

# Maths for fun: Mathématiques des jeux et casse-têtes

Laurent Fousse `laurent.fousse@imag.fr`

20 janvier 2009

# Plan

1 Procédure Sift

2 Rubik's Cube

# Plan

1 Procédure Sift

2 Rubik's Cube

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

- On considère le sous-groupe  $\langle S \rangle$  de  $\mathcal{S}_n$  engendré par les éléments de  $S$ .

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

- On considère le sous-groupe  $\langle S \rangle$  de  $\mathcal{S}_n$  engendré par les éléments de  $S$ .

Questions :

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

- On considère le sous-groupe  $\langle S \rangle$  de  $\mathcal{S}_n$  engendré par les éléments de  $S$ .

Questions :

- ① Combien  $\langle S \rangle$  a-t-il d'éléments ?

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

- On considère le sous-groupe  $\langle S \rangle$  de  $\mathcal{S}_n$  engendré par les éléments de  $S$ .

Questions :

- 1 Combien  $\langle S \rangle$  a-t-il d'éléments ?
- 2 Pour une permutation quelconque  $\alpha$ , a-t-on

$$\alpha \in \langle S \rangle ?$$

# Problématique

- On se donne un ensemble fini de permutations sur  $n$  éléments :

$$S = \{\alpha_1, \alpha_2, \dots, \alpha_k\}$$

- On considère le sous-groupe  $\langle S \rangle$  de  $\mathcal{S}_n$  engendré par les éléments de  $S$ .

Questions :

- 1 Combien  $\langle S \rangle$  a-t-il d'éléments ?
- 2 Pour une permutation quelconque  $\alpha$ , a-t-on

$$\alpha \in \langle S \rangle ?$$

- 3 Pour  $\alpha \in \langle S \rangle$  comment le décomposer en produit d'éléments de  $S$  ?

# Tableau de calcul de $S$

## Tableau de permutations

Un tableau de permutations sur  $n$  est un tableau  $(n, n)$  tel que :

- Pour tout  $1 \leq i \leq n$ ,  $T[i, i] = \text{id}$ .
- Pour tout  $i \neq j$ ,  $T[i, j]$  est soit indéfinie soit une permutation  $\sigma$  telle que

$$\forall k < i, \sigma(k) = k \text{ et } \sigma(i) = j$$

# Tableau de calcul de $S$

## Tableau de permutations

Un tableau de permutations sur  $n$  est un tableau  $(n, n)$  tel que :

- Pour tout  $1 \leq i \leq n$ ,  $T[i, i] = \text{id}$ .
- Pour tout  $i \neq j$ ,  $T[i, j]$  est soit indéfinie soit une permutation  $\sigma$  telle que

$$\forall k < i, \sigma(k) = k \text{ et } \sigma(i) = j$$

## Tableau de calcul

On dit que  $T$  est un tableau de calcul du groupe  $G$  si tous les éléments de  $T$  appartiennent à  $G$  et si  $G$  est engendré par les éléments de  $T$ .

# Exemple

Pour  $n = 7$  on considère les permutations

$$\sigma = (1, 2, 3, 4, 5, 6, 7) \quad \alpha = (2, 6)(4, 5)$$

# Exemple

Pour  $n = 7$  on considère les permutations

$$\sigma = (1, 2, 3, 4, 5, 6, 7) \quad \alpha = (2, 6)(4, 5)$$

|    |          |    |    |    |          |    |
|----|----------|----|----|----|----------|----|
| id | $\sigma$ | —  | —  | —  | —        | —  |
| —  | id       | —  | —  | —  | $\alpha$ | —  |
| —  | —        | id | —  | —  | —        | —  |
| —  | —        | —  | id | —  | —        | —  |
| —  | —        | —  | —  | id | —        | —  |
| —  | —        | —  | —  | —  | id       | —  |
| —  | —        | —  | —  | —  | —        | id |

# Résultats

## Unicité

Soit  $T$  un tableau de calcul du groupe  $G$  et pour tout  $1 \leq i \leq p$  deux permutations  $\sigma_i$  et  $\sigma'_i$  de la même ligne  $T_i$  de  $T$  alors

$$\sigma_p \sigma_{p-1} \cdots \sigma_2 \sigma_1 = \sigma'_p \sigma'_{p-1} \cdots \sigma'_2 \sigma'_1$$

implique  $\sigma_i = \sigma'_i$  pour tout  $i$ .

# Résultats

## Unicité

Soit  $T$  un tableau de calcul du groupe  $G$  et pour tout  $1 \leq i \leq p$  deux permutations  $\sigma_i$  et  $\sigma'_i$  de la même ligne  $T_i$  de  $T$  alors

$$\sigma_p \sigma_{p-1} \cdots \sigma_2 \sigma_1 = \sigma'_p \sigma'_{p-1} \cdots \sigma'_2 \sigma'_1$$

implique  $\sigma_i = \sigma'_i$  pour tout  $i$ .

## Tableau complet

$T$  est un tableau complet de calcul du groupe  $G$  si toute permutation du groupe admet une décomposition de la forme

$$\sigma_n \sigma_{n-1} \cdots \sigma_2 \sigma_1$$

où  $\sigma_i$  appartient à la ligne  $T_i$  de  $T$ .

# Procédure Sift

**Require:**  $\alpha$  : permutation.

**Ensure:**  $u$  : permutation.

```
1:  $u \leftarrow \alpha$ 
2:  $i \leftarrow 1$ 
3:  $j \leftarrow \alpha(i)$ 
4: while  $i \leq n$  et défini( $t[i, j]$ ) do
5:    $u \leftarrow u \cdot (t[i, j])^{-1}$ 
6:    $i \leftarrow i + 1$ 
7:    $j \leftarrow u(i)$ 
8: end while
```

## Théorème

Les assertions suivantes sont équivalentes :

- 1 Le groupe  $G$  a un cardinal égal à  $\prod_{i=1}^n t_i$  où  $t_i$  est le nombre de permutations se trouvant sur la ligne  $T_i$  du tableau  $T$ .

## Théorème

Les assertions suivantes sont équivalentes :

- 1 Le groupe  $G$  a un cardinal égal à  $\prod_{i=1}^n t_i$  où  $t_i$  est le nombre de permutations se trouvant sur la ligne  $T_i$  du tableau  $T$ .
- 2  $T$  est un tableau complet de calcul pour  $G$ .

## Théorème

Les assertions suivantes sont équivalentes :

- 1 Le groupe  $G$  a un cardinal égal à  $\prod_{i=1}^n t_i$  où  $t_i$  est le nombre de permutations se trouvant sur la ligne  $T_i$  du tableau  $T$ .
- 2  $T$  est un tableau complet de calcul pour  $G$ .
- 3 Pour toute permutation  $\alpha$  engendrée par les éléments de  $T$  on a  $\text{Sift}_T(\alpha) = \text{id}$ .

## Théorème

Les assertions suivantes sont équivalentes :

- 1 Le groupe  $G$  a un cardinal égal à  $\prod_{i=1}^n t_i$  où  $t_i$  est le nombre de permutations se trouvant sur la ligne  $T_i$  du tableau  $T$ .
- 2  $T$  est un tableau complet de calcul pour  $G$ .
- 3 Pour toute permutation  $\alpha$  engendrée par les éléments de  $T$  on a  $\text{Sift}_T(\alpha) = \text{id}$ .
- 4 Pour tout couple  $(x, y)$  d'éléments de  $T$  on a  $\text{Sift}_T(xy) = \text{id}$ .

# Plan

1 Procédure Sift

2 Rubik's Cube

# Modélisation

- 6 faces, 54 carrés.

# Modélisation

- 6 faces, 54 carrés.
- Centres fixés : 48 carrés mobiles.

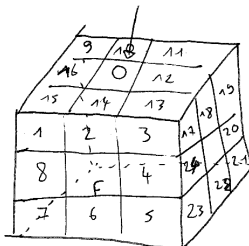
# Modélisation

- 6 faces, 54 carrés.
- Centres fixés : 48 carrés mobiles.
- 6 actions possibles, agissant en permutant certains carrés.

$$\mathcal{R} = \langle F, B, U, D, L, R \rangle \subset S_{48}$$

# Modélisation

|    |    |    |
|----|----|----|
| 41 | 42 | 43 |
| 48 |    | 44 |
| 47 | 46 | 45 |



|    |    |    |
|----|----|----|
| 33 | 34 | 35 |
| 40 |    | 36 |
| 39 | 38 | 37 |

|    |    |    |
|----|----|----|
| 25 | 26 | 27 |
| 32 |    | 28 |
| 31 | 30 | 29 |

# Modélisation

Rotation = produit de 5 cycles de longueur 4 :

$$F = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)(15\ 17\ 29\ 39)(14\ 24\ 30\ 40)(13\ 23\ 31\ 33)$$

$$U = (9\ 11\ 13\ 15)(10\ 12\ 14\ 16)(1\ 35\ 43\ 17)(2\ 34\ 42\ 18)(3\ 33\ 41\ 19)$$

$$L = (33\ 35\ 37\ 39)(34\ 36\ 38\ 40)(1\ 9\ 47\ 31)(8\ 16\ 48\ 32)(7\ 15\ 41\ 25)$$

$$R = (17\ 19\ 21\ 23)(18\ 20\ 22\ 24)(3\ 11\ 45\ 29)(4\ 12\ 44\ 28)(5\ 13\ 43\ 27)$$

$$D = (31\ 25\ 27\ 29)(30\ 32\ 26\ 28)(5\ 39\ 47\ 21)(6\ 38\ 46\ 22)(7\ 37\ 45\ 23)$$

$$B = (41\ 43\ 45\ 47)(42\ 44\ 46\ 48)(9\ 19\ 27\ 37)(10\ 20\ 26\ 36)(11\ 21\ 25\ 35)$$

# Questions sur le Rubik's Cube

- Combien y a-t-il de configurations atteignables ?

# Questions sur le Rubik's Cube

- Combien y a-t-il de configurations atteignables ?
- Combien faut-il au maximum de mouvements de rotation pour résoudre une configuration donnée (*i.e.* la distance à la configuration initiale) ?

# Cardinal du Rubik's Cube

|    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|
| 0  | 24 | 1  | 24 | 2  | 21 | 3  | 22 | 4  | 18 | 5  | 20 |
| 6  | 15 | 7  | 18 | 8  | 12 | 9  | 16 | 10 | 9  | 11 | 14 |
| 12 | 1  | 13 | 1  | 14 | 1  | 15 | 12 | 16 | 1  | 17 | 1  |
| 18 | 1  | 19 | 10 | 20 | 6  | 21 | 8  | 22 | 1  | 23 | 1  |
| 24 | 1  | 25 | 6  | 26 | 1  | 27 | 1  | 28 | 1  | 29 | 1  |
| 30 | 1  | 31 | 2  | 32 | 1  | 33 | 1  | 34 | 1  | 35 | 1  |
| 36 | 1  | 37 | 1  | 38 | 1  | 39 | 1  | 40 | 1  | 41 | 1  |
| 42 | 1  | 43 | 1  | 44 | 1  | 45 | 1  | 46 | 1  | 47 | 1  |

$$|\mathcal{R}| = 24 \cdot 24 \cdot 21 \cdot 3 \dots 1 = 43252003274489856000$$

( $\approx 1,17 \cdot 2^{65} \approx 4,32 \cdot 10^{19}$ ).

# Nombre optimal de coups

*Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .
- 1995 :  $17 \leq \mathcal{G} \leq 29$ .

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .
- 1995 :  $17 \leq \mathcal{G} \leq 29$ .
- 2006 :  $17 \leq \mathcal{G} \leq 27$ .

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .
- 1995 :  $17 \leq \mathcal{G} \leq 29$ .
- 2006 :  $17 \leq \mathcal{G} \leq 27$ .
- 2007 :  $20 \leq \mathcal{G} \leq 26$ .

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .
- 1995 :  $17 \leq \mathcal{G} \leq 29$ .
- 2006 :  $17 \leq \mathcal{G} \leq 27$ .
- 2007 :  $20 \leq \mathcal{G} \leq 26$ .
- Chaînes de sous-groupes.

# Nombre optimal de coups

## *Twenty-Six Moves Suffice for Rubik's Cube*

Daniel Kunkle, Gene Cooperman (2007).

- Coup = face touchée (donc 18 générateurs).
- 1982 :  $17 \leq \mathcal{G} \leq 52$ .
- 1995 :  $17 \leq \mathcal{G} \leq 30$ .
- 1995 :  $17 \leq \mathcal{G} \leq 29$ .
- 2006 :  $17 \leq \mathcal{G} \leq 27$ .
- 2007 :  $20 \leq \mathcal{G} \leq 26$ .
- Chaînes de sous-groupes.

Pour Kunkle et Cooperman, on choisit  $S$  le sous-groupe carré et on considère les classes sous l'action de  $S$ .

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)
- Calcul de la distance de toute classe à la classe  $id$ .

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)
- Calcul de la distance de toute classe à la classe  $id$ .
- Multiplication efficace d'éléments et de classes du groupe.

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)
- Calcul de la distance de toute classe à la classe  $id$ .
- Multiplication efficace d'éléments et de classes du groupe.
- Calcul parallèle sur 7TB de données.

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)
- Calcul de la distance de toute classe à la classe  $id$ .
- Multiplication efficace d'éléments et de classes du groupe.
- Calcul parallèle sur 7TB de données.
- Une fonction de hachage parfaite efficace.

# Plan du résultat

- Construction du graphe de Cayley de  $S$  (exploration en profondeur)
- Calcul de la distance de tout élément de  $S$  à  $id$  (*meet in the middle*)
- Calcul de la distance de toute classe à la classe  $id$ .
- Multiplication efficace d'éléments et de classes du groupe.
- Calcul parallèle sur 7TB de données.
- Une fonction de hachage parfaite efficace.
- Une représentation compacte du graphe des classes (4 bits par état).

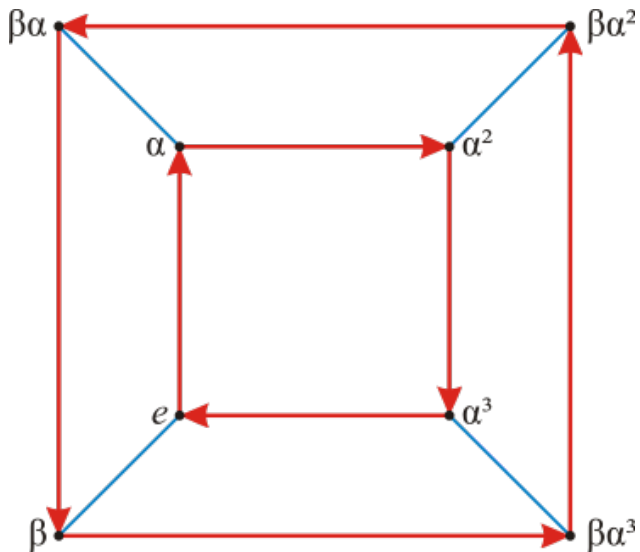
# Cardinal de $S$

|    |   |    |   |    |   |    |   |    |   |    |   |
|----|---|----|---|----|---|----|---|----|---|----|---|
| 0  | 4 | 1  | 4 | 2  | 4 | 3  | 4 | 4  | 3 | 5  | 3 |
| 6  | 1 | 7  | 3 | 8  | 2 | 9  | 2 | 10 | 1 | 11 | 4 |
| 12 | 1 | 13 | 1 | 14 | 1 | 15 | 3 | 16 | 1 | 17 | 1 |
| 18 | 1 | 19 | 2 | 20 | 1 | 21 | 1 | 22 | 1 | 23 | 1 |
| 24 | 1 | 25 | 1 | 26 | 1 | 27 | 1 | 28 | 1 | 29 | 1 |
| 30 | 1 | 31 | 1 | 32 | 1 | 33 | 1 | 34 | 1 | 35 | 1 |
| 36 | 1 | 37 | 1 | 38 | 1 | 39 | 1 | 40 | 1 | 41 | 1 |
| 42 | 1 | 43 | 1 | 44 | 1 | 45 | 1 | 46 | 1 | 47 | 1 |

$$|S| = 663552$$

$$\text{et } [G : S] = 65182537728000 (6,51 \cdot 10^{13}).$$

# Graphe de Cayley



# Graphe de Cayley de $S$

- 663552 sommets ;

# Graphe de Cayley de $S$

- 663552 sommets ;
- Construit par exploration en profondeur sur les 6 générateurs ;

# Graphe de Cayley de $S$

- 663552 sommets ;
- Construit par exploration en profondeur sur les 6 générateurs ;
- Recherche « en avant » de profondeur 7 ;

# Graphe de Cayley de $S$

- 663552 sommets ;
- Construit par exploration en profondeur sur les 6 générateurs ;
- Recherche « en avant » de profondeur 7 ;
- Recherche arrière depuis les 663552 sommets ;

# Graphe de Cayley de $S$

- 663552 sommets ;
- Construit par exploration en profondeur sur les 6 générateurs ;
- Recherche « en avant » de profondeur 7 ;
- Recherche arrière depuis les 663552 sommets ;
- On prouve que la distance est majorée par 13.

# Graphe des classes de Schreier

- 65182537728000 sommets ;

# Graphe des classes de Schreier

- 65182537728000 sommets ;
- Construit par exploration en profondeur sur les 12 générateurs ;

# Graphe des classes de Schreier

- 65182537728000 sommets ;
- Construit par exploration en profondeur sur les 12 générateurs ;
- Stocké sur le disque niveau par niveau.

# Grphe des classes de Schreier

- 65182537728000 sommets ;
- Construit par exploration en profondeur sur les 12 gnrérateurs ;
- Stocké sur le disque niveau par niveau.
- On prouve que la distance est majorée par 16.

# Multiplication rapide

- Représentation unique d'un élément du groupe en produit d'actions sur les coins, et sur les arêtes ;

# Multiplication rapide

- Représentation unique d'un élément du groupe en produit d'actions sur les coins, et sur les arêtes ;
- Tables de précalcul dans ces sous-groupes ;

# Multiplication rapide

- Représentation unique d'un élément du groupe en produit d'actions sur les coins, et sur les arêtes ;
- Tables de précalcul dans ces sous-groupes ;
- Composition = addition mod 2 pour l'action sur les arêtes, mod 3 sur les coins.