The group of moves of the Rubik's cube

The fall school 2014

Adam Stejskal

November 21, 2014

Labeling and notation

Basic structure

- Structure of cube - three layers
- corner, edge and central subcubes
- twist and flip

Labeling and notation

The group of illegal moves

- the basic moves are F,U,R,B,D,L
- the illegal moves via disassembling
- group $H = \langle \{R, L, F, B, U, D\} \cup \{\text{'illegal moves'}\} \rangle$

Labeling and notation

Reference marks

- The standard reference mark
- edges: *uf, ur, ub, ul, lf, fr, rb, bl, df, dr, db, dl*
- corners: U or D facets
- The relative reference mark

Labeling and notation

numbering of subcubes

- The set of edges E, $|E| = 12$
- The set of vertices V, $|V| = 8$

Labeling and notation

subcube permutations

- The action of H on E induces a homomorphism $\sigma : H \to S_{12}$
- The action of H on V induces a homomorphism $\rho : H \to S_8$

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)
- *Orientation* of an edge 'is in' C_2

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)
- *Orientation* of an edge 'is in' C_2
- *Orientation vector* 'is in' C_2^{12}

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)
- *Orientation* of an edge 'is in' C_2
- *Orientation vector* 'is in' C_2^{12}
- *Edge orientation change* is $w : H \to C_2^{12}$, where $h \in H$ is mapped to the orientation vector after applying move h.

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)
- *Orientation* of an edge 'is in' C_2
- *Orientation vector* 'is in' C_2^{12}
- *Edge orientation change* is $w : H \to C_2^{12}$, where $h \in H$ is mapped to the orientation vector after applying move h.

Lemma 1: For $g, h \in H$: $w(gh) = w(g) + Pw(h)$, where P is permutation matrix of $\sigma(g)^{-1}$.

Labeling and notation

orientation vectors

- *Orientation* of an edge: Number of flips needed to obtain the standard position. (0 or 1)
- *Orientation* of an edge 'is in' C_2
- *Orientation vector* 'is in' C_2^{12}
- *Edge orientation change* is $w : H \to C_2^{12}$, where $h \in H$ is mapped to the orientation vector after applying move h.

Lemma 1: For $g, h \in H$: $w(gh) = w(g) + Pw(h)$, where P is permutation matrix of $\sigma(g)^{-1}$.

'Proof': After move g, the numbers of edges are changed.

Labeling and notation

orientation vectors

- *Orientation* of a vertex: Number of (clockwise) twists needed to obtain the standard position. (0, 1 or 2)

Labeling and notation

orientation vectors

- *Orientation* of a vertex: Number of (clockwise) twists needed to obtain the standard position. (0, 1 or 2)
- *Orientation* of a vertex 'is in' C_3

Labeling and notation

orientation vectors

- *Orientation* of a vertex: Number of (clockwise) twists needed to obtain the standard position. (0, 1 or 2)
- *Orientation* of a vertex 'is in' C_3
- *Orientation vector* 'is in' C_3^8

Labeling and notation

orientation vectors

- *Orientation* of a vertex: Number of (clockwise) twists needed to obtain the standard position. (0, 1 or 2)
- *Orientation* of a vertex 'is in' C_3
- *Orientation vector* 'is in' C_3^8
- *Vertex orientation change* is $v : H \to C_3^8$, where $h \in H$ is mapped to the orientation vector after applying move h.

Labeling and notation

orientation vectors

- *Orientation* of a vertex: Number of (clockwise) twists needed to obtain the standard position. (0, 1 or 2)
- *Orientation* of a vertex 'is in' C_3
- *Orientation vector* 'is in' C_3^8
- *Vertex orientation change* is $v : H \to C_3^8$, where $h \in H$ is mapped to the orientation vector after applying move h.

Lemma 1: For $g, h \in H$: $v(gh) = v(g) + Pv(h)$, where P is permutation matrix of $\rho(g)^{-1}$.

It looks familiar, doesn't it?

The group structure

semi-direct product

- Consider the following semi-direct product:

$$H' = (C_3^8 \rtimes_\varphi S_8) \times (C_2^{12} \rtimes_\psi S_{12}),$$

- together with

$$\varphi : S_V \to Aut(C_3^8),$$

$\pi \mapsto P$, where P is the permutation matrix of π^{-1}

and

$$\psi : S_E \to Aut(C_2^{12}),$$

$\omega \mapsto Q$, where Q is the permutation matrix of ω^{-1}

The group structure

semi-direct product

Proposition: $H \cong H'$

Proof: The isomorphism is
$\phi : g \mapsto (v(g), \rho(g), w(g), \sigma(g))$. (Lemma 1)
ϕ is surjective, because we can disassemble the cube.
$Ker\phi$ is trivial.

The group structure
legal moves

By previous proposition, we can represent the positions of the Rubik's cube as elements of $C_3^8 \times S_8 \times C_2^{12} \times S_{12}$.

Question: Given a 4-tuple $(v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$, how can we decide, whether it is a legal move of the Rubik's cube?

Answer: next theorem

The group structure

legal moves

Theorem: *For all $g \in H$:*

$g \in \langle\{R, L, F, B, U, D\}\rangle$ *(i.e. g is a legal move)*

if and only if the following conditions hold

(P) $sgn(\rho(g)) = sgn(\sigma(g))$

(F) $\sum_{i=1}^{8}(v(g))_i = 0$ *(mod 3)*

(T) $\sum_{i=1}^{12}(w(g))_i = 0$ *(mod 2)*

Proof of Theorem

downward implication

Assume that $g = (v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$ is a legal move.

Proof of Theorem

downward implication

Assume that $g = (v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$ is a legal move.

It means that $g = X_1 X_2 \ldots X_k$, where X_i are basic moves.

Proof of Theorem

downward implication

Assume that $g = (v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$ is a legal move.

It means that $g = X_1 X_2 \dots X_k$, where X_i are basic moves.

For each basic move X: $sgn(\rho(X)) = sgn(\sigma(X))$

Proof of Theorem

downward implication

Assume that $g = (v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$ is a legal move.

It means that $g = X_1 X_2 \dots X_k$, where X_i are basic moves.

For each basic move X: $sgn(\rho(X)) = sgn(\sigma(X))$

$sgn(r) = sgn(\rho(g)) = \Pi_{i=1}^{k} sgn(\rho(X_i)) = \Pi_{i=1}^{k} sgn(\sigma(X_i)) =$
$= \ sgn(s)$.

Proof of Theorem

downward implication

Assume that $g = (v, r, w, s) \in C_3^8 \times S_8 \times C_2^{12} \times S_{12}$ is a legal move.

It means that $g = X_1 X_2 \ldots X_k$, where X_i are basic moves.

For each basic move X: $sgn(\rho(X)) = sgn(\sigma(X))$

$sgn(r) = sgn(\rho(g)) = \Pi_{i=1}^{k} sgn(\rho(X_i)) = \Pi_{i=1}^{k} sgn(\sigma(X_i)) = $
$= \; sgn(s)$.

And it's the condition *(P)*.

Proof of Theorem

downward implication

- We know $g = X_1 X_2 \ldots X_k$, where X_i are basic moves.

Proof of Theorem

downward implication

- We know $g = X_1 X_2 \dots X_k$, where X_i are basic moves.
- Assume k is minimal. The condition *(T)* follows from induction on k.

Proof of Theorem

downward implication

- We know $g = X_1 X_2 \dots X_k$, where X_i are basic moves.
- Assume k is minimal. The condition *(T)* follows from induction on k.

$v = v(g) = v(X_1 X_2 \dots X_k) = Pv(X_k) + v(X_1 X_2 \dots X_{k-1})$ (By Lemma 1)

Proof of Theorem

downward implication

- We know $g = X_1 X_2 \dots X_k$, where X_i are basic moves.
- Assume k is minimal. The condition *(T)* follows from induction on k.

  $v = v(g) = v(X_1 X_2 \dots X_k) = Pv(X_k) + v(X_1 X_2 \dots X_{k-1})$ (By Lemma 1)

  But condition *(T)* holds for both summands on the right hand size.

Proof of Theorem

downward implication

- We know $g = X_1 X_2 \ldots X_k$, where X_i are basic moves.
- Assume k is minimal. The condition *(T)* follows from induction on k.

  $v = v(g) = v(X_1 X_2 \ldots X_k) = Pv(X_k) + v(X_1 X_2 \ldots X_{k-1})$ (By Lemma 1)

  But condition *(T)* holds for both summands on the right hand size.

  The condition *(F)* may be prooved analogically.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P)*, *(T)*, *(F)*.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.
- At first, we find a move $m_1 = (a, \pi, b, \tau)$, such that $gm_1 = (a', 1, b', \tau')$. So m_1 solves the corners.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.
- At first, we find a move $m_1 = (a, \pi, b, \tau)$, such that $gm_1 = (a', 1, b', \tau')$. So m_1 solves the corners.
- Lets look at the move $m_0 = (DRD^{-1}R^{-1}F)^3$.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.
- At first, we find a move $m_1 = (a, \pi, b, \tau)$, such that $gm_1 = (a', 1, b', \tau')$. So m_1 solves the corners.
- Lets look at the move $m_0 = (DRD^{-1}R^{-1}F)^3$.
- $\rho(m_0) = (dbr, urb)$

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.
- At first, we find a move $m_1 = (a, \pi, b, \tau)$, such that $gm_1 = (a', 1, b', \tau')$. So m_1 solves the corners.
- Lets look at the move $m_0 = (DRD^{-1}R^{-1}F)^3$.
- $\rho(m_0) = (dbr, urb)$
- There exists ω, such that $\rho(m_0)^\omega$ is an arbitrary transposition of corners.

Proof of Theorem

upward implication

- Assume $g = (v, r, w, s)$ satisfies conditions *(P), (T), (F)*.
- We will 'solve the cube'.
- At first, we find a move $m_1 = (a, \pi, b, \tau)$, such that $gm_1 = (a', 1, b', \tau')$. So m_1 solves the corners.
- Lets look at the move $m_0 = (DRD^{-1}R^{-1}F)^3$.
- $\rho(m_0) = (dbr, urb)$
- There exists ω, such that $\rho(m_0)^\omega$ is an arbitrary transposition of corners.
- So there exists the desired legal move m_1.

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.
- Lets look at the move $n_0 = (DR^{-1})^3(D^{-1}R)^3$

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.
- Lets look at the move $n_0 = (DR^{-1})^3(D^{-1}R)^3$
- $v(n_0) = (0,2,0,0,1,0,0,0)$, $\rho(n_0) = 1$

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.
- Lets look at the move $n_0 = (DR^{-1})^3(D^{-1}R)^3$
- $v(n_0) = (0, 2, 0, 0, 1, 0, 0, 0)$, $\rho(n_0) = 1$
- By conjugation, we can twist any pair of corners.

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.
- Lets look at the move $n_0 = (DR^{-1})^3(D^{-1}R)^3$
- $v(n_0) = (0, 2, 0, 0, 1, 0, 0, 0)$, $\rho(n_0) = 1$
- By conjugation, we can twist any pair of corners.
- So we can set 7 corners into right orientation.

Proof of Theorem

upward implication

- Now we need to solve the orientation of corners.
- Lets look at the move $n_0 = (DR^{-1})^3(D^{-1}R)^3$
- $v(n_0) = (0, 2, 0, 0, 1, 0, 0, 0)$, $\rho(n_0) = 1$
- By conjugation, we can twist any pair of corners.
- So we can set 7 corners into right orientation.
- The 8th corner has to be oriented right, thanks to the condition *(T)*.

Proof of Theorem

upward implication

- How to solve the edges?

Proof of Theorem

upward implication

- How to solve the edges?
- $m_0' = LR^{-1}U^2L^{-1}RB^2$ is a 3-cycle of edges.

Proof of Theorem

upward implication

- How to solve the edges?
- $m_0' = LR^{-1}U^2L^{-1}RB^2$ is a 3-cycle of edges.
- Moreover $\rho(m_0') = 1$, $v(m_0') = \mathbf{0}$ (and $w(m_0') = \mathbf{0}$)

Proof of Theorem

upward implication

- How to solve the edges?
- $m_0' = LR^{-1}U^2L^{-1}RB^2$ is a 3-cycle of edges.
- Moreover $\rho(m_0') = 1$, $v(m_0') = \mathbf{0}$ (and $w(m_0') = \mathbf{0}$)
- By conjugation, we can cycle arbitrary three edges without affecting corners.

Proof of Theorem

upward implication

- How to solve the edges?
- $m_0' = LR^{-1}U^2L^{-1}RB^2$ is a 3-cycle of edges.
- Moreover $\rho(m_0') = 1$, $v(m_0') = \mathbf{0}$ (and $w(m_0') = \mathbf{0}$)
- By conjugation, we can cycle arbitrary three edges without affecting corners.
- So we can perform any even permutation on the edges.

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation
- $sgn(\tau'') = sgn(s)sgn(\sigma(m_1))sgn(\sigma(m_2)) =$
  $= \ sgn(r)sgn(\rho(m_1))sgn(\rho(m_2)) = sgn(r\rho(m_1)\rho(m_2))$

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation
- $sgn(\tau'') = sgn(s)sgn(\sigma(m_1))sgn(\sigma(m_2)) =$
  $= \ sgn(r)sgn(\rho(m_1))sgn(\rho(m_2)) = sgn(r\rho(m_1)\rho(m_2))$
- $sgn(\tau'') = sgn(1)$

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation
- $sgn(\tau'') = sgn(s)sgn(\sigma(m_1))sgn(\sigma(m_2)) =$
  $= \ sgn(r)sgn(\rho(m_1))sgn(\rho(m_2)) = sgn(r\rho(m_1)\rho(m_2))$
- $sgn(\tau'') = sgn(1)$
- So we can perform the move m_3, such that $\rho(m_3) = 1$, $v(m_3) = \mathbf{0}$ and $\sigma(m_3) = (\tau'')^{-1}$

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation
- $sgn(\tau'') = sgn(s)sgn(\sigma(m_1))sgn(\sigma(m_2)) =$
  $= \; sgn(r)sgn(\rho(m_1))sgn(\rho(m_2)) = sgn(r\rho(m_1)\rho(m_2))$
- $sgn(\tau'') = sgn(1)$
- So we can perform the move m_3, such that $\rho(m_3) = 1$, $v(m_3) = \mathbf{0}$ and $\sigma(m_3) = (\tau'')^{-1}$
- It remains to orient the edges.

Proof of Theorem

upward implication

- We have moves m_1, m_2 such that $gm_1m_2 = (\mathbf{0}, 1, w', \tau'')$, where $\tau'' = s\sigma(m_1)\sigma(m_2)$
- τ'' is even permutation
- $sgn(\tau'') = sgn(s)sgn(\sigma(m_1))sgn(\sigma(m_2)) =$
  $= \ sgn(r)sgn(\rho(m_1))sgn(\rho(m_2)) = sgn(r\rho(m_1)\rho(m_2))$
- $sgn(\tau'') = sgn(1)$
- So we can perform the move m_3, such that $\rho(m_3) = 1$, $v(m_3) = \mathbf{0}$ and $\sigma(m_3) = (\tau'')^{-1}$
- It remains to orient the edges.
- Try $LR^{-1}FLR^{-1}DLR^{-1}BLR^{-1}ULR^{-1}F^{-1}LR^{-1}D^{-1}LR^{-1}B^{-1}LR^{-1}U^{-1}$

The Rubik's cube group

- Consider $G_0 = \{(v, r, w, s) \in H | conditions(T), (F) hold\}$, with the group operation of H.
- The Rubik's cube group G is the kernel of homomorphism

$$\phi : G_0 \to \{-1, 1\},$$

  where $(v, r, w, s) \mapsto sgn(r)sgn(s)$.
- $[H : G] = 12$