'orientation du sommet fixe y_5 par exemple, alors on aura donc:

v: $y_5 \dashrightarrow 1+y_5$

v^2: $y_5 \dashrightarrow 2+y_5$

v3: $y_5 \dashrightarrow 3+y_5 = y_5 \pmod 3$

Quand on applique v trois fois , les sommets fixes reviennent à l'état initial, si les sommets mobiles mettent k fois pour revenir à l'état initial alors v met d=ppcm(k,3) pour revenir à l'état initial c'est-à-dire d est l'ordre de v, vd=1 mais d=ppcm(k,3) ≥ 3 , donc v est d'ordre 3 (minimum) ce qui contredit que v est d'ordre 2.

* v est pair car les arêtes ne bougent pas sig(u)=sig(id)=1=sig(v). (ce qui justifie la notation V_+)

v est composé donc de transpositions (disjoints, en Rubik les cycles sont toujours disjoints) en nombre pair c'est-à-dire v est de la forme:

v=(a,b)(c,d) ou

v=(a,b)(c,d)(e,f)(g,h)

On est maintenant en mesure de compter V_+ .

* sélectionner un nombre p de couples (a,b) à échanger.

* sachant que chaque couple (disjoint) apporte 3 orientations: en effet dans un k-cycle disjoint à 3 orientations on a 3k orientations mais le cycle doit vérifier la loi des twists: si l'orientation des (k-1) sommets sont connus alors le dernier sera automatiquement connu, on aura donc $\frac{3^k}{3}$=3k-1 au lieu de 3k orientations. Finalement

un k-cycle disjoint apporte 3k-1 orientations. Dans notre cas k=2.

* Une fois choisi p couples on peut les placer comme on veut, par ex pour p=3, on a: $c_1c_2c_3$, $c_1c_3c_2$, $c_2c_1c_3$, ... il y a p! de placements mais c'est la même permutation $u=c_1c_2c_3= c_1c_3c_2= c_2c_1c_3=$ ... puisque ce sont des cycles disjoints donc ils sont permutables. Chaque parquet de p! couples c'est en réalité une seule permutation, donc il faut diviser par p! $\Rightarrow \frac{1}{p!}$

cas: (a,b)(c,d) -→ $\frac{1}{2!}\binom{8}{2}\binom{6}{2}3^2 = 1890$

<u>explication</u> :

(a,b)-→$\binom{8}{2}$ on choisit 2 sommets parmi 8 (il reste donc 6)

(c,d)-→$\binom{6}{2}$ on choisit 2 sommets parmi 6.

$\frac{1}{2!}$ -→ diviser par 2! car on a 2! placements identiques.

3^2 -→ 3 orientations et 2 couples

cas: (a,b)(c,d)(e,f)(g,h) -→ $\frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}3^4 = 8505$

donc au total

$|V_+| = \frac{1}{2!}\binom{8}{2}\binom{6}{2}3^2 + \frac{1}{4!}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}3^4 = 10395$

On fait la même chose pour E_+ . Un état-arête est $\mu=(u,x)\in S_{12} \times Z_2^{12}$, v=id, y=0.

Contrairement à v, u peut renverser les arêtes fixes, rien ne lui est interdit.

Et puis comme les sommets ne bougent pas la signature de u vaut 1, sig(u)=1 , u est pair (d'où notation E_+) . On va donc sélectionner des couples comme pour V_+ .

* 0 couple: Aucun couple-arête à échanger, mais les arêtes peuvent renverser

$$\left(\frac{1}{0!}\binom{12}{0}2^0\frac{2^{12}}{2}-1\right)$$

dans 2^{12} on a compté le vecteur nul (0,0,...,0) c'est-à-dire identité u=id et x=0 c'est pourquoi il faut enlever 1.

* 2 couples à échanger:

$$+\frac{1}{2!}\binom{12}{2}\binom{10}{2}2^2\frac{2^8}{2}$$

Contrairement à V_+ on doit traiter les arêtes fixes qui peuvent renverser. Les 8 arêtes restant doivent aussi vérifier la loi de flips: $2^8/2$

* 4 couples à échanger:

$$+\frac{1}{4!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}2^4\frac{2^4}{2}$$

* 6 couples à échanger:

$$+\frac{1}{6!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}\binom{2}{2}2^6$$

= 8080447 = $|E_+|$

Pour v impair on a:

$|V_-| = \frac{1}{1!}\binom{8}{2}3^1 + \frac{1}{3!}\binom{8}{2}\binom{6}{2}\binom{4}{2}3^3 = 11424$

Pour u impair on a:

$|E_-| =$
$\frac{1}{1!}\binom{12}{2}2^1\frac{2^{10}}{2} + \frac{1}{3!}\binom{12}{2}\binom{10}{2}\binom{8}{2}2^3\frac{2^6}{2} + \frac{1}{5!}\binom{12}{2}\binom{10}{2}\binom{8}{2}\binom{6}{2}\binom{4}{2}2^5\frac{2^2}{2}$

= 7607424

finalement $|O_2|$ vaut:

$|O_2| = |V_+| + |E_+| + |V_+|\,|E_+| + |V_-|\,|E_-|$

$|O_2|$ = 10395 + 8080447 + (10395 x 8080447) + (11424 x 7607424) = 170911549183 wwwoooaa ....

N_2 = 170911549183 ; le nombre d'éléments d'ordre 2

9.1 LE NOMBRE D'ÉLÉMÉNTS D'ORDRE 3

On pose :

$$S_{(a,b)} = \frac{8!\,3^{b-1}9^a}{a!\,b!\,3^a}$$

$$A_{(a,b)} = \frac{12!\,4^a}{a!\,b!\,3^a}$$

$S = S_{(0,8)} + S_{(1,5)} + S_{(2,2)}$; 3a+b=8, a=0,1,2

S = 2187 + 81648 + 272160 = 355995

$A = A_{(0,12)} + A_{(1,9)} + A_{(2,6)} + A_{(3,3)} + A_{(4,0)}$; 3a+b=12, a=0,1,2,3,4

A = 1+1760+591360+31539200+63078400 = 95210721

On démontre alors le nombre d'éléments d'ordre 3 est :

$N_3 = SA - 1$;

$N_3 = (355995)(95210721) - 1 = 33894540622394$

$N_3 = 33894540622394$.

9.2 LES ORDRES DANS G

Déjà en 1981, Jesper GERVED, Torben Maack BISGAARD ont fait un programme pour calculer le nombre d'ordres du Rubik's Cube et pour chaque ordre le nombre d'états correspondants. Voici le résultat, ces ordres sont classés de rare vers abondant ...

[l' ordre, le nombre d'états]

1. [1, 1],
2. [11, 44590694400],
3. [2, 170911549183], ; le nombre d'états d'ordre 2

4. [3, 33894540622394], ; le nombre d'états d'ordre 3
5. [5, 133528172514624],
6. [7, 153245517148800],
7. [22, 927085127270400],
8. [4, 4346957030144256],
9. [55, 4854321355161600],
10. [110, 4854321355161600],
11. [80, 13349383726694400],
12. [15, 14385471333209856],
13. [33, 15874019662233600],
14. [14, 23298374383021440],
15. [21, 39337151559333120],
16. [1260, 51490480088678400],
17. [9, 55333752398428896],
18. [10, 65250897836352192],
19. [35, 65526218912563200],
20. [280, 68653973451571200],
21. [28, 97419760907673600],
22. [315, 99309879652515840],

23. [44, 100120377950208000],
24. [99, 104367909135974400],
25. [720, 120144453540249600],
26. [112, 128726200221696000],
27. [6, 140621059298755526],
28. [16, 150731886270873600],
29. [495, 174755568785817600],
30. [990, 174755568785817600],
31. [154, 187238109413376000],
32. [77, 187238109413376000],
33. [45, 197329441659727104],
34. [20, 198732245664927744],
35. [165, 213590139627110400],
36. [330, 213590139627110400],
37. [140, 223125413717606400],
38. [105, 232824419423354880],
39. [504, 238381852262400000],
40. [840, 240288907080499200],
41. [336, 257452400443392000],

42. [63, 264371433705308160],

43. [8, 294998638981939200],

44. [70, 353490834273730560],

45. [462, 374476218826752000],

46. [231, 374476218826752000],

47. [630, 395380140162416640],

48. [66, 404051175250329600],

49. [240, 407156203664179200],

50. [126, 425696352223887360],

51. [18, 520622849158124832],

52. [360, 571019888909352960],

53. [132, 637129677864960000],

54. [56, 671205306846412800],

55. [252, 689877080447385600],

56. [144, 714192029378150400],

57. [42, 737199776831097600],

58. [198, 759701292082790400],

59. [48, 911497647410380800],

60. [420, 961155628321996800],

61. [168, 1050269239266508800],

62. [40, 1136258380254412800],

63. [210, 1339232732046950400],

64. [72, 1681092660339671040],

65. [84, 1697725818678067200],

66. [90, 1925069051617383168],

67. [120, 1947044011463147520],

68. [30, 2033284208966740224],

69. [12, 2330232827455554048],

70. [180, 2453889005738311680],

71. [36, 3186202597973176320],

72. [24, 3293932519796244480],

73. [60, 4601524692892925952]

Les ordres de rare vers abondant ...

[1, 11, 2, 3, 5, 7, 22, 4, 55, 110, 80, 15, 33, 14, 21, 1260, 9, 10, 35, 280, 28, 315, 44, 99, 720, 112, 6, 16, 495, 990, 154, 77, 45, 20, 165, 330, 140, 105, 504, 840, 336, 63, 8, 70, 462, 231, 630, 66, 240, 126, 18, 360, 132, 56, 252, 144, 42, 198, 48, 420, 168, 40, 210, 72, 84, 90, 120, 30, 12,180, 36, 24, 60]

L'ordre 11 est très rare, l'ordre 60 il y en a beaucoup .

9.3 L'ENTROPIE DU RUBIK'S CUBE

Gâce à la table des [ordre, nbr d'état] on peut définir une entropie sur le Rubik's Cube.

En effet pour définir une entropie il faut connaitre 3 choses :

1) Avoir un ensemble d'états .

2) À chaque état μ on peut associer un nombre q

3) Connaitre le nombre d'états Ω ayant la même valeur q

Alors l'entropie S de μ est par définition :

$S = \log_{10} \Omega$

Soit E (|E|=Ω) l'ensemble des états ayant le même q , on dit que E est un macro-état, pourque le macro-état E apparaisse il suffit que l'un des éléments de E apparaît.

Pour nous le q sera l'ordre de μ

$\mu = e \bullet V$

$\mu^d = e$, ou c'est la même chose $V^d = I$

par ex

¤ V = H D H' G ⇒ d=28 ⇒ Ω = 97419760907673600

$S = \log_{10} \Omega$

$S = \log_{10}(97419760907673600) \simeq 16{,}99$

¤ V = H D A^2 P B' H D A^2 P B' ⇒ d=11 ⇒ Ω = 44590694400

$S = \log_{10} \Omega$

$S = \log_{10}(44590694400) \simeq 10{,}65$

¤ V = H D' A' ⇒ d=60 ⇒ Ω = 4601524692892925952

$S = \log_{10} \Omega$

$S = \log_{10}(4601524692892925952) \simeq 18{,}66$

¤ V = H H' ⇒ d=1 ⇒ Ω = 1

$S = \log_{10} \Omega$

$S = \log_{10}(1) = 0$

Voici un Javascript qui permet de calculer l'entropie d'une formule V (ou l'état μ=e•V)

https://fan2cube.fr/entropie_ordre.html

9.4 LA CHROMATIQUE D'UN ÉTAT

On pose :

b = le nombre de blanc d'une face

j = le nombre de jaune d'une face

v = le nombre de vert d'une face

k = le nombre de klein d'une face

o = le nombre d' orange d'une face

r = le nombre de rouge d'une face

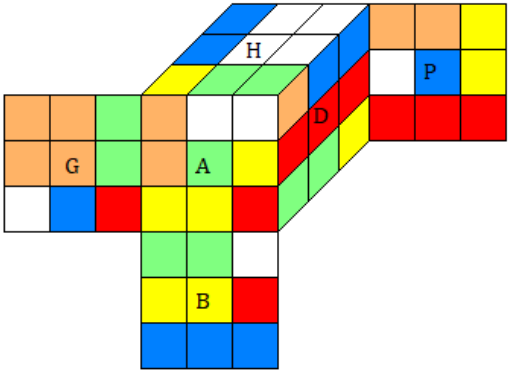
La chromatique de la face Haut :

$\chi_H = 81 - (b^2+j^2+v^2+k^2+o^2+r^2)$

Pour l'état μ , la chromatique de l'état μ :

$\chi_\mu = (\chi_H + \chi_B + \chi_A + \chi_P + \chi_G + \chi_D)/6$

par exemple :



l'état μ=e•(ADHGB)

$\chi_H = 81 - (4^2+2^2+2^2+1) = 56$

$\chi_B = 81 - (3^2+2^2+2^2+1+1) = 62$

$\chi_A = 81 - (3^2+2^2+2^2+1+1) = 62$

$\chi_P = 81 - (3^2+2^2+2^2+1+1) = 62$

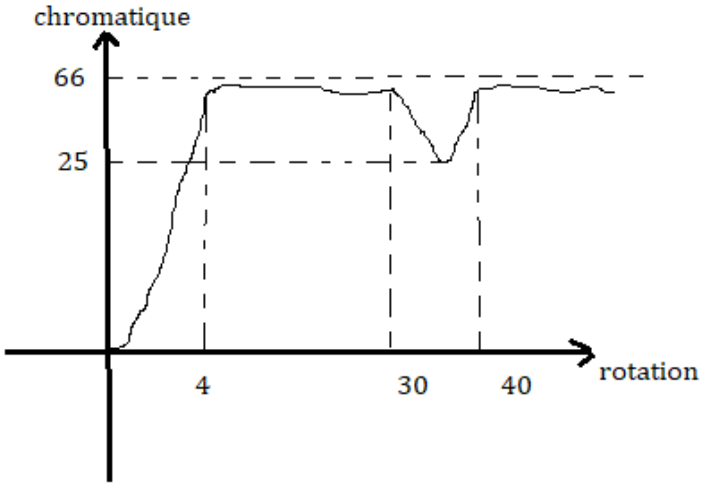
$\chi_G = 81 - (4^2+2^2+1+1+1) = 58$

$\chi_D = 81 - (3^2+2^2+2^2+1+1) = 62$

$\chi_\mu = (\chi_H + \chi_B + \chi_A + \chi_P + \chi_G + \chi_D) = 362/6$

Le minimum de la chromatique d'une face est 0, quand la face a une seule couleur.

Le maximum de la chromatique d'une face est 66, quand la face possède 6 couleurs et aucune apparait plus de 3 fois càd $81 - (2^2+2^2+2^2+1^2+1^2+1^2)$



Lorsqu'on mélange le Cube au hasard , la graphe montre que la chromatique est maximum en quelque rotations et elle oscille autour de cette valeur. Puis de 30 à 40 rotations χ_μ descend à 25, et au-delà de 40 rotations

$\chi_\mu \geq 57$

pour $\chi_\mu = 0$, on a un seul état, l'état résolu

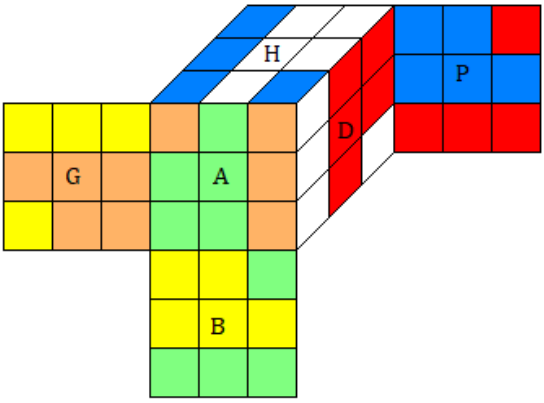
pour $\chi_\mu = 30$, on a 12 états (une rotation)

pour un χ_μ donné , il se peut qu'il y ait beaucoup états correspondants.

Le but : On cherche les états (les motifs) dont les faces ont le même nombre chromatique .

exemple :

V = H'A D'A'D PH'P' DPD' HP'H



l'état "pd" = e•V

$\chi_H = 81 - (5^2+4^2) = 40$

$\chi_H = \chi_B = \chi_A = \chi_P = \chi_G = \chi_D$

$\chi_\mu = 40$

Le SuperFlip

$\chi_H = 81 - (5^2+1+1+1+1) = 52$

$\chi_H = \chi_B = \chi_A = \chi_P = \chi_G = \chi_D$

$\chi_\mu = 52$

10 QUELQUES SOUS GROUPES DE M

Position du problème : On mélange le Cube avec un certain type de rotations, peut-on restaurer le Cube avec ce même type de rotations ??

Par exemple on mélange le Cube avec seulement deux rotations H, D. Peut-on restaurer le Cube uniquement avec ces deux rotations H, D ?? Si oui dans ce cas, il faudrait trouver de nouvelles formules qui pivotent deux sommets mais composées uniquement en H, D, pas évident !! de plus si les centres sont orientés, il faudrait trouver des formules qui pivotent les centres, mais composées uniquement les rotations H, D !! pas évident du tout !.

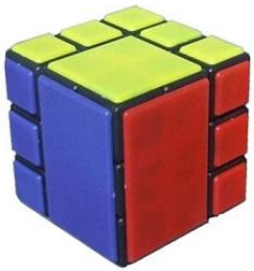
Ceci revient à trouver un algorithme de résolution pour le BigBlock.

Il est donc intéressant d'étudier d'un certain sous groupe de M et savoir combien y a-t-il de nombre d'éléments ? , quels motifs engendent ces sous groupes ? etc ...

¤ $Q = < H,D >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}|$ = 73483200 ; le groupe du BigBlock



BigBlock

<u>Résolution du BigBlock</u> :

1) On range les sommets-Bas avec:

(HDA)->(BAD) = [DH]

$(BAD)^{+} = [DH]^2$

2) One fois les 2 sommets-Bas sont bien placés, les sommets-Haut sont automatiquement sont bien placés (quitte à faire des rotations H) , on pivote les sommets-Haut par:

$(HAG)^{-}(HGP)^{+} = (DHD'H\ DH^2D'H^2\ )(D'H'DH'D'H^2DH^2)$

$(HGP)^{+}(HPD)^{+}(HDA)^{+} = DHD'H\ DH^2D'H^2$ (perturber les arêtes)

$(HAG)\cdot(HDA)\cdot(HPD)^{-} = D'H'DH'D'H^2DH^2$ (perturber les arêtes)

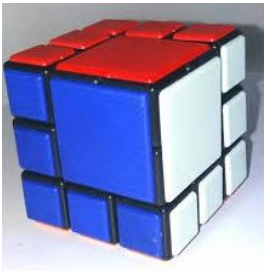
2) On range les arêtes avec:

$(HG)\text{->}(HD)\text{->}(HA) = D\,.(DH)^2\,(D'H')^2\;.D'HD'$

¤ $Q = < H,D,A >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V\,,\, V \in Q\}$

$|\mathcal{S}|$ = 170659735142400 ; le groupe du Fused

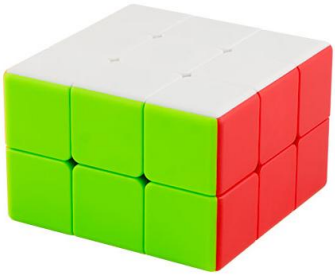


Fused

¤ $Q = < H,B,D^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V\,,\, V \in Q\}$

$|\mathcal{S}| = (8!)^2 = 1625702400$; le groupe du Domino



Domino

¤ $Q = < H,B,A^2,P^2,G^2,D^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}| = (8!)^2 .12 = 12$. Domino

* Pour un sommet, si on est en Haut on peut aller partout en Haut (avec H) , si on est en Bas on peut aussi aller partout en Bas (avec B) , on passe de Haut en Bas par D^2 par ex. Donc pour un sommet on peut aller partout c'est donc c'est S_8

* Même raisonnement pour une arête Haut/Bas elle peut aller partout en 8 positions donc c'est aussi S_8

* Pour les arêtes-équateur on a affaire à S_4 mais le mouvement a une contrainte il doit être déphasé avec les sommets en effet

quand

rotation H: $\begin{cases} \text{sig(sommets)} = -1 \\ \text{sig(arêtes\_équateur)} = 1 \end{cases}$

rotation D^2: $\begin{cases} \text{sig(sommets)} = 1 \\ \text{sig(arêtes\_équateur)} = -1 \end{cases}$

d'où $S_8 S_8 S_4/2$

donc finalement on a $|\mathcal{S}| = 8! .8! .4!/2 = 12$. Domino

¤ $Q = < H^2, D^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}| = 12$

¤ $Q = < H^2, D^2, A^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}| = 2\ 592$ $(=(\frac{4!}{4})^4 \sqrt{4}$, un quatrix)

¤ $Q = < H, B, A, P, G^2, D^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}| = 2^{16} 3^{14} 5^3 7^2 11$

¤ $Q = < H^2,B^2,A^2,P^2,G^2,D^2 >$

$\mathcal{S} = \{\mu \mid \mu = e \bullet V , V \in Q\}$

$|\mathcal{S}| = 2^{13}\,3^4$; le groupe Carré

On pose :

$K = < H^2,B^2,A^2,P^2,G^2,D^2 >$, On va raisonner comme pour le cas M agit sur les autocollants=X, le résultat de cette action donne G, ce sont des éléments de G^+ qui vérifient les 3 lois, et on a $|M|=|G|$.

Ici c'est pareil. K agit sur X pour donner disons $K^+ \subset G^+$ et K' = {K^+ et vérifié les 3 lois } ;

on a: $|K|=|K'|$

$K^+ = E \times V$; E=états-arêtes, V=états-sommets

voyons ce que c'est K^+ .

On sait que seules les rotations A, P modifient l'orientation des arêtes, mais A^2, P^2 ne modifient pas l'orientation des arêtes donc pour les arêtes $\mathbb{Z}_2$ n'intervient pas.

Pour les sommets c'est pareil, les $H,^2B^2,A^2,P^2,G^2,D^2$ ne modifient pas l'orientation des sommets donc $\mathbb{Z}_3$ n'intervient pas non plus dans les sommets.

D'autre part

E est divisé en 3 morceaux (3 orbites) α, β, γ et V divisé en 2 morceaux (2 orbites) δ, λ .

α={(AD),(AG),(PG),(PD)}

β={(HA),(HP),(BP),(BA)}

γ={(HG),(HD),(BD),(BG)}

δ={(HDA),(HGP),(BGA),(BDP)}

λ={(HAG),(HPD),(BPG),(BAD)}

et

$K^+ = S_\alpha \times S_\beta \times S_\gamma \times S_\delta \times S_\lambda$

Dans α les arêtes se baladent où qu'elles veulent donc on a $S_\alpha = S_4$, même chose pour les autres orbites.

$K^+ = S_4 \times S_4 \times S_4 \times S_4 \times S_4$

d'où

$|K^+| = (4!)^5 \Rightarrow |K'| = |K^+|/2.2.3$

$|K| = |K'| = (4!)^5/2.2.3$ on divise par (2.2.3) pour respecter les 3 lois du Rubik's Cube.

$|K| = (4.3.2.1)^5/2.2.3 = 2^{15}\, 3^5/2.2.3 = 2^{13}\, 3^4$

finalement l'ordre du groupe Carré vaut :

$|\mathcal{S}| = 2^{13}\, 3^4 = 663552$ $(= (4!)^4 \frac{4}{\sqrt{4}}$; un quatrix !!)

<u>Propriétés de K</u> :

* K ne modifie pas les orientations des arêtes et des sommets .

* Les arêtes se trouvent dans les 3 tranches (orbites) h,d,a.

Les arêtes du tranche a ne peuvent pas aller au tranche d (par ex), donc il n'existe pas de formules σ composées uniquement $\{H^2,B^2,A^2,P^2,G^2,D^2\}$ qui donne le 3-cycle

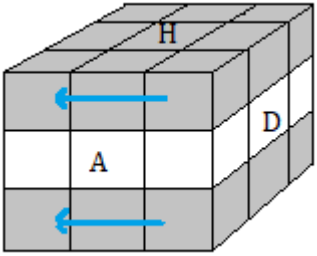
σ = (HG)->(HD)->(HP)

* Les sommet se divisent en 2 orbites :

-{(HDA), (HGP), (BGA), (BDP)}

-{(HAG), (HPD), (BAD), (BPG)}

¤ Voici un autre groupe intéressant, le groupe Glissant (Slice group) du Rubik's Cube.



HB'

On pose :

Q = < HB' , DG' , AP' >

$\mathcal{S}$ = {μ | μ=e•V , V∈Q}

Par définition : On appelle le groupe Glissant (deux rotations opposées dans le même sens) c'est un sous

groupe de G. Pour étudier ce groupe on va plutôt étudier le groupe défini par:

< b,g,p > qui n'est pas un sous groupe de G mais on démontre qu'il est isomorphe à $\mathcal{S}$. Allons-y

On pose :

T = < b,g,p > , T agit sur les arêtes E et sur les centres C, ce qui nous donne un morphisme f:

$f: T \rightarrow S_E \times S_C$

On on pose $T^+ = f(S_E) \times f(S_C)$

Mais $f(S_E)$ est divisé en 3 morceaux (3 orbites)

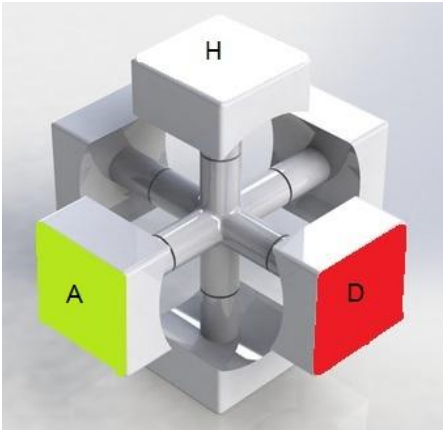
α={(AD),(AG),(PG),(PD)}

β={(HA),(HP),(BP),(BA)}

γ={(HG),(HD),(BD),(BG)}

et $S_\alpha=\mathbb{Z}_4$, $S_\beta=\mathbb{Z}_4$, $S_\gamma=\mathbb{Z}_4$, car les arêtes font des 4-cycles c'est-à-dire des rotations 90° d'un carré.

On a 6 centres qui se déplacent on a donc affaire à S_6 , mais il est clair qu'on n'a pas S_6 tout entier pour la simple raison que les centres sont collés dans le core, on n'a pas la permutation (H,A) par exemple, on a moins de permutations , mais moins de combien ???



Le core

Oublions les arêtes, regardons seulement les centres, ils sont collés dans le core. Faire la rotation d revient à faire ${}^{t}D$, on tourne le cube entier, b -→ ${}^{t}B$, g -→ ${}^{t}G$ ..., ce sont des rotations qui conservent le cube c'est donc $\mathfrak{D}$ le groupe de déplacement (Isometrie^{+} du cube), or $\mathfrak{D}=S_4$ il y a 24 rotations de ce type $|S_4|=24$

$T^{+} = S_\alpha \times S_\beta \times S_\gamma \times S_C = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times S_4 = \mathbb{Z}_4^3 \times S_4$

d'autre part on a signature(arête) = signature(centre) car pour les rotations h, d, a on a, par ex :

b = uc = (4-cycle-arête)(4-cycle-centre)

T = {T^{+} et sig(u) = sig(c)}

d'où

$[T| = |T^{+}|/2$

$|T| = 4^3 .4! /2$, on divise par 2 pour respecter la loi sig(u)=sig(c) .

$|T| = 4^3 (4.3.2.1)/2 = 2^9 .3/2 = 2^8 .3 = 768$

$|< b,g,p >| = 2^8 .3 = 768$

< b,g,p > est isomorphe à < HB' , DG' , AP' > l'isomorphisme est donné par les relations:

$b = HB' {}^tH'$

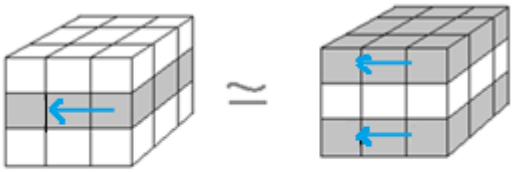
$g = DG' {}^tD'$

$p = AP' {}^tA'$

donc

$|\mathcal{S}| = 768$ (= 4x4x4!$\sqrt{4}$, un quatrix)

Remarque : L'orientation des arêtes n'intervient pas car les rotations tranches ne pivotent pas les arêtes sur place, càd une arête bien placée par <b,g,p> est automatiquement bien orientée



$b = HB' {}^tH'$

La définition du groupe Glissant est:

Q = < Z $\underline{Z}$ | Z rotation-donnée, $\underline{Z}$ opposé de Z, Z et $\underline{Z}$ dans le même sens. >

$\mathcal{S}$ = {μ | μ=e•V , V∈Q}

→Exemple le groupe Glissant du Megaminx

On pose :

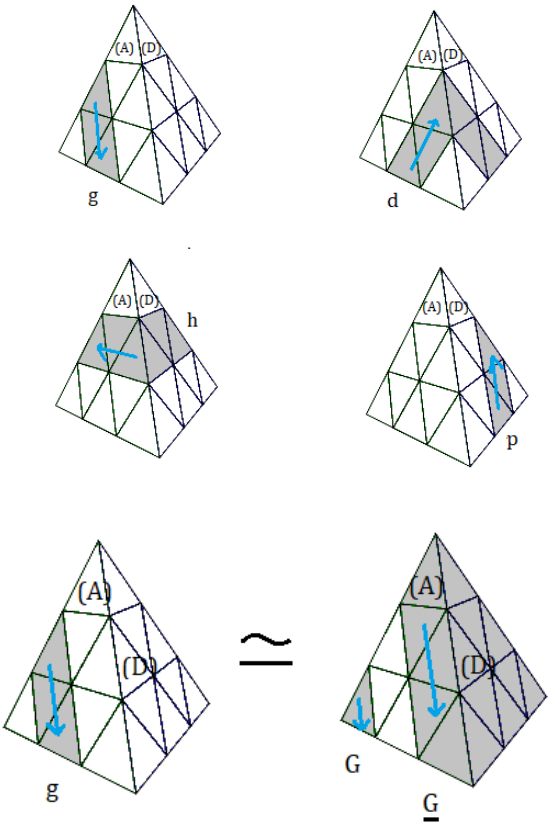
Q = < H$\underline{H}$', B$\underline{B}$', A$\underline{A}$', P$\underline{P}$', G$\underline{G}$', D$\underline{D}$' >

$\mathcal{S}$ = {μ | μ=e•V , V∈Q}

H $\underline{H}$'

$$|\mathcal{S}| = \frac{15!}{2} 4^{14} \frac{10!}{2} 6^9 3 =$$
$$= 96277552061212778121016639488000000$$

→Le groupe Glissant du Pyraminx



$g = {}^{t}g\, G'\, \underline{G'}$

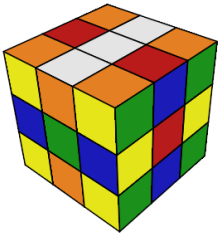
Q = < g, d, h, p >

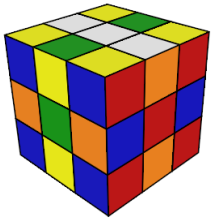
$\mathcal{S}$ = {μ | μ=e•V , V∈Q}

$|\mathcal{S}|$ = 933120

→Le groupe Glissant du Rubik's Cube donne des motifs assez jolis ...

* Spot, X, +





Et on observe que la motif de chaque face est de la forme:

x	y	x
z	t	z
x	y	x

une face

x'	y'	x'
z'	t'	z'
x'	y'	x'

face opposée

* Les sommets ont la même couleur x
* Les arêtes opposées ont la même couleur y, z
* La face opposée a des couleurs opposées x',y',z',t'

11 ALGORITHME DE THISTLETHWAITE

11.1 LE GRAPHE CAYLEY DE G

Définition : Le graphe Cayley de G ou le graphe du Rubik's Cube c'est:

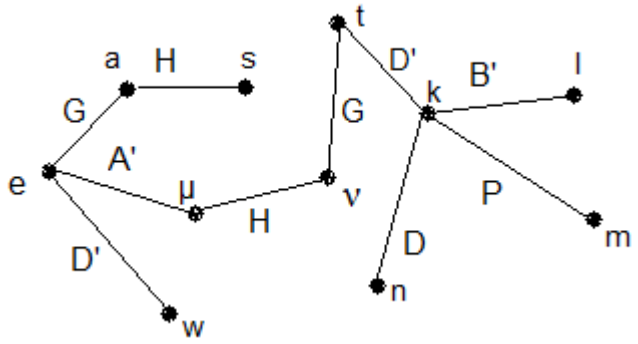
* Les sommets du graphe sont des états (les éléments de G).

* Les arêtes du graphe sont des rotations de base ou leur inverse c'est-à-dire si deux sommets μ,ν forment une arête (μ,ν) alors ils sont reliés par une rotation de base ou son inverse.

(μ,ν)=arête ⇒ $\mu \xrightarrow{V} \nu$ ou $\mu \xrightarrow{V'} \nu$ avec V∈{H,B,A,P,G,D}

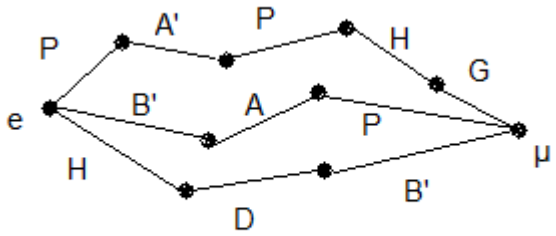
μ•V = ν ou μ•V' = ν

exemple : (a,s)=H , (t,k)=D'



Un chemin c(x,y) est une suite finie d'arêtes qui commence par x et se termine par y. Et la longueur d'un chemin est le nombre d'arêtes qu'il contient.

c(e,m)=A'HGD'P , longueur = 5



Parfois il y a plusieurs chemins pour aller de x à y, par ex pour aller de e à μ on a trois chemins

C_1(e,μ) = PA'PHG , longueur=5

$C_2(e,\mu)$ = HDB' , longueur=3

$C_3(e,\mu)$ = B'AP , longueur=3

La distance d(x,y) de x à y est le plus court chemin entre x et y

$$d(x,y) = \min_{c(x,y)} c(x,y)$$

Et le diamètre du graphe c'est la plus grande distance

$$\delta = \max_{x,y \in G} d(x,y)$$

On appelle δ aussi le nombre de Dieu.

On voit donc qu'un chemin n'est rien d'autre qu'une formule (plus précisément une l'écriture d'une formule).

La longueur d'un chemin est donc la longueur d'une formule.

donc pour chaque formule V on associe à une longueur |V| par exemple
$V = HB^2PA'D^3G'^2$
|V| = 10

Attention!! V = T n'implique pas |V| = |T| !!! ex: $A'=A^3$ mais $|A'|=1$ et $|A^3|=3$

Position du problème : En résolvant le Rubik's Cube, on se pose deux questions naturelles suivantes:

1- On se donne un nombre a, et se pose la question suivante:
-Existent-ils des situations (des états) dont on n'a aucun espoir de restaurer le Cube avec un nombre de rotations moindre que a ? autrement dit il faut au minimum a rotations pour s'en sortir.
exemple si on prend a = 2, il est clair qu'il y a des états qu'on ne peut pas s'en sortir avec une seule rotation !
Il est donc naturelle de se demander s'il y a des états les plus compliqués en augmentant a, par ex a=10, 11, ... nous montrerons par un raisonnement simple qu'il y a des états dont on ne peut pas s'en sortir avec 19 rotations donc il faut au minimum 20 rotations...

2- Une autre question aussi intéressante: On se donne un nombre b et se pose la question suivante:
-Quel que soit l'état, est-il toujours possible de s'en sortir avec b rotations (au maximum) ??
par exemple si on prend b=36540, peut-on toujours s'en sortir avec b=36540 rotations ? la réponse est sûrement 'oui', on a donc l'intérêt de diminuer b
Pour a : on augmente a pour atteindre les états les plus compliqués.
Pour b : on diminue b pour avoir le minimum de rotations nécessaires.
Soit m le nombre de rotations de la restauration, le problème revient donc à minorer et majorer m: $a \leq m \leq b$

1. Un nombre minimum de rotations

Un raisonnement simple permet de trouver qu'il y a des états qu'on ne peut pas s'en sortir avec 19 rotations (a=20)

- Le 1er coup : 6 faces à choisir {H,B,A,P,G,D} , on prend par ex la face A, on a alors 2 choix : A, A' et comme il y a 6 faces on a: 2x6=12 choix.

A: A,A',A^2 ⇒ 2x6 = 12

- Le 2ème coup : on évite de reprendre A sinon on revient au même point, donc 5 faces à choisir {H,B,P,G,D} ,on prend par ex la face D

D: D,D',D^2 ⇒ 2 x 5 = 10, comme on a 12 choix au 2ème coup d'où
12 x 10

- Le 3ème coup : on évite de reprendre D sinon on revient au même point, mais on peut reprendre A car D a modifié A, on ne revient pas au même point si on reprend A, donc 5 faces à choisir {H,B,A,P,G} , on prend par ex P

P: P,P',P^2 ⇒ 2 x 5 = 10, mais on a 12x10 choix d'où
12 x 10 x 10

- Le 4ème coup : on évite de reprendre P, donc 5 faces à choisir {H,B,A,G,D} , on prend par ex H

H: H,H',H^2 ⇒ 2 x 5 = 10,
mais on a maintenant 12x10x10 choix d'où
12 x 10x10x10
.....

Le nombre d'états en n rotations vaut donc:
$S = 12 + 12.10 + 12.10^2 + 12.10^3 + ... + 12.10^{n-1}$ (il y a n ternes)

$S = 12(1 + 10 + 10^2 + 10^3 + ... + 10^{n-1})$

$S = 12(10^n - 1)/(10 - 1) \approx 4.10^n/3$
$10^n \approx 3x4{,}3x10^{19}/4$
$10^n \approx 3{,}22x10^{19}$
En passant par ln
$n \approx [\ln(3{,}22)+19\ln(10)]/\ln(10)$
$n \approx 19{,}50$

d'où
$n = 20$

la borne inférieure est donc a = 20 autrement dit il existe des états dont on n'a aucun espoir de les restaurer avec 19 rotations !
on a $20 \leq m \leq b$

11.2 ANALYSE

Pour trouver le majorant b, Thistlethwaite a une idée géniale suivante:

On a d'un côté (M, .) le groupe des formules, et de l'autre côté G, l'ensemble des états.
Si on se donne une tour $\{\mathcal{K}_i\}_i$ de sous-groupes de M
$M = \mathcal{K}_0 \supset \mathcal{K}_1 \supset \mathcal{K}_2 \supset \mathcal{K}_3 \supset ... \supset \mathcal{K}_n = \{I\}$
à cette tour il correspond à une tour $\{E_i\}_i$ de sous-ensemble de G
$G = E_0 \supset E_1 \supset E_2 \supset E_3 \supset ... \supset E_n = \{e\}$
où les E_i sont des états atteints par les $\mathcal{K}_i$

$E_i = \{\mu \in G \mid \mu = e \bullet V, V \in \mathcal{K}_i\}$

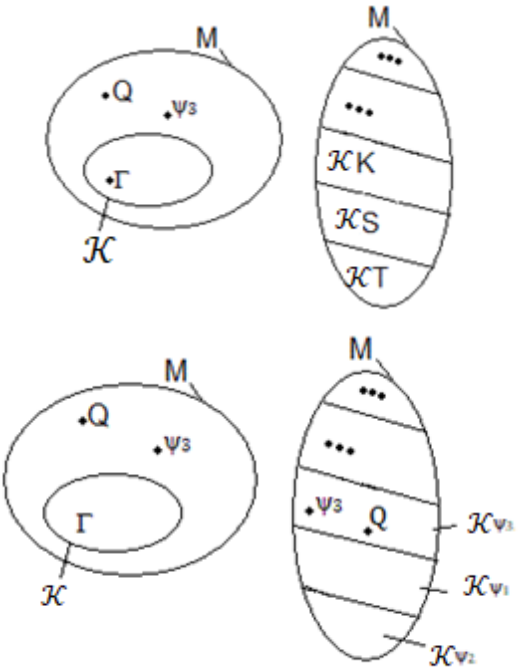
$$G \xrightarrow{\mathcal{K}_1} E_1 \xrightarrow{\mathcal{K}_2} E_2 \rightarrow \cdots \xrightarrow{\{I\}} \{e\}$$

Ainsi on a donc un algorithme de résolution (on part de G et on arrive à {e}), on pourrait alors calculer le nombre de rotations utilisées dans cet algorithme donc un majorant b de m.

11.3 LES CLASSES

Pour comprendre l'idée de Thistlethwaite, càd comment il compte le nombre de rotations, il faut connaître la notion de classes. Thistlethwaite a utilisé les classes pour compter les rotations c'est vraiment génial comme l'angle d'attaque.

Pour fixer les idées on va prendre simplement une tour à un étage :
Soit $\mathcal{K}$ un sous-groupe de M ($\mathcal{K}$ n'est pas forcement normal) et E les états atteints par $\mathcal{K}$ ($E=\{\mu \mid \mu = e \bullet V, V \in \mathcal{K}\}$)
$\mathcal{K} \subset M$, et $E \subset G$
$\mathcal{K}$ étant donné, les classes $\mathcal{K}\backslash M = \{ \mathcal{K}K, \mathcal{K}S, \mathcal{K}T, ... \}$ où les K, S, T, ... (dans M) sont, donc aussi données . Soient μ un état quelconque de G et Q la formule associée à μ :
$e \bullet Q = \mu \in G$



Une classe a un nombre fini d'éléments (puisque M est fini -c'est ici qu'on a besoin que M soit fini-), parmi ces éléments il y a un "plus court" , et on peut le prendre comme représentant de la classe.
Soient: $\mathcal{K}K = \mathcal{K}\psi_1$, $\mathcal{K}S = \mathcal{K}\psi_2$, $\mathcal{K}T = \mathcal{K}\psi_3$, ... où les $\psi_i \in M$ et sont des plus courts et $|\psi_i|$=longueur
on pose
$L = \text{Max}\ (|\psi_1|, |\psi_2|, |\psi_3|, \ldots.)$

Q étant un élément de M , mais comme les classes forment une partition de M donc Q se trouve quelque part dans

$\mathcal{K}\psi_1$, ou $\mathcal{K}\psi_2$, ou $\mathcal{K}\psi_3$, ...
supposons que Q soit dans $\mathcal{K}\psi_3$ ça signifie que Q est de la forme :
$Q = \Gamma\psi_3$ avec $\Gamma \in \mathcal{K}$
d'où

$Q = \Gamma\psi_3$
$Q\psi'_3 = \Gamma$
$e \bullet (Q\psi'_3) = e \bullet \Gamma$
$(e \bullet Q) \bullet \psi'_3 = e \bullet \Gamma$
$\mu \bullet \psi'_3 = e \bullet \Gamma = \nu \in E$, car Γ est dans $\mathcal{K}$
d'où:
$\mu \bullet \psi'_3 = \nu \in E$

Donc on passe de l'état $\mu \in G$ à l'état $\nu \in E$ au maximum L rotations.

NOTE Il est clair qu'on ne cherche pas les ψ_i à la main !!! , les ordinateurs sont là pour ça ...
En effet le nombre d'éléments d'une classe est fini, souvenez vous il vaut $|\mathcal{K}|$. Donc on peut très bien faire un programme qui cherche le plus court élément ψ d'une classe et le prend comme représentant . Pour trouver L là aussi il y a un nombre fini de classes (un nombre fini de ψ_i) , il vaut $|M|/|\mathcal{K}|$ donc on peut toujours trouver $L = \text{Max}(|\psi_1|, |\psi_2|, |\psi_3|, \dots)$ par ordinateur. Donc $\mathcal{K}$ est donné , L est donné.

11.4 MÉTHODE DE THISTLETHWAITE

Dans cette section on applique le couple (M, $\mathcal{K}$) par les couples ($\mathcal{K}_i$, $\mathcal{K}_{i+1}$)
Thistlethwaite a proposé la suite $\mathcal{K}_i$ des sous groupes de M suivantes :

$\mathcal{K}_0 = < H, B, A, P, G, D > = M$
$\mathcal{K}_1 = < H, B, A^2, P^2, G, D >$
$\mathcal{K}_2 = < H, B, A^2, P^2, G^2, D^2 >$
$\mathcal{K}_3 = < H^2, B^2, A^2, P^2, G^2, D^2 >$
$\mathcal{K}_4 = \{I\}$

$E_0 = \{\mu \mid \mu = e \bullet V, V \in \mathcal{K}_0\} = G$
$E_1 = \{\mu \mid \mu = e \bullet V, V \in \mathcal{K}_1\}$
$E_2 = \{\mu \mid \mu = e \bullet V, V \in \mathcal{K}_2\}$
$E_3 = \{\mu \mid \mu = e \bullet V, V \in \mathcal{K}_3\}$
$E_4 = \{\mu \mid \mu = e \bullet V, V \in \mathcal{K}_4\} = \{e\}$

Et il démontrait (grâce à l'ordinateur) que pour passer :
¤ de G à E_1, avec $|\psi_i| \leq 14$
¤ de E_1 à E_2, avec $|\psi_i| \leq 26$,
¤ de E_2 à E_3, avec $|\psi_i| \leq 30$,
¤ de E_3 à $E_4 = \{e\}$, avec $|\psi_i| \leq 34$,

Soit au maximum 14+26+30+34=104 rotations ,
$20 \leq m \leq 104$
NOTE: Avec quelques astuces on arrive à diminuer b=90 (14+20+26+30=90).

E_1 c'est l'ensemble des états dont toutes les arêtes sont bien orientées.

E_2 c'est l'ensemble des états dont toutes les arêtes et tous les sommets sont bien orientées.

E_3 c'est l'ensemble des états dont toutes les arêtes sont bien orientées et tous les sommets sont bien rangés.

E_4 c'est l'ensemble des états dont toutes les arêtes sont bien rangées et tous les sommets sont bien rangés, càd l'état résolu.

==> Passer de G à E_1 signifie : à partir de l'état $\mu \in G$ il existe une formule $V_0 \in \mathcal{K}_0$ avec $|V_0| \leq 14$, telle que $\mu \bullet V_0 = \mu_1 \in E_1$

==> Passer de E_1 à E_2 signifie : à partir de l'état $\mu_1 \in E_1$ il existe une formule $V_1 \in \mathcal{K}_1$ avec $|V_1| \leq 26$, telle que $\mu_1 \bullet V_1 = \mu_2 \in E_2$

==> Passer de E_2 à E_3 signifie : à partir de l'état $\mu_2 \in E_2$ il existe une formule $V_2 \in \mathcal{K}_2$ avec $|V_2| \leq 30$ telle que $\mu_2 \bullet V_2 = \mu_3 \in E_3$.

==> Passer de E_3 à E_4 signifie : à partir de l'état $\mu_3 \in E_3$ il existe une formule $V_3 \in \mathcal{K}_3$ avec $|V_3| \leq 34$ telle que $\mu_3 \bullet V_3 = \mu_4 \in E_4$

Remarque : Le travail Thistlethwaite est important, il nous dit deux choses:
1. On est sûr de s'en sortir !!.

2. Quel que soit l'état du Cube on le restaure au maximum 104 rotations.

3. Algorithme de Thistlethwaite :

a. Orienter les arêtes et les formules dans
< H, B, A, P, G, D > ; pas de contraintes sur les formules
b. Orienter les sommets, et les formules dans
< H, B, A^2, P^2, G, D > ; contraintes sur les formules
c. Placer les sommets , et les formules dans
< H, B, A^2, P^2, G^2, D^2 > ; contraintes sur les formules
d. Placer les arêtes, et les formules dans
< H^2, B^2, A^2, P^2, G^2, D^2 > ; contraintes sur les formules

Dans cet algorithme, la difficulté c'est connaitre par coeur le shéma d'orientation et les couleurs dominantes pour bien orienter les arêtes et les sommets !

Algorithme de Thistlethwaite version humain

1) Orienter les arêtes : pas de contraites sur les formules

a) Placer les arêtes-équateur dans l'équateur (arête sans couleur blanche, ni jaune)
$(HG) <-> (HP) = A[DH]A'H$

b) Orienter les arêtes
$(HG)°(HP)° = (A[DH]A'H)^2$

2) Orienter les sommets : les formules dans $< H,B,A^2,P^2,G,D >$

Orienter les sommets
$(HAG)^{+}(HGP)^{-} = [DH]^2 .G'[HD]^2G$

3) Ranger les sommets : les formules dans $< H,B,A^2,P^2,G^2,D^2 >$

a) Ranger les sommets-Bas
$(HDA)->(BAD) = A^2H'A^2HA^2$

b) Ranger les sommets-Haut
$(HDA)<->(HPD) = D^2H\ (D^2H')^2\ B.D^2H'D^2HD^2.B'$

4) Ranger les arêtes : les formules dans $< H^2,B^2,A^2,P^2,G^2,D^2 >$

a) Ranger les arêtes-Bas
$(HD)->(BD) = B^2A^2B^2\ (D^2P^2)^3\ B^2A^2B^2$

b) Ranger les arêtes-équateur
$(AD)<->(PD) = (D^2H^2)^3$

c) Ranger les arêtes-Haut
$(HG)->(HD)->(BD) = (A^2H^2A^2D^2)^2$

Durant les années on augmente le minorant a et on diminue le majorant b : $a=20 \leq m \leq b=104$

Jan/1981, Dan Hoey montre que : $21 \leq m \leq 140$
Jul/1981, Morwen Thistlethwaite montre que b=104 rotations suffisent : $21 \leq m \leq 104$
Mai/1992, Michael Reid montre b=56 : $21 \leq m \leq 56$
Jan/1995, Michael Reid : $21 \leq m \leq 42$
Jan/1995, Michael Reid : $22 \leq m \leq 42$
Aût/1998, Michael Reid a=24 (SuperFlip) : $24 \leq m \leq 42$

Aût/1998, Michael Reid a=26 (SuperFlip4Spot): 26 ≤ m ≤ 42
Nov/2005, Silviu Radu : 26 ≤ m ≤ 40
Jan/2006, Bruce Norskog : 26 ≤ m ≤ 38
Jan/2006, Silviu Radu : 26 ≤ m ≤ 36
Mar/2006, Silviu Radu : 26 ≤ m ≤ 35
Jul/2007, Silviu Radu : 26 ≤ m ≤ 34
Jan/2009, Tomas Rokicki : 26 ≤ m ≤ 32
Jan/2009, Tomas Rokicki : 26 ≤ m ≤ 31
Fév/2009, Tomas Rokicki : 26 ≤ m ≤ 30
Jui/2009, Tomas Rokicki : 26 ≤ m ≤ 29
Aût/2014, Tomas Rokicki et Morley Davidson : 26≤ m ≤26

Théorème (Tomas Rokicki et Morley Davidson, 2014) :
∀μ état, ∃V formule avec |V|≤26 telle que μ•V=e

Ils démontrent ainsi le diamètre du Rubik's Cube est 26.
ouf !! 33 ans de galère !! ...

4Spot face(A,P) et face(G,D) = Ω = $BP^2A^2BH'G^2D^2H'$ (12)

*Le SuperFlip de formule :
Φ = $D'H^2PG'$ AH'PBA $HB'GB^2$ A'DP'BA' H'P'HB'
Michael Reid a trouvé cette formule en 1995 par ordinateur et c'est Jerry Bryan qui démontre (1995) que c'est la plus courte formule |Φ| = 24

*Le SuperFlip4Spot de formule :
Π = H^2B^2G A^2 H'BD^2 PH'B'D GA^2D HB' D'GHA'P'
Michael Reid a trouvé cette formule par ordinateur, et a prouvé que c'est la plus courte formule |Π|=26
Une autre l'écriture de Π:
Π = A DG'PBA D'HBPD' B'D'PH^2 B^2P^2D GB^2DG

$|\Pi| = 26$, c'est le seul état de longueur maximale 26 qu'on connaît.

Le nom "SuperFlip4Spot" provient de la relation:

$\Pi = \Phi\Omega = \Omega\Phi$.

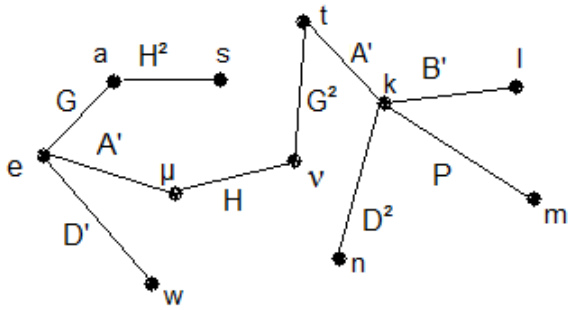
11.5 LA MÉTRIQUE FACE

Dans le graphe de Cayley, au lieu d'imposer deux états se lient par une rotation de base ou leur inverse on autorise aussi les carrées A^2, B^2, ...

(μ,ν)=arête $\Rightarrow \mu \xrightarrow{V} \nu$ ou $\mu \xrightarrow{V'} \nu$ ou $\mu \xrightarrow{V^2} \nu$ avec $V \in \{H,B,A,P,G,D\}$

$\mu \bullet V = \nu$, ou $\mu \bullet V' = \nu$, ou $\mu \bullet V^2 = \nu$

dans ce cas on dit qu'on est en métrique face , et les longueurs seront notées avec un 'f', par ex 20f, 1f, 17f, etc. ....



et la longueur du chemin sera compté
$|A^2|$ = 1f (f=face rotation)

c(e,n) = A'HG^{2}A'D^2 , longueur=5f

<u>1. Le nombre minimum de rotations en f</u>

On reprend le même raisonnement plus haut.

- Le 1er coup : 6 faces à choisir {H,B,A,P,G,D} , on prend par ex la face A, on a alors 3 choix : A, A', A^2 et comme il y a 6 faces on a: 3x6=18 choix.

A: A,A',A^2 ⇒ 3x6 = 18
- Le 2ème coup : on évite de reprendre A sinon on revient au même point, donc 5 faces à choisir {H,B,P,G,D} ,on prend par ex la face D
D: D,D',D^2 ⇒ 3 x 5 = 15, comme on a 18 choix au 2ème coup d'où
18 x 15

- Le 3ème coup : on évite de reprendre D sinon on revient au même point, mais on peut reprendre A car D a modifié A, on ne revient pas au même point si on reprend A, donc 5 faces à choisir {H,B,A,P,G} , on prend par ex P

P: P,P',P^2 ⇒ 3 x 5 = 15, mais on a 18x15 choix d'où
18 x 15 x 15

- Le 4ème coup : on évite de reprendre P, donc 5 faces à choisir {H,B,A,G,D} , on prend par ex H

H: H,H',H^2 ⇒ 3 x 5 = 15,
mais on a maintenant 18x15x15 choix d'où
18 x 15x15x15
.....

Le nombre d'états en n rotations vaut donc:
$S = 18 + 18.15 + 18.15^2 + 18.15^3 + ... + 18.15^{n-1}$ (il y a n ternes)

$S = 18(1 + 15 + 15^2 + 15^3 ... + 15^{n-1})$

$S = 18(15^n - 1)/(15 - 1) \approx 9.15^n/7$
$15^n \approx 7x4,3x10^{19}/9$
$15^n \approx 3,34x10^{19}$
En passant par ln
$n \approx [\ln(3,34)+19\ln(10)]/\ln(15)$
$n \approx 16,60$

d'où
n = 17
la borne inférieure est donc a = 17f autrement dit il existe des états dont on n'a aucun espoir de les restaurer avec

16f rotations !
on a $17f \leq m \leq b$.

Le résultat de Morwen Thistlethwaite montre que (dans le cas f-rotation)

Pour passer :
¤ de G à E_1, il y a 2048 ψ_i et le maxi $|\psi_i|=7f$, càd L=7f
¤ de E_1 à E_2, il y a 1082565 ψ_i et le maxi $|\psi_i|=13f$, càd L=13f
¤ de E_2 à E_3, il y a 29400 ψ_i et le maxi $|\psi_i|=15f$, càd L=15f
¤ de E_3 à E_4, il y a 663552 ψ_i et le maxi $|\psi_i|=17f$, càd L=17f

Soit au total b=52f rotations , $17f \leq m \leq 52f$
NOTE: Avec quelques astuces on arrive à diminuer b=45f (7f+10f+13f+15f) .

Durant les années on augmente le minorant a et on diminue le majorant b : $a=17f \leq m \leq b=52f$

Morwen Thistlethwaite : $17f \leq m \leq 52f$
Déc/1990, Hans Kloosterman : $17f \leq m \leq 42f$
Mai/1992, Michael Reid : $17f \leq m \leq 39f$
Mai/1992, Dik Winter : $17f \leq m \leq 37f$
Jan/1995, Michael Reid a=20f (SuperFlip) : $20f \leq m \leq 29f$
Déc/2005, Silviu Radu : $20f \leq m \leq 28f$
Avr/2006, Silviu Radu : $20f \leq m \leq 27f$
Mai/2007, Dan Kunkle et Gene Cooperman: $20f \leq m \leq 26f$
Mar/2008, Tomas Rokicki : $20f \leq m \leq 25f$
Avr/2008, Tomas Rokicki et John Welborn : $20f \leq m \leq 23f$
Aût/2008, Tomas Rokicki et John Welborn : $20f \leq m \leq 22f$
Jul/2010, Tomas Rokicki, Herbert Kociemba, Morley Davidson, et John Dethridge : $20f \leq m \leq 20f$

Théorème (Tomas Rokicki, Herbert Kociemba, Morley Davidson, et John Dethridge, 2010) :
$\forall \mu$ état, $\exists V$ formule avec $|V| \leq 20f$ telle que $\mu \bullet V = e$

Autrement dit ils démontrent que le diamètre du Rubik's Cube est exactement 20f ($|A^2| = 1f$) . Il fallait 30 ans pour répondre à cette question !

Note :
Voici quelques états les SuperLoin en f-rotation (20f)
Le SuperFlip avec la formule
$\Phi = AH'A^2B'P.\ HD'A'GB'.\ D'H'GHP'.\ B^2D'AH^2B^2$ ($|\Phi|=20f$)
$X = DGH^2AH'.\ BA^2D^2P^2G.\ H^2A'P'HD^2.\ BA^2HD^2H$
$Y = AH'A^2B'P.\ HD'A'GB'.\ D'H'GHP'.\ B^2D'AH^2B^2$
Il y a environ 490.000.000 états SuperLoin en f-rotation

Résumons :

Le SuperFlip: $|\Phi|=24$, $|\Phi|=20f$
Le SuperFlip4Spot: $|\Pi|=26$, $|\Pi|=20f$
Le diamètre du Rubik's Cube : 20f (2010), 26 (2014)

12 LA SYMÉTRIE $\mathcal{I}$-CONJUGAISON

Parfois on entend dire que:
- Le nombre 43252003274489856000 d'états du Rubik's Cube n'est pas bon !! on a compté plusieurs fois le même état et donc il faut le diviser par 24 car le Cube a 24 symétries !!
- Ou encore ce nombre n'est pas tout à fait correct !! car on a compté plusieurs fois le même état, le nombre correct est 901083404981813616 !! ???

Alors où est la vérité ?

12.1 AU DÉBUT ...

Il faut remonter vers les années 1980 , on s'est posé la question suivante:
-Quel est le nombre de rotations nécessaire b, pour restaurer le Rubik's Cube à partir de n'importe quel état ?
On peut prendre par ex b = 65256 c'est bien, mais il y a beaucoup trop de rotations non utilisées ....
de même si on prend b = 23 , il y a des états qu'on ne peut pas s'en sortir avec 23 rotations par ex l'état SuperFlip, il faut au minimum 24 rotations !!
Chercher b revient à chercher le diamètre du Rubik's

Cube.
Donc on a le graphe (le graphe Cayley) du Rubik's Cube mais ce graphe est énorme !!! l'idée est de réduire ce graphe à fin que la recherche du diamètre soit accessible par l'ordinateur ...
On va classer les états suivant un certain nombre de critères, ainsi on réduit le nombre sommets donc on réduit le graphe, le nouveau graphe sera plus facile à exploter.
Mais alors quels sont les critères ?

12.2 LA SYMÉTRIE $\mathcal{I}$

Avant de parler "mathématiquement" du Rubik's Cube il faut "orienter" le Cube càd déclarer officiellement qui est le Haut, qui est la Droite ....
traditionnellement on oriente le Cube ainsi:

(H)aut=(b)lanc, (B)as=(j)aune, (A)vant=(v)ert,
(P)ostérieur=(k)lein, (G)auche=(o)range,
(D)roite=(r)ouge.

Observons ces trois images ci-dessous.
Parmi ces trois images lequel est l'état résolu ? et pourquoi ?

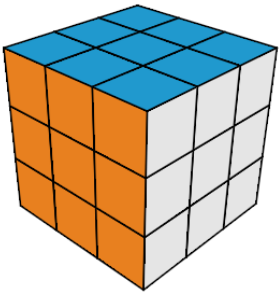


image (a)

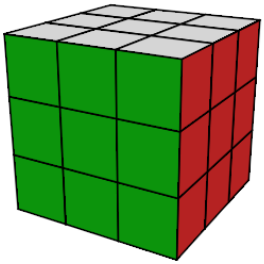


image (b)

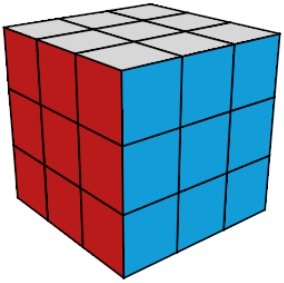


image (c)

L'image (b) est l'état résolu car les centres ne sont pas bougés, comme les centres de (a) et de (c) ont bougé ces images ne présentent pas l'état résolu mais une configuration ! or pour un jury de compétition ces 3 configurations jouent le même rôle .... d'où l'idée de classer (mettre dans la même boîte) les configurations du Rubik's Cube suivant un certain nombre de critères .... afin que les confuguratios (a), (b), (c) soient dans la même classe, dans la même boîte.
Le critère utilisé est la " symétrie $\mathcal{I}$ " où $\mathcal{I}$ est le groupe des

isométries du cube, en effet on passe de la configuration (b) à (a), ou de la configuration (b) à (c) par des rotations-cube.

Le groupe $\mathcal{I}$ a 48 éléments en voici :

<u>Isométries positives</u>
Identité (1)
RotCentre ±90° (3+3)
RotCentre 180° (3)
RotArete 180° (6)
RotSommet ±120° (4+4)

<u>Isométries négatives</u>
SymCentrale (1)
SymRot ±90° (3+3)
SymPlan (3)
SymArete (6)
SymSommet (4+4)

Total = 48 éléments

En plus des rotations de base {H;B,A,P,G,D} on ajoute les rotations-cube, les symétries-cube càd les isométries du cube $\mathcal{I}$.

On pose :

$M_* = M \cup \mathcal{I}$

$M_* = < H,B,A,P,G,D, f,g,h , ...> , f,g,h ... \in \mathcal{I}$

$G_*^+ = G^+ \times S_6$; S_6 car les centres bougent

M_* agit (librement) sur G_*^+ :
$G_*^+ \times M_* \to G_*^+$
$(\alpha, m) \to \alpha \bullet m$

On définit alors deux relations d'équivalences suivantes :

i) <u>La symétrie $\mathcal{I}$</u> : Deux configurations $\alpha, \beta \in G_*^+$ sont dans la même classe (même boîte) ssi:
il existe un $f \in \mathcal{I}$ tel que :

$\alpha \bullet f = \beta$

Les clases de cette relation s'appellent les $\mathcal{I}$-classes dans G_*^+.

ex :

$b \bullet ({}^tA {}^tD') = a$

$b \bullet ({}^tH) = c$

Rappelle sur la formule de Burnside.
Soient K un groupe fini et X un ensemble fini, K agit sur X (on passe un élément de X à un autre par un élément de K)
On pose $F_g = \{ x \in X \mid x \bullet g = x \}$ l'ensemble des points fixes de $g \in K$, $F_g \subset X$

<u>Lemme de Burnside</u>

$$\mathcal{N} = \frac{1}{|K|} \sum_{g \in K} |F_g|$$

où $\mathcal{N}$ = le nombre d'orbites = c'est la somme des points fixes (quand g parcourt K) divisé par |K|.

On prend K=M_* et X=G_{*^+}

Comme M_* agit librement, la formule de Burnside nous donne

$$\mathcal{N} = \frac{|G_*^+|}{|J|} = \frac{12 \text{ x } 6!\ |G|}{|J|}$$

Et par définition le nombre :

$$\frac{\mathcal{N}}{12 \text{ x } 6!} = \frac{|G|}{48} = 901\,083\,401\,551\,872\,000$$

est le nombre de $\boldsymbol{\mathcal{I}}$-classes (dans G) .

Autrement dit si on ignore les centres on a l'action (libre) suivante:

G x $\boldsymbol{\mathcal{I}} \rightarrow$ G
$(\mu,f) \rightarrow \mu \bullet f$

Et la formule de Burnside nous donne

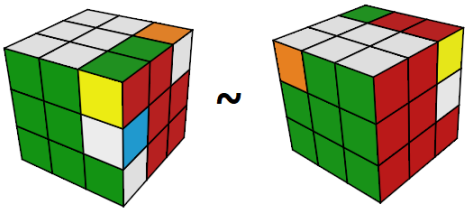
$$\mathcal{N} = \frac{|G|}{48} = 901\,083\,401\,551\,872\,000$$

ii) <u>La symétrie $\boldsymbol{\mathcal{I}}$-conjugaison</u> :

En 1994 Jerry BRYAN a eu l'idée suivante : On va classer les états suivant un critère nommé la symétrie $\boldsymbol{\mathcal{I}}$-conjugaison définie ainsi : deux états $\mu,\nu \in G$, $\mu = e \bullet V$, $V \in M$ sont dans la même classe (même boîte) ssi:
il existe un $f \in \boldsymbol{\mathcal{I}}$ tel que :

$e \bullet (f\ V f^{-1}) = \nu$, où e=état résolu.

Les clases de cette relation s'appellent les $\mathcal{I}$-conjugaison classes
ex :
$\mu = e \bullet V$; $V = DHD'H'$ et ν
$\mu \sim \nu \Leftrightarrow e \bullet ({}^{t}H\, V\, {}^{t}H') = \nu$



$\mu \sim \nu$

Note : f perturbe les centres, V ne touche pas les centres, et f^{-1} remet les centres en ordre, on a bien une relation d'équivalence sur G .

Il a calculé et a trouvé 901 083 404 981 813 616 $\mathcal{I}$-conjugaison classes . Les classes se distribuent en fonction des éléments de $\mathcal{I}$ de la façon suivante:

Classes de type	Nombre de $\mathcal{I}$-conjugaison classes
Identité (1)	901083401551872000
RotCentre±90° (3+3)	18432
RotCentre180° (3)	955514880
RotArete180° (6)	318504960
RotSommet±120° (4+4)	629856
SymCentrale (1)	955514880
SymRot ±90° (3+3)	55296

SymPlan (3)	1146617856
SymArete (6)	53084160
SymSommet (4+4)	1296
Total = 48 éléments	Total = 901083404981813616

Chaque classe contient donc un certain nombre d'états.

Le nombre 901 083 404 981 813 616 est donc le nombre de $\mathcal{I}$-conjugaison classes et non le nombre d'états de G !

Remarque important : Lorsque |G| est divisible par k on peut interpréter |G|/k comme le nombre de classes d'une certaine relation d'équivalence, et la formule de Burnside permet de calculer ces classes, ces classes sont homogènes chaque classe possède le même nombre d'éléments k.

REMARQUE : On peut travailler dans Λ, dans ce cas les élements sont des permutations de S_{48} en effet

$\mathcal{I} \subset S_{48}$ gâce au théorème : si G est un groupe fini, alors G est isomorphe à un sous groupe de $S_{|G|}$

$\mathcal{I} \subset S_{48}$ et $\Lambda \subset S_{48}$

$p,q \in \Lambda$, $p \sim q \Leftrightarrow \exists f \in \mathcal{I}$ tel que $fpf^{-1} = q$

les classes de cette relation d'équivalance sont les $\mathcal{I}$-conjugaison-classe.

12.3 LA PROGRAMMATION

Voici trois programmes en GAP qui calcule le nombre de $\mathcal{J}$-conjugaison classes.

Programme 1 :

```
#gap_J-rubik.txt

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


# Iso=le groupe isometrie du cube

j1 :=
(6,46,18,26)(8,14,24,12)(38,48,36,32)(2,30,22,42)(16,20,
10,4)(28,40,44,34)

(5,45,11,17)(7,13,9,3)(21,31,41,35)(43,33,23,29)(1,25,15,
37)(47,39,19,27) ;
```

```
j2 :=
(6,16,22,14)(8,24,20,4)(38,30,40,46)(2,10,18,12)(28,32,4
8,44)(34,42,36,26)

(5,31,15,43)(7,45,13,25)(21,19,33,39)(1,35,11,23)(47,41,
27,29)(3,17,9,37);

Iso := Group(j1,j2) ;

# Dep=le groupe isometrie+ du cube (24) Dep = ssg de Iso

d1 :=
(1,11)(2,18)(3,9)(4,24)(5,15)(6,22)(7,13)(8,20)(10,12)


(14,16)(17,37)(19,39)(21,33)(23,35)(25,45)(26,42)(27,4
7)(28,48)(29,41)

    (30,46)(31,43)(32,44)(34,36)(38,40);

d2 :=
(1,15)(2,22)(3,13)(4,20)(5,11)(6,18)(7,9)(8,24)(10,16)(1
2,14)


(17,45)(19,47)(21,41)(23,43)(25,37)(26,46)(27,39)(28,4
4)(29,33)(30,42)

    (31,35)(32,48)(34,40)(36,38) ;

d3 := (1,17,19)(2,32,10)(3,31,33)(4,40,42)
```

```
(5,45,39)(6,48,12)(7,35,21)(8,34,26)(9,23,29)(11,25,47)(
13,43,41)

    (14,22,44)(15,37,27)(16,18,28)(20,38,46)(24,36,30);


d4 :=
(1,35,11,23)(2,10,18,12)(3,17,9,37)(4,8,24,20)(5,31,15,43
)


(6,16,22,14)(7,45,13,25)(19,33,39,21)(26,34,42,36)(27,29
,47,41)

    (28,32,48,44)(30,40,46,38) ;


Dep := Group(d1,d2,d3,d4) ;


# Rubik=le groupe du Rubik's Cube

pH := (2,4,6,8)(26,28,30,32)
(1,3,5,7)(17,21,25,29)(19,23,27,31) ;

pB := (18,24,22,20)(42,48,46,44)
(9,15,13,11)(33,45,41,37)(35,47,43,39);

pA := (2,34,18,36)(26,10,42,12)
(1,35,11,23)(17,9,37,3)(19,33,39,21);
```

```
pP := (6,38,22,40)(30,14,46,16)
(7,25,13,45)(29,27,41,47)(31,5,43 ,15);

pG := (4,12,20,14)(28,36,44,38)
(3,39,13,27)(21,11,41,5)(23,37,43,25);

pD := (8,16,24,10)(32,40,48,34)
(1,29,15,33)(17,31,45,35)(19,7,47,9);

Rubik := Group(pH,pB,pA,pP,pG,pD);

# Pocket=le groupe Pocket (= Rubik sans arêtes)

#pH :=  (1,3,5,7)(17,21,25,29)(19,23,27,31) ;

#pB :=  (9,15,13,11)(33,45,41,37)(35,47,43,39);

#pA :=  (1,35,11,23)(17,9,37,3)(19,33,39,21);

#pP :=  (7,25,13,45)(29,27,41,47)(31,5,43 ,15);

#pG :=  (3,39,13,27)(21,11,41,5)(23,37,43,25);

#pD :=  (1,29,15,33)(17,31,45,35)(19,7,47,9);

#Pocket := Group(pH,pB,pA,pP,pG,pD);


G := Rubik ;;

GG := "Rubik" ;;

J := Iso ;;
```

```
JJ := "J" ;;


etat := 0 ;;

Jcjg := 0 ;;


   # Les classes des sous groupes conjugaisons de J

   Cl := ConjugacyClassesSubgroups( J );;

   ptfixe := [];


         Print("\n\n No \tetat \tclasses-conjugaisons\n" );

         Print("================================
================ \n" );

   # pour toute classe Cl[i], on cherche les pt fixes générés
par Cl[i]

   for i  in [Length(Cl),Length(Cl)-1..1]  do


      # prendre un représentant

      H := Representative( Cl[i] );
```

```
    # les pt fixes engendrés par H
    aux := Size( Centralizer( G, H ) );

    # si Q inclus dans H,on supprime dans H les pt fixes
générés par Q
    for k  in [Length(Cl),Length(Cl)-1..i+1]  do
      for Q  in Elements( Cl[k] )  do
        if IsSubgroup( Q, H )  then
                aux := aux - ptfixe[k];
        fi;
      od;
    od;
    # sauver les pt fixes génégrés par H
    ptfixe[i] := aux;

    # print N° classe
    Print("\n ", i, ":\t" );
```

```
    # le nbr de pt fixes (= nbr états) générés par Cl[i]
    Print( Size(Cl[i]) *  ptfixe[i], "\t" );
                etat := etat + ( Size(Cl[i]) *  ptfixe[i] );

    # le nbr de J-cjg classes générés par Cl[i]
    Print( (Size(Cl[i]) *  ptfixe[i]) /  Index(J,H), " " );
Jcjg := Jcjg + ( (Size(Cl[i]) *  ptfixe[i] )/  Index(J,H) );

  od;
        Print("\n\n ",GG," = ", etat, "\n" );
        Print("\n ",JJ,"-cjg = ", Jcjg , "\n" );
```

Programme2 :

```
#gap_J-rubik-burnside.txt
#       5  6  7
#       4  H  8
#       3  2  1
#25 28 23|21 26 19|17 32 31|29 30 27
#38 G  36|12 A  10|34 D  40|16 P  14
#43 44 37|39 42 33|35 48 45|47 46 41
#       11 18 9
#       20 B  24
```

```
#       13 22 15


# Iso=le groupe isometrie du cube

j1 :=
(6,46,18,26)(8,14,24,12)(38,48,36,32)(2,30,22,42)(16,20,
10,4)(28,40,44,34)

(5,45,11,17)(7,13,9,3)(21,31,41,35)(43,33,23,29)(1,25,15,
37)(47,39,19,27) ;

j2 :=
(6,16,22,14)(8,24,20,4)(38,30,40,46)(2,10,18,12)(28,32,4
8,44)(34,42,36,26)

(5,31,15,43)(7,45,13,25)(21,19,33,39)(1,35,11,23)(47,41,
27,29)(3,17,9,37);

Iso := Group(j1,j2) ;


# Dep=le groupe isometrie+ du cube (24) Dep = ssg de Iso

d1 :=
(1,11)(2,18)(3,9)(4,24)(5,15)(6,22)(7,13)(8,20)(10,12)


(14,16)(17,37)(19,39)(21,33)(23,35)(25,45)(26,42)(27,4
7)(28,48)(29,41)

     (30,46)(31,43)(32,44)(34,36)(38,40);
```

```
d2 :=
(1,15)(2,22)(3,13)(4,20)(5,11)(6,18)(7,9)(8,24)(10,16)(1
2,14)


(17,45)(19,47)(21,41)(23,43)(25,37)(26,46)(27,39)(28,4
4)(29,33)(30,42)

    (31,35)(32,48)(34,40)(36,38) ;

d3 := (1,17,19)(2,32,10)(3,31,33)(4,40,42)


(5,45,39)(6,48,12)(7,35,21)(8,34,26)(9,23,29)(11,25,47)(
13,43,41)

    (14,22,44)(15,37,27)(16,18,28)(20,38,46)(24,36,30);


d4 :=
(1,35,11,23)(2,10,18,12)(3,17,9,37)(4,8,24,20)(5,31,15,43
)


(6,16,22,14)(7,45,13,25)(19,33,39,21)(26,34,42,36)(27,29
,47,41)

    (28,32,48,44)(30,40,46,38) ;


Dep := Group(d1,d2,d3,d4) ;
```

```
# Rubik=le groupe du Rubik's Cube

pH := (2,4,6,8)(26,28,30,32)
(1,3,5,7)(17,21,25,29)(19,23,27,31) ;

pB := (18,24,22,20)(42,48,46,44)
(9,15,13,11)(33,45,41,37)(35,47,43,39);

pA := (2,34,18,36)(26,10,42,12)
(1,35,11,23)(17,9,37,3)(19,33,39,21);

pP := (6,38,22,40)(30,14,46,16)
(7,25,13,45)(29,27,41,47)(31,5,43 ,15);

pG := (4,12,20,14)(28,36,44,38)
(3,39,13,27)(21,11,41,5)(23,37,43,25);

pD := (8,16,24,10)(32,40,48,34)
(1,29,15,33)(17,31,45,35)(19,7,47,9);

Rubik := Group(pH,pB,pA,pP,pG,pD);


# Pocket=le groupe Pocket (= Rubik sans arêtes)

#pH :=  (1,3,5,7)(17,21,25,29)(19,23,27,31) ;

#pB :=  (9,15,13,11)(33,45,41,37)(35,47,43,39);

#pA :=  (1,35,11,23)(17,9,37,3)(19,33,39,21);

#pP :=  (7,25,13,45)(29,27,41,47)(31,5,43 ,15);
```

```
#pG :=  (3,39,13,27)(21,11,41,5)(23,37,43,25);

#pD :=  (1,29,15,33)(17,31,45,35)(19,7,47,9);

#Pocket := Group(pH,pB,pA,pP,pG,pD);


G := Rubik ;;

GG := "Rubik" ;;

J := Iso ;;

JJ := "J" ;;


Jcjg := Sum(J,f -> Size(Centralizer(G,f))) / Size(J);;

Print("\n\n ",GG," = ", Size(G), "\n" );

Print("\n ",JJ,"-cjg = ", Jcjg, "\n" );
```

Programme 3 :

```
#gap_J-rubik-cjg.txt
#       5  6  7
#       4  H  8
#       3  2  1
#25 28 23|21 26 19|17 32 31|29 30 27
#38 G  36|12 A  10|34 D  40|16 P  14
#43 44 37|39 42 33|35 48 45|47 46 41
```

```
#       11 18 9
#       20 B  24
#       13 22 15


# Iso=le groupe isometrie du cube

j1 :=
(6,46,18,26)(8,14,24,12)(38,48,36,32)(2,30,22,42)(16,20,
10,4)(28,40,44,34)

(5,45,11,17)(7,13,9,3)(21,31,41,35)(43,33,23,29)(1,25,15,
37)(47,39,19,27) ;

j2 :=
(6,16,22,14)(8,24,20,4)(38,30,40,46)(2,10,18,12)(28,32,4
8,44)(34,42,36,26)

(5,31,15,43)(7,45,13,25)(21,19,33,39)(1,35,11,23)(47,41,
27,29)(3,17,9,37);

Iso := Group(j1,j2) ;


# Dep=le groupe isometrie+ du cube (24) Dep = ssg de Iso

d1 :=
(1,11)(2,18)(3,9)(4,24)(5,15)(6,22)(7,13)(8,20)(10,12)


(14,16)(17,37)(19,39)(21,33)(23,35)(25,45)(26,42)(27,4
7)(28,48)(29,41)
```

```
(30,46)(31,43)(32,44)(34,36)(38,40);

d2 :=
(1,15)(2,22)(3,13)(4,20)(5,11)(6,18)(7,9)(8,24)(10,16)(1
2,14)


(17,45)(19,47)(21,41)(23,43)(25,37)(26,46)(27,39)(28,4
4)(29,33)(30,42)

(31,35)(32,48)(34,40)(36,38) ;

d3 := (1,17,19)(2,32,10)(3,31,33)(4,40,42)


(5,45,39)(6,48,12)(7,35,21)(8,34,26)(9,23,29)(11,25,47)(
13,43,41)

(14,22,44)(15,37,27)(16,18,28)(20,38,46)(24,36,30);


d4 :=
(1,35,11,23)(2,10,18,12)(3,17,9,37)(4,8,24,20)(5,31,15,43
)


(6,16,22,14)(7,45,13,25)(19,33,39,21)(26,34,42,36)(27,29
,47,41)

(28,32,48,44)(30,40,46,38) ;


Dep := Group(d1,d2,d3,d4) ;
```

```
# Rubik=le groupe du Rubik's Cube

pH := (2,4,6,8)(26,28,30,32)
(1,3,5,7)(17,21,25,29)(19,23,27,31) ;

pB := (18,24,22,20)(42,48,46,44)
(9,15,13,11)(33,45,41,37)(35,47,43,39);

pA := (2,34,18,36)(26,10,42,12)
(1,35,11,23)(17,9,37,3)(19,33,39,21);

pP := (6,38,22,40)(30,14,46,16)
(7,25,13,45)(29,27,41,47)(31,5,43 ,15);

pG := (4,12,20,14)(28,36,44,38)
(3,39,13,27)(21,11,41,5)(23,37,43,25);

pD := (8,16,24,10)(32,40,48,34)
(1,29,15,33)(17,31,45,35)(19,7,47,9);

Rubik := Group(pH,pB,pA,pP,pG,pD);


# Pocket=le groupe Pocket (= Rubik sans arêtes)

#pH :=  (1,3,5,7)(17,21,25,29)(19,23,27,31) ;

#pB :=  (9,15,13,11)(33,45,41,37)(35,47,43,39);

#pA :=  (1,35,11,23)(17,9,37,3)(19,33,39,21);
```

```
#pP :=  (7,25,13,45)(29,27,41,47)(31,5,43 ,15);

#pG :=  (3,39,13,27)(21,11,41,5)(23,37,43,25);

#pD :=  (1,29,15,33)(17,31,45,35)(19,7,47,9);

#Pocket := Group(pH,pB,pA,pP,pG,pD);


G := Rubik ;;

GG := "Rubik" ;;

J := Iso ;;

JJ := "J" ;;


Jcjg := Sum(ConjugacyClasses(J),i -> (Size(i) *
Size(Centralizer(G,Representative(i)))) / Size(J));;

Print("\n\n ",GG," = ", Size(G), "\n" );

Print("\n ",JJ,"-cjg = ", Jcjg, "\n" );
```

13 L'ALGORITHME $[DH]^X$

Il y a plusieurs façons de résoudre le Rubik's Cube:

1. On peut résoudre en basant sur la vitesse, c'est-à-dire on le résout de plus en plus vite peu importe le nombre de formules utiliser, peu importe la forme des formules, le but c'est finir la résolution le plus vite possible.
2. On peut aussi le résoudre en fermant les yeux !!
3. On le résout en une seule main !
4. Ou encore en nombre minimum de rotations de base {H,B,A,P,G,D}
5. Durant la résolution , on utilise une seule formule.
6. etc ...

Ici nous allons attaquer la résolution sous un autre angle, c'est aussi un nouveau défi bien étrange... On veut que la résolution utilise uniquement les formules de la forme $[DH]^X = X[DH]X'$ où X est une formule $X \in M$
Allons y .....

13.1 ANALYSE

* Les états du Cube forment un groupe G dans un truc comme ça

$G \subset G^+ = S_{12} \times \mathbb{Z}_2^{12} \times S_8 \times \mathbb{Z}_3^8$
G est composé de 4 morceaux donc l'algorithme de résolution comporte 4 phases ou 4 étapes

* Le Rubik's Cube possède la loi de parité sig(u)=sig(v) ; u=permutation des arêtes, v=permutation des sommets, on écrit aussi sig(arêtes)=sig(sommets) donc il suffit d'étudier les arêtes en état pair (sig(arêtes)=1), et on passe les arêtes en état impair (sig(arêtes)=-1) à l'état pair par une simple rotation H.

* sig(arêtes)=1 signifie que la permutation des arêtes est pair, or les permutations paires sont engendrées par les 3-cycles, donc il suffit de trouver un 3-cycle particulier t et on aura tous les 3-cycles par les conjugués de t

Désormais nous supposons que les arêtes sont en état pair sig(u)=1

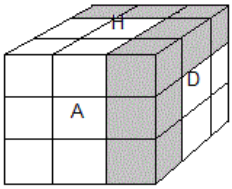
13.2 LES ÉGALITÉS

Quelques égalités

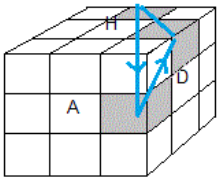
1. [DH] = I[DH]I'
2. $[DH]^n$ = (I[DH]I') (I[DH]I') (I[DH]I')... ; n fois
3. [DH]' = $[DH]^{-1}$ = [HD]=$[DH]^5$ car $[DH]^6$=I
4. $[DH]^{-2}$ = $[DH]^4$
5. X$[DH]^n$X' = (X[DH]X') (X[DH]X') (X[DH]X')... ; n fois
6. X(V[DH]V')(W[DH]W')X' = X(V[DH]V')X' . X(W[DH]W')X' = (XV)[DH](XV)' . (XW)[DH](XW)'

13.3 PLACER LES ARÊTES

Observons ce que fait le commutateur [DH], il agit sur le Cube comme une sorte de **'Z'** c'est pourquoi nous le notons Z=[DH]



Z = [DH]

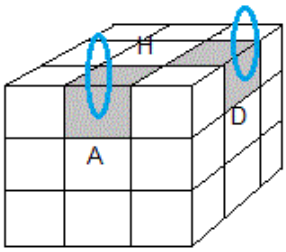


[DH] = (HP)→(AD)→(HD)

[DH] agit sur les arêtes:
[DH] = (HP)→(AD)→(HD) c'est un 3-cycle-arête donc avec les conjugués de [DH], X[DH]X' on peut placer toutes les arêtes puisque les arêtes sont en état pair.

13.4 ORIENTER LES ARÊTES

Ici c'est le point le plus difficile. Au début j'ai utilisé [D'A] pour renverser 2 arêtes, puis H'[HD]H pour remettre les pièces, mais là on a introduit le crochet [D'A] et je me demande s'il est possible de renverser 2 arêtes avec le crochet [DH] ? j'ai mis beaucoup de temps à chercher, très désespéré et sur le point d'abandonner et hup d'un seul coup j'ai trouvé cette formule
$A[DH]^5A'.(H'GA^2)[DH](H'GA^2)' = (HA)°(HD)°$
qui est construite sur le même principe que [D'A]. $H'[HD]H = (HA)°(AD)°$
$A[DH]^5A' = A[HD]A'$=> renverse 2 arêtes
$(H'GA^2)[DH](H'GA^2)'$ => remet les pièces en place
$A[HD]A' \Rightarrow$ renverse 2 arêtes
$(H'GA^2)[HD]^5(H'GA^2)' \Rightarrow$ remet les pièces en place

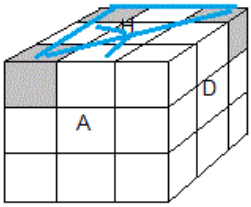


$A[HD]A'.(H'GA^2)[DH](H'GA^2)' = (HA)°(HD)°$

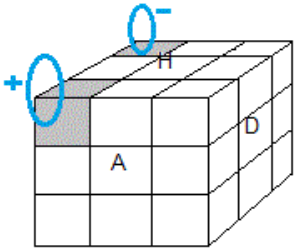
13.5 LES SOMMETS

Pour placer les sommets on a le 3-cycle ci-dessous
$[DH].G'[HD]G = (HGP) \rightarrow (HAG) \rightarrow (HPD)$

Pour pivoter les sommets on a la formule suivante
$[DH]^2.G'[HD]^2G = (HPG)^-(HAG)^+$



$[DH].G'[HD]G = (HGP) \rightarrow (HAG) \rightarrow (HPD)$



$[DH]^2.G'[HD]^2G = (HPG)^-(HAG)^+$

13.6 L'ALGORITHME $[DH]^X$

Et voilà , nous avons notre algorithme exigé !!

- Si sig(arêtes)=-1 alors H
- On place les arêtes par [DH]
- On oriente les arêtes par $A[HD]A'.(H'GA^2)[DH](H'GA^2)'$
- On place les sommets par [DH].G'[HD]G
- Pour pivoter les sommets on utilise $[DH]^2.G'[HD]^2G$

C'est vraiment étonnant qu'on peut remonter le Cube seulement avec H, [DH] (sous entendu bien sûr avec les conjugués de [DH], car [DH] agit sur les emplacements fixes, ses conjugués permettent de varier les emplacements)

13.7 COMMENTAIRE

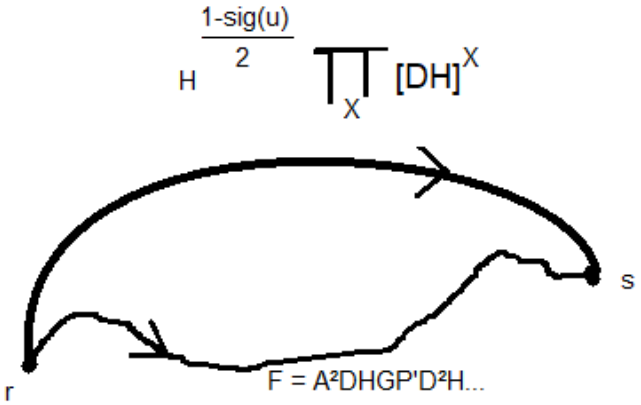
C'est extraordinaire, cela signifie que pour toute formule F on peut la décomposer en produit des conjugués de [DH] !!

$$F = H^{\frac{1-sig(u)}{2}} \prod_X [DH]^X$$

Le coefficient $H^{\frac{1-sig(u)}{2}}$ est là pour dire que quand les arêtes en état impair on fait un H avant d'appliquer l'algorithme.

[DH] joue le rôle des nombres premiers dans les nombres entiers : tout entier est décomposable en produit des nombres premiers

On pourrait aussi dire qu' à partir de l'état résolu e , pour arriver à l'état μ il y a toujours un chemin plus "propre", plus "joli" ou plus "sécurisé" que le chemin F



14 LES FORMULES PREMIÈRES

En cherchant l'algorithme théorique nous avons trouvé la formule J = A[DH]A'H de longueur 7 , |J| = 7 il est vraiment extraordinaire que cette formule contient tout ce qui faut pour restaurer le Cube à elle toute seule. On pourrait se demander s' il existe d'autres types de formules du même genre et que J est - elle de longueur minimale ?

14.1 UNE REMARQUE

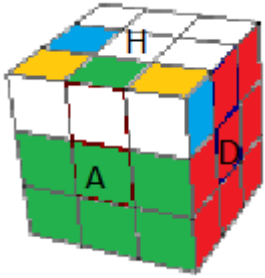
Quand on écrit
J = A[DH]A'H = (HG)↔(HP) ou plus simple J = (HG,HP) on voit que les pièces se déplacent mais on ne voit pas qu'elles se pivotent ! il faut donc trouver une notation qu'on voit aussi les pièces se pivotent en déplaçant. Si on écrit
J = $(HG)^{+}$↔(HP).$(HA)^{+}$ ou plus simple J = $(HG^{+},HP)(HA)^{+}$ là on voit que (HG) et (HA) pivotent (note on a: $(HA)^{+}$ = $(HA)^{-}$ = (HA)°)

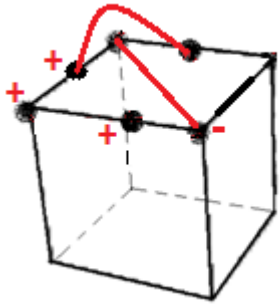
de même pour les sommets

J = (HGP)↔(HDA) ou plus simple J = (HGP,HDA^{-}) n'est pas précis, on ne voit pas les sommets pivotent, comme pour

les arêtes on écrit
J = (HGP)↔(HDA)$^{-}$. (HAG)$^{+}$ ou plus simple
J = (HGP,HDA^{-})(HAG)$^{+}$ là , on voit le sommet (HDA) pivote dans le sens anti-horaire et (HAG) pivote dans le sens horaire

Finalement la notation
J = (HG^{+},HP)(HA)$^{+}$ (HGP,HDA^{-})(HAG)$^{+}$ sera beaucoup plus précise, elle décrit exactement l'état du Cube. Si on n'a pas besoin de l'orientation mais simplement les déplacements on écrira
J = (HG,HP)(HGP,HDA) comme d'habitude



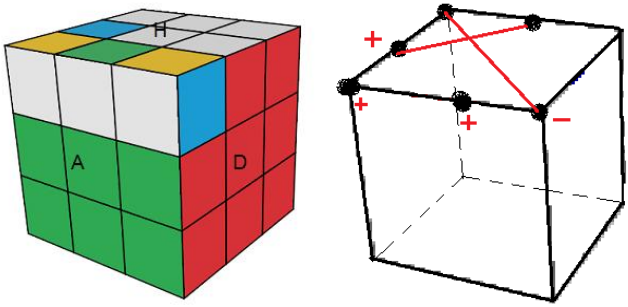


J = (HG^{+},HP)(HA)$^{+}$ (HGP,HDA^{-})(HAG)$^{+}$

14.2 FORMULE PREMIÈRE

Définition : On dit qu'une formule V est première si elle peut restaurer le Cube.
Par exemple J est première car on peut restaurer le Cube avec seulement J.

1. $(HG)\leftrightarrow(HP) = J$
2. $(HGP)\leftrightarrow(HDA) = J$
3. $(HG)^{+}(HP)^{+} = J^{2}$
4. $(HGP)^{+}(HAG)^{+}(HDA)^{+} = J^{4}$



J = A[DH]A'.H

Il est donc naturel de se demander s'il existe d'autres formules du même genre ? et quelle est la plus courte ?

14.3 ANALYSE DE J

Rappelle J = A[DH]A'H . Nous allons examiner minutieusement J et essayer de comprendre sa structure, comment se fait-il qu'elle peut restaurer le Cube à elle toute seule.

[1]- J permute un couple d'arêtes $(HG)^+ \leftrightarrow (HP)$ ou plus simple (HG^+,HP) cela permet de placer toutes les arêtes.

[2]- En permutant elle renverse l'une des arêtes $(HG)^+$, mais elle renverse aussi une autre arête extérieure de la permutation $(HA)^+$ (la loi des flips est bien vérifiée)
- Si on regarde de plus près , tout cela permet de renverser un couple d'arêtes, en effet :
$J = (HG^+,HP)(HA)^+$
$J^2 = (HG^+,HP^+)(HA)^{++} = (HG^+,HP^+)$; donc J^2 renverse bien le couple d'arêtes (HG),(HP)

- si J renverse 2 arêtes en les permutant, ça ne va pas marcher, on ne peut pas renverser les arêtes, en effet
si $J = (HG^+,HP^+) \Longrightarrow J^2 = (HG,HP)$ on ne renverse pas !!
- si J renverse 2 arêtes extérieures de la permutation, ça ne va pas marcher non plus, en effet
si $J = (HG,HP)(HA)^+(HD)^+$ (par ex) => $J^2 = (HG,HP)$ on ne renverse rien !!

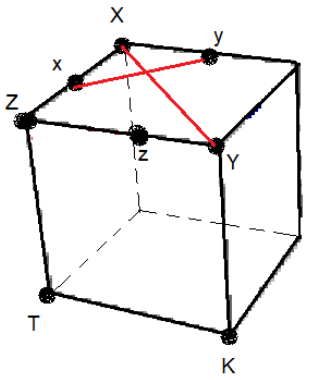
Il y a un seul cas qui marche c'est quand J renverse une arête dans la permutation et une autre arête à l'extérieure de la permutation

J = $(HG^+,HP)(HA)^+$

[3]- Pour les sommets tout se passe exactement comme les arêtes
- J permute 2 sommets en pivotant l'un d'eux (HGP,HDA^-), et elle pivote aussi un autre sommet $(HAG)^+$ à extérieur de la permutation
finalement J est de type
J = $(HG^+,HP)(HA)^+(HGP,HDA^-)(HAG)^+$

14.4 D'AUTRES TYPES

Pour ne pas alourdir les notations on va noter:
x,y,z minuscule les 3 arêtes
X,Y,Z,K,T majuscule les 5 sommets



Analyse

I. Pour pouvoir déplacer, et renverser toutes les arêtes d'après ce qui est dit plus haut on doit avoir $(x^+,y)z^+$ en effet (x,y) permet de déplacer toutes les arêtes car toute permutation est décomposée en transpositions. Et la loi de parité du Rubik's Cube impose qu'on doit aussi permuter deux sommets (X,Y) c'est-à-dire on doit avoir: $(x^+,y)z^+(X,Y)$

II. La loi des twists impose que pour pivoter les sommets on a:

$(X^+,Y)Z^-$
$(X^-,Y)Z^+$
$(X^+,Y^+)Z^+$
$(X^-,Y^-)Z^-$

$(X,Y)Z^+K^-$
$(X,Y)Z^+K^+T^+$
$(X,Y)Z^-K^-T^-$
$(X^+,Y)Z^+K^+$
etc ...
par ex $V=(x^+,y)z^+(X^+,Y^+)Z^+$
et V^4 pivotent les sommets

Voici les types
$N = (x^+,y)z^+(X,Y)Z^+K^-$
$N^+ = (x^+,y)z^+(X,Y)Z^+K^+T^+$
$N^- = (x^+,y)z^+(X,Y)Z^-K^-T^-$

$J = (x^+,y)z^+(X,Y^-)Z^+$
$\underline{J} = (x^+,y)z^+(X,Y^+)Z^-$; l'anti-θ
$J^+ = (x^+,y)z^+(X,Y^+)Z^+K^+$
$J^- = (x^+,y)z^+(X,Y^-)Z^-K^-$

$\Delta^+ = (x^+,y)z^+(X^+,Y^+)Z^+$
$\Delta^- = (x^+,y)z^+(X^-,Y^-)Z^-$

Il y a donc 9 types de formules premières divisées en 3 groupes, et d'après Cube Explorer J a la longueur minimale 7, |J|=7, et les autres ont une longueur plus grande

$N = H' D H D^2 A' G' A' G B' P' G P A' B D A'$; $|N|=17$
$N^+ = D^2 P' B P' G' B' P' D' A D H P' D' H A' H D' H'$; $|N^+|=19$
$N^- = A' D A B P' B G P' H G' P' H' D P' D' B^2$; $|N^-|=17$

$J = A D H D' H' A' H$; $|J|=7$
$\underline{J} = D A' H G' A D' A' G H' A^2 D A' H' D' H^2$; $|\underline{J}|=17$
$J^+ = H G H' D P' H A H' P H^2 A' H' G' D'$; $|J^+|=15$
$J^- = H' D^2 P H P^2 B' P H' P' B D' P D' H^2$; $|J^-|=17$

$\Delta^+ = A H A' H' D' H G' H' D P' H' P G$; $|\Delta^+|=13$
$\Delta^- = P^2 D B' D' H' D H P H' P' B D' P^2$; $|\Delta^-|=15$

NOTE : l'algorithme théorique est donc

- $(x,y) = V$
- $(X,Y) = V$
- $x^+y^+ = V^2$
- $X^iY^jZ^k = V^4$

où V est une formule première, x,y arêtes, X,Y,Z sommets et i+j+k = 0 (mod 3)

NOTE : Il existe d'autres formules premières de longueur 7
$\mathcal{C}$ = D'[A'H']DH' , bien, c'est le symétrique de J (une A-formule)
$\mathcal{Q}$ = A[HD]A'H' , moyen (une P-formule)

TABLE DES MATIÈRES

Biographie

* Cube Explorer (Herbert Kociemba) : On donne un état, il trouve une formule correspondant en face-métrique ou quart-métrique.

http://kociemba.org/cube.htm

* Voici les javascripts pour calculer l'ordre maximal et l'ordre d'un élément.

https://fan2cube.fr/javascript/ordre_maxi.html

https://fan2cube.fr/javascript/ordre_calcul.html

* GAP, est un programme qui permet de calculer, l'ordre d'un groupe de permutations, ...

https://www.gap-system.org/Releases/index.html

* Les quiz pour tester vos connaissances

https://fan2cube.fr/certificat/mc1.html

* Un simulateur des cubes

http:/pMetro.su/pCubes.zip

* Rubik résolution

https://fan2cube.fr/softs/rubiks-solver-master.zip

* Rubik animation

https://fan2cube.fr/softs/rubik_animation.zip

* Virtualcube

https://fan2cube.fr/softs/virtualcubejs2017.zip

Du même auteur

¤*1 La conjecture de Fermat*

C'est un livre qui démontre la conjecture de Fermat, (appelé souvent "le dernier théorème de Fermat") en s'appuyant sur deux théorèmes: le théorème de Ribet et le théorème de Wiles. Un document rare et exceptionnel.

¤*2 La Relativité Générale*

Tout sur la Relativité Générale et on trouve une démonstration de l'équation tensorielle d'Einstein à partir du principe moindre action, ce qui est très rare.

¤*3 Le Groupe du Rubik's Cube (Tome I, II)*

Le Rubik's Cube possède un groupe très riche en propriétés et si la partie mathématique du puzzle vous intéresse alors ce livre est pour vous.

¤*4 La Relativité Restreinte*

La Relativité Restreinte est une théorie physique proposée par Einstein pour remplacer la mécanique newtonienne quand la vitesse des objets est proche à celle de la lumière c.

¤*5 Les nombres transcendants*

Les nombres transcendants sont très mystérieux, ils sont partout, beaucoup plus nombreux que les nombres algébriques et pour tant on connaît très peu de ces nombres, le premier est e, puis π, cos(1) , ...

¤*6 La Cubologie (Tome I, II)*

Pour comprendre les propriétés des twists il faut passer par les mathématiques, à chaque twist on associe un groupe et ce sont des propriétés de ce groupe qui expliquent les propriétés du twist.

¤*7 La physique quantique (Tome I, II)*

Si vous voulez savoir ce que c'est la physique quantique , ce livre est pour vous.