Gottfried Wilhelm
Leibniz Universität Hannover
Fakultät für Elektrotechnik und Informatik
Institut für Theoretische Informatik

Finden einer optimalen Lösung von Rubik's Cube ist NP-vollständig

Finding an optimal solution for Rubik's Cube is NP-complete

Bachelorarbeit

im Studiengang Bachelor of Science Informatik

von

Kai Christian Hallmann

Matrikelnummer: 10019681

Prüfer: Prof. Dr. rer. nat. Heribert Vollmer
Zweitprüfer: PD Dr. rer. nat. habil. Arne Meier
Betreuerin: Sabrina Gaube, M. Sc.

Hannover, 2022-01-10

Erklärung der Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Bachelorarbeit selbständig und ohne fremde Hilfe verfasst und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel verwendet habe. Die Arbeit hat in gleicher oder ähnlicher Form noch keinem anderen Prüfungsamt vorgelegen.

Hannover, den 2022-01-10

Kai Christian Hallmann

Inhaltsverzeichnis

Kapitel 1

Einleitung

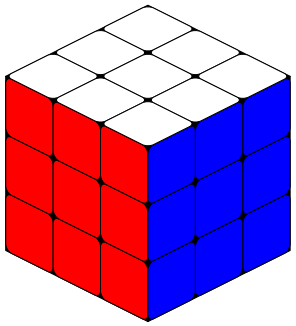


Abbildung 1.1: Der Rubik's Cube

Der Rubik's Cube, der in Abbildung 1.1 zu sehen ist, ist ein weltbekanntes Drehpuzzle mit dem Ziel, durch Drehungen der Außenseiten die verschiedenfarbigen Aufkleber so anzuordnen, dass die Aufkleber auf jeder Außenseite jeweils dieselbe Farbe haben. Weit verbreitete Problemstellungen sind es, überhaupt eine Lösung zu finden und in möglichst kurzer Zeit eine Lösung zu finden. Eine weitere Disziplin besteht darin, einen Rubik's Cube in möglichst wenig Zügen zu lösen. Es ist denkbar, dass eine Lösung mit möglichst wenig Zügen auch hilfreich sein könnte, um einen Rubik's Cube möglichst schnell zu lösen. In der Praxis stellt sich jedoch heraus, dass es zumindest für Menschen viel zu lange dauert, kurze Lösungen zu finden. Die schnellsten Lösungen bei Wettbewerben brauchen meist nur einige Sekunden, während die Teilnehmer in der Kategorie "3x3x3 Fewest Moves", in der es genau darum geht, eine möglichst kurze Lösung zu finden, eine volle Stunde Zeit haben und trotzdem fast nie die optimale Lösung finden. Die besten gefundenen Lösungen brauchen meist zwischen 20 und 30 Zügen ([WCA21]), obwohl bekannt ist, dass ein Rubik's Cube immer in maximal 20 und in den meisten Fällen in weniger Zügen gelöst werden kann, wie in [Rok+10] gezeigt wurde.

Computer sind inzwischen in der Lage, tatsächlich optimale Lösungen für Rubik's Cube zu finden. Jedoch kann dies immer noch mehrere Stunden dauern ([Bot20] und [Bot21]). Daher wollen wir in dieser Arbeit zeigen, dass das Finden einer optimalen Lösung schon aus komplexitätstheoretischen Gründen ein schwieriges Problem ist. Dafür betrachten wir nicht nur $3\times3\times3$ Rubik's Cube, sondern auch verallgemeinerte $n \times n \times n$ Rubik's Cube und definieren in Kapitel 3 Entscheidungsprobleme, die dem Finden von optimalen Lösungen entsprechen. Dann werden wir in den Kapiteln 5 und 6 zeigen, dass diese Probleme NP-vollständig sind, das heißt, dass sie zu den schwierigsten Problemen in der Klasse NP gehören und damit, dass es vermutlich keinen Algorithmus bzw. kein Programm gibt, dass sie in Polynomialzeit, also effizient, lösen kann.

Wir werden insbesondere zeigen, dass die Probleme NP-schwer sind, indem wir zeigen, dass Graphenprobleme, von denen bereits bekannt ist, dass sie NP-schwer sind, auf unsere Probleme in Polynomialzeit m-reduzierbar sind. Außerdem werden wir, bevor wir uns mit dem Rubik's Cube beschäftigen, zuerst den Rubik's Square betrachten, der einem $n \times n \times 1$ Quader mit ähnlichen Eigenschaften zum Rubik's Cube entspricht. Weil dem Rubik's Square quasi eine der drei Dimensionen fehlt, ist es einfacher, zuerst mit ihm zu arbeiten und sich erst dann dem Rubik's Cube zuzuwenden, wenn die Beweisideen bereits bekannt sind.

Der Aufbau dieser Arbeit orientiert sich hauptsächlich an [DER17], dessen Inhalte in den Kapiteln 3-6 vorgestellt werden.

Kapitel 2

Grundlagen

In diesem Kapitel finden sich grundlegende Definitionen, die wir in dieser Arbeit verwenden.

2.1 Graphen

In diesem Abschnitt geht es um die graphentheoretischen Grundlagen, die wir im Weiteren brauchen werden. Die Definitionen sind aus [SW16] und [DER17] übernommen und ggf. angepasst.

Die folgenden Definitionen 2.1.1-2.1.4 sollten weitestgehend bekannt sein und sind hier nur angegeben, um Uneindeutigkeiten zu vermeiden.

Definition 2.1.1. Ein **Graph** ist ein Tupel $G = (V, E)$, das aus einer nichtleeren Knotenmenge V und einer Kantenmenge

$$E \subseteq \{\{v, w\} \mid v, w \in V \text{ und } v \neq w\}$$

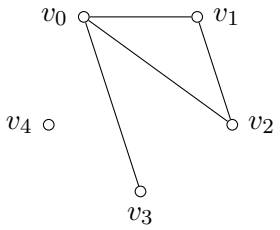
besteht.

Definition 2.1.2. Ein **endlicher Graph** $G = (V, E)$ ist ein Graph, dessen Knotenmenge V endlich groß ist.

Ein beispielhafter endlicher Graph ist in Abbildung 2.1 zu sehen.

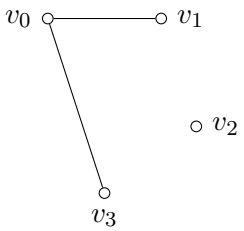
Definition 2.1.3. Ein **Teilgraph** eines Graphen $G = (V, E)$ ist ein Graph $G' = (V', E')$, dessen Knotenmenge $V' \subseteq V$ ist und dessen Kantenmenge $E' \subseteq E$ ist.

Ein beispielhafter Teilgraph ist in Abbildung 2.2 zu sehen.



$$G_1 = (\{v_0, v_1, v_2, v_3, v_4\}, \{\{v_0, v_1\}, \{v_1, v_2\}, \{v_0, v_2\}, \{v_0, v_3\}\})$$

Abbildung 2.1: Ein endlicher Graph



$$G_2 = (\{v_0, v_1, v_2, v_3\}, \{\{v_0, v_1\}, \{v_0, v_3\}\})$$

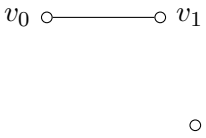
Abbildung 2.2: Ein Teilgraph von G_1

Definition 2.1.4. Ein **induzierter Teilgraph** eines Graphen G ist ein Teilgraph $G' = (V', E')$ von $G = (V, E)$, dessen Kantenmenge

$$E' = \{\{v, w\} \mid v, w \in V'\} \cap E$$

ist.

Ein induzierter Teilgraph lässt sich also in einem Graph G anhand nur seiner Knotenmenge bestimmen. Ein beispielhafter induzierter Teilgraph ist in Abbildung 2.3 zu sehen.



$$G_3 = (\{v_0, v_1, v_2\}, \{\{v_0, v_1\}\})$$

Abbildung 2.3: Ein induzierter Teilgraph von G_2

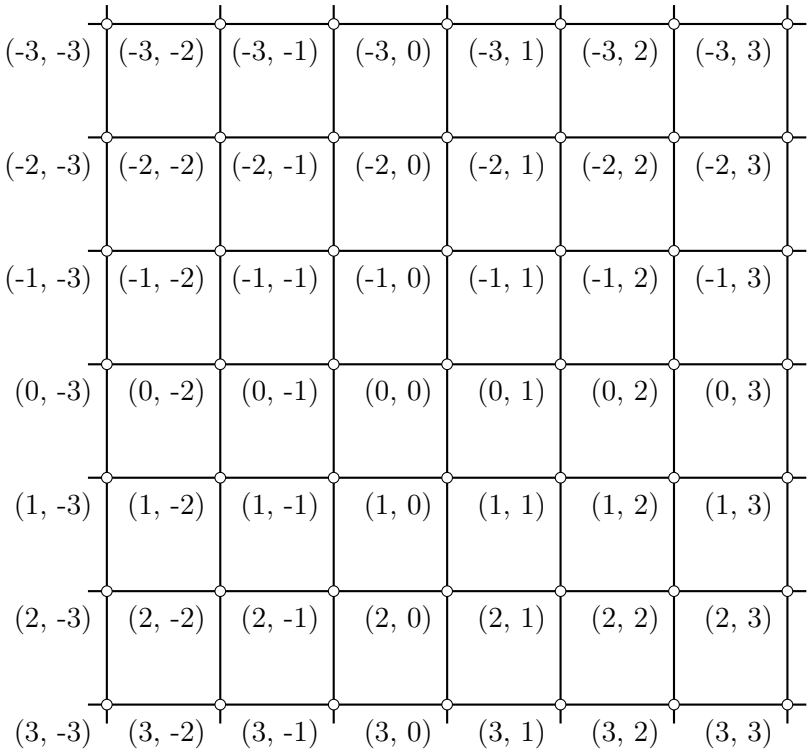
Die Gittergraphen und kubischen Graphen in den Definitionen 2.1.5-2.1.8 werden wir in Entscheidungsproblemen verwenden, mithilfe derer wir später die NP-Schwere unserer Probleme zeigen werden.

Definition 2.1.5. Der **unendliche vollständige Gittergraph** G^∞ ist der Graph in der Ebene $\mathbb{Z}^2$, dessen Knoten ganzzahlige Koordinaten haben und genau dann mit einer Kante verbunden sind, wenn sie einen euklidischen Abstand von 1 haben. Es gilt also

$$G^\infty = (\mathbb{Z}^2, \{\{v, w\} \mid v, w \in \mathbb{Z}^2 \text{ und } d(v, w) = 1\})$$

mit $d((v_x, v_y), (w_x, w_y)) = \sqrt{(v_x - w_x)^2 + (v_y - w_y)^2}$.

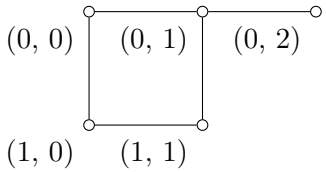
Ein Ausschnitt davon ist in Abbildung 2.4 zu sehen.



$G_4 = G^\infty$

Abbildung 2.4: Ein Ausschnitt des unendlichen vollständigen Gittergraphen im Bereich $-3 \leq x, y \leq 3$

Definition 2.1.6. Ein **Gittergraph** ist ein endlicher induzierter Teilgraph von G^∞. Er lässt sich also durch eine endliche Teilmenge von $\mathbb{Z}^2$ eindeutig bestimmen.



$G_5 = (\{(0,0),(0,1),(0,2),(1,0),(1,1)\}, E_5)$ induziert in G^∞

Abbildung 2.5: Ein Gittergraph

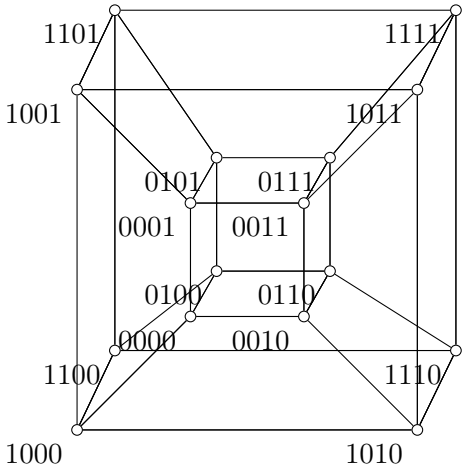
Ein beispielhafter Gittergraph ist in Abbildung 2.5 zu sehen.

Definition 2.1.7. Der m-dimensionale **Hyperwürfelgraph** H_m für ein $m \in \mathbb{Z}_{>0}$ ist der Graph, dessen Knoten die Bitstrings der Länge m sind und genau dann mit einer Kante verbunden sind, wenn sie einen Hamming-Abstand von 1 haben. Formal ausgedrückt heißt dies

$$H_m = (\{0,1\}^m, \{\{v,w\} \mid v,w \in \{0,1\}^m \text{ und } \Delta(v,w) = 1\})$$

mit $\Delta((v_1, v_2, \ldots, v_m), (w_1, w_2, \ldots, w_m)) = \big|\{i \in \{1,2,\ldots,m\} \mid v_i \neq w_i\}\big|$.

Ein beispielhafter Hyperwürfelgraph ist in Abbildung 2.6 zu sehen.

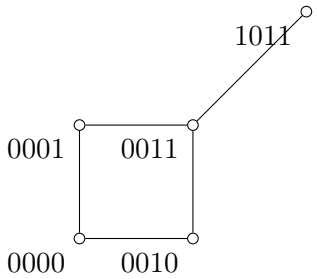


$G_6 = H_4$

Abbildung 2.6: Der 4-dimensionale Hyperwürfelgraph

Definition 2.1.8. Ein **kubischer Graph** ist ein induzierter Teilgraph des Hyperwürfelgraphen H_m für ein $m \in \mathbb{Z}_{>0}$.

Ein beispielhafter kubischer Graph ist in Abbildung 2.7 zu sehen.



$G_7 = (\{0000, 0001, 0010, 0011, 1011\}, E_7)$ induziert in H_4

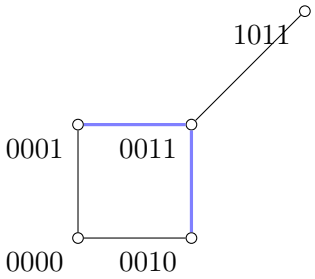
Abbildung 2.7: Ein kubischer Graph

Anmerkung. Ein Zusammenhang von Gittergraphen und kubischen Graphen wird in Kapitel 4 erläutert.

Zuletzt halten wir in den Definitionen 2.1.9-2.1.12 die Bedeutungen der Begriffe "Hamiltonweg" und "Hamiltonkreis" fest, die vermutlich auch bekannt sind.

Definition 2.1.9. Ein **elementarer Weg** in einem Graphen $G = (V, E)$ von v_0 nach v_n ist eine Folge von Knoten $(v_0, v_1, \ldots, v_n)$ für ein $n \in \mathbb{Z}_{\geq 0}$, bei der für alle $i, j \in \{0, 1, \ldots, n\}$ mit $i \neq j$ $v_i \neq v_j$ gilt und für alle $k \in \{0, 1, \ldots, n-1\}$ $\{v_k, v_{k+1}\} \in E$ gilt. Diese Zahl n wird als die **Länge** des Wegs bezeichnet.

Ein beispielhafter elementarer Weg ist in Abbildung 2.8 zu sehen.

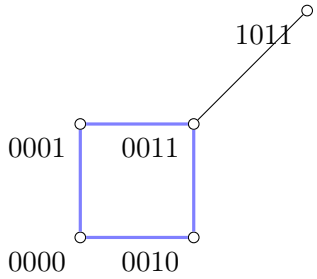


$p_1 = (0001, 0011, 0010)$

Abbildung 2.8: Ein elementarer Weg in G_7

Definition 2.1.10. Ein **elementarer Kreis** in einem Graphen $G = (V, E)$ ist eine Folge von Knoten $(v_0, v_1, \ldots, v_n)$ für ein $n \in \mathbb{Z}_{>2}$, bei der $(v_0, v_1, \ldots, v_{n-1})$ ein elementarer Weg ist, $\{v_{n-1}, v_n\} \in E$ ist und $v_0 = v_n$ ist. Diese Zahl n wird als die **Länge** des Kreises bezeichnet.

Beim Ablaufen eines elementaren Kreises wird keine Kante mehrfach besucht. Ein beispielhafter elementarer Kreis ist in Abbildung 2.9 zu sehen.



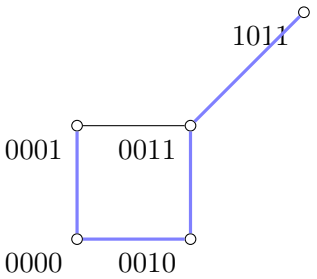
$$c_1 = (0001, 0011, 0010, 0000)$$

Abbildung 2.9: Ein elementarer Kreis in G_7

Definition 2.1.11. Ein **Hamiltonweg** in einem Graphen $G = (V, E)$ ist ein elementarer Weg, der alle Knoten von G enthält.

Anmerkung. Die Länge n eines Hamiltonwegs ist also gleich $|V| - 1$.

Ein beispielhafter Hamiltonweg ist in Abbildung 2.10 zu sehen.



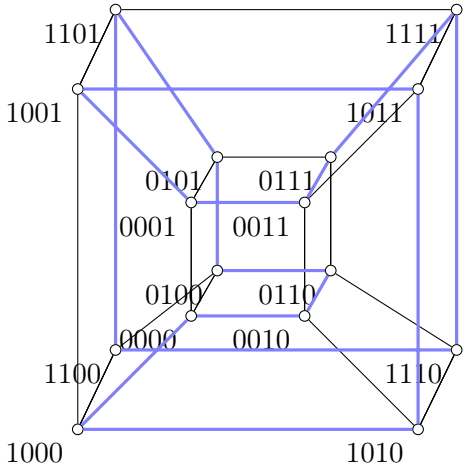
$$p_2 = (0001, 0000, 0010, 0011, 1011)$$

Abbildung 2.10: Ein Hamiltonweg in G_7

Definition 2.1.12. Ein **Hamiltonkreis** in einem Graphen $G = (V, E)$ ist ein elementarer Kreis, der alle Knoten von G enthält.

Anmerkung. Die Länge n eines Hamiltonkreises ist also gleich $|V|$.

Ein beispielhafter Hamiltonkreis ist in Abbildung 2.11 zu sehen.



$c_2 = (0000, 0010, 0110, 0100, 0101, 1101, 1100, 1110,$
$1111, 0111, 0011, 0001, 1001, 1011, 1010, 1000, 0000)$

Abbildung 2.11: Ein Hamiltonkreis in H_4

2.2 NP-Vollständigkeit

In diesem Abschnitt geht es um die komplexitätstheoretischen Grundlagen, die wir im Weiteren brauchen werden. Die Definitionen sind aus [MV20] übernommen und ggf. angepasst.

Die Definitionen 2.2.1-2.2.13 dienen alle dem Zweck, den Begriff der NP-Vollständigkeit festzuhalten.

Definition 2.2.1. Eine **deterministische Turingmaschine** oder auch **DTM** ist ein Tupel $M = (Z, \Gamma, \delta, z_0, A, V)$, das folgende Bestandteile hat:

- Z: Die Menge der Zustände
- Γ: Die Menge der Bandsymbole
- $\delta\colon Z \times \Gamma \to Z \times \Gamma \times \{L, R, N\}$: Die Übergangsfunktion
- $z_0 \in Z$: Der Startzustand
- $A \subseteq Z$: Die Menge der akzeptierenden Zustände
- $V = Z \setminus A$: Die Menge der verwerfenden Zustände

Sie **akzeptiert** eine Eingabe genau dann, wenn die Folge der δ-Übergänge zu einem $z \in A$ führt.

Definition 2.2.2. Eine **nichtdeterministische Turingmaschine** oder auch **NTM** ist ein Tupel $M = (Z, \Gamma, \delta, z_0, A, V)$, das folgende Bestandteile hat:

- Z: Die Menge der Zustände
- Γ: Die Menge der Bandsymbole
- $\delta\colon Z \times \Gamma \to \mathcal{P}(Z \times \Gamma \times \{L, R, N\})$: Die Übergangsfunktion
- $z_0 \in Z$: Der Startzustand
- $A \subseteq Z$: Die Menge der akzeptierenden Zustände
- $V = Z \setminus A$: Die Menge der verwerfenden Zustände

Sie **akzeptiert** eine Eingabe genau dann, wenn es eine Folge von δ-Übergängen gibt, die zu einem $z \in A$ führt.

Definition 2.2.3. Es sei $n \in \mathbb{Z}_{>0}$. Eine **Mehrband-Turingmaschine** mit n Bändern ist eine Turingmaschine, bei der die Übergangsfunktion wie folgt aussieht:

- DTM: $\delta\colon Z \times \Gamma^n \to Z \times \Gamma^n \times \{L, R, N\}^n$
- NTM: $\delta\colon Z \times \Gamma^n \to \mathcal{P}(Z \times \Gamma^n \times \{L, R, N\}^n)$

Ein Übergang hängt also bei einer Mehrband-Turingmaschine vom Zustand und von den n Bandsymbolen, die auf den n Bändern gelesen werden, ab. Bei einem solchen Übergang schreibt die Mehrband-Turingmaschine auf jedem der n Bänder ein neues Symbol und bewegt sich dann unabhängig von den anderen Bändern möglicherweise nach links oder rechts.

Definition 2.2.4. Eine Turingmaschine M **entscheidet** eine Sprache L genau dann, wenn die Menge der Wörter, die sie akzeptiert, gleich L ist und sie bei jeder möglichen Eingabe hält.

Definition 2.2.5. Es sei M eine Turingmaschine und $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ eine Funktion. M **arbeitet in Zeit** f genau dann, wenn für alle $n \in \mathbb{Z}_{\geq 0}$ und alle Wörter w der Länge n die Laufzeit von M bei Eingabe w kleiner oder gleich $f(n)$ ist.

Definition 2.2.6. Es sei M eine Turingmaschine. M **arbeitet in Polynomialzeit** genau dann, wenn es ein Polynom p gibt, sodass M in Zeit p arbeitet.

Definition 2.2.7. Es sei $t\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ eine Funktion. Die Komplexitätsklasse $\mathbf{NTIME}(t)$ ist die Menge aller Sprachen A, für die es eine Mehrband-NTM gibt, die A entscheidet und in Zeit $O(t)$ arbeitet.

Definition 2.2.8. NP := NTIME($n^{O(1)}$).

Definition 2.2.9. Es seien $A \subseteq \Sigma^*$, $B \subseteq \Delta^*$ Sprachen. A ist ~~genau dann~~ auf B **in Polynomialzeit** m**-reduzierbar**, wenn es eine Funktion $f\colon \Sigma^* \to \Delta^*$ mit folgenden Eigenschaften gibt:

- Es gibt eine DTM M, die in Polynomialzeit arbeitet und bei Eingabe eines Wortes $x \in \Sigma^*$ das Wort $f(x) \in \Delta^*$ ausgibt.
- Für alle $x \in \Sigma^*$ gilt: $x \in A$ genau dann, wenn $f(x) \in B$ ist.

Dies wird auch als $A \leq_m^P B$ geschrieben.

Lemma 2.2.10. *Die m-Reduzierbarkeit in Polynomialzeit ist transitiv.*

Beweis. Es seien A, B und C Sprachen, für die $A \leq_m^P B$ und $B \leq_m^P C$ gilt. Dann gibt es eine Reduktionsfunktion f von A nach B und eine Reduktionsfunktion g von B nach C, die beide in Polynomialzeit berechenbar sind. Die Funktion $f \circ g$ ist eine Reduktionsfunktion von A nach C, die daher auch in Polynomialzeit arbeitet. Die Korrektheit dieser Reduktionsfunktion folgt direkt aus der Korrektheit von f und g. Es gilt also $A \leq_m^P C$. □

Definition 2.2.11. Eine Sprache L ist genau dann **NP-schwer**, wenn für alle $A \in$ NP gilt, dass $A \leq_m^P L$ ist.

Die Aussage des folgenden Satzes werden wir an einigen Stellen verwenden, um die NP-Schwere verschiedener Probleme zu zeigen.

Satz 2.2.12. *Es seien B und C Sprachen, für die gilt, dass B NP-schwer und $B \leq_m^P C$ ist. Dann ist C auch NP-schwer.*

Beweis. Es sei $A \in$ NP eine beliebige Sprache. Da B NP-schwer ist, gilt $A \leq_m^P B$. Aus Lemma 2.2.10 folgt, dass auch $A \leq_m^P C$ gilt. Weil A aber beliebig aus NP gewählt ist, heißt dies, dass alle Sprachen in NP in Polynomialzeit auf C m-reduzierbar sind. C ist also NP-schwer. □

Definition 2.2.13. Eine Sprache L ist genau dann **NP-vollständig**, wenn L NP-schwer und $L \in$ NP ist.

2.3 Gruppen

In diesem Abschnitt geht es um die gruppentheoretischen Grundlagen, die wir im Weiteren brauchen werden. Die Definitionen sind aus [Bos20] übernommen und ggf. angepasst.

Die Definitionen 2.3.1-2.3.4 bieten einen kleinen Einblick in die Gruppentheorie, die nicht unbedingt Teil des Informatikstudiums ist. Dieser Einblick reicht aber dennoch aus, um mit den gruppentheoretischen Entscheidungsproblemen zu arbeiten, die wir in Abschnitt 3.4 definieren werden.

Definition 2.3.1. Eine **Gruppe** ist eine Menge G mit einer dazugehörigen Verknüpfung $\circ\colon G \times G \to G, (a, b) \mapsto a \circ b$, die folgende Axiome erfüllt:

- Assoziativität: Für alle $a, b, c \in G$ gilt

$$(a \circ b) \circ c = a \circ (b \circ c).$$

- Existenz eines Einselements: Es existiert ein Einselement $1 \in G$, sodass für alle $a \in G$

$$1 \circ a = a = a \circ 1$$

gilt.

- Existenz eines Inversen: Für alle $a \in G$ existiert ein $a^{-1} \in G$, sodass

$$a \circ a^{-1} = 1 = a^{-1} \circ a$$

gilt.

Lemma 2.3.2. *Für eine Gruppe G und zwei Elemente $a, b \in G$ gilt*

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Beweis. $(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ 1 \circ a^{-1} = a \circ a^{-1} = 1.$ □

Anmerkung. Analog dazu gilt auch für ein Produkt von endlich vielen Elementen einer Gruppe, dass sein Inverses gleich dem Produkt der Inversen der einzelnen Elemente in umgekehrter Reihenfolge ist. Diese Eigenschaft, die leicht durch Induktion gezeigt werden kann, werden wir im Weiteren an einigen Stellen verwenden.

Definition 2.3.3. Ein **Erzeugendensystem** einer Gruppe G ist eine Teilmenge $E \subseteq G$ mit der Eigenschaft, dass sich alle Elemente in G als endliche Produkte der Elemente in E und ihrer Inversen darstellen lassen. Die Gruppe G wird von E **erzeugt**.

Definition 2.3.4. Eine **Operation** einer Gruppe G auf einer Menge X ist eine Abbildung $\circ\colon G \times X \to X, (g, x) \mapsto g \circ x$, die folgende Bedingungen erfüllt:

- Für alle $x \in X$ gilt $1 \circ x = x$.
- Für alle $g, h \in G$ und für alle $x \in X$ gilt $(g \circ h) \circ x = g \circ (h \circ x)$.

Kapitel 3

Die Rubik's Cube- und Rubik's Square-Probleme

Der Begriff Rubik's Cube bezeichnet üblicherweise ein Drehpuzzle, bei dem es darum geht, durch Drehungen einzelner Schichten eines $3 \times 3 \times 3$ Würfels gleichfarbige Aufkleber auf der Außenseite jeweils auf dieselbe Seite zu bringen. Hier verwenden wir den Begriff mit der Verallgemeinerung, dass ein $n \times n \times n$ Rubik's Cube für ein $n \in \mathbb{Z}_{>0}$ einen entsprechenden $n \times n \times n$ Würfel bezeichnet. Ein Zug bewegt jeweils eine $1 \times n \times n$ (bzw. $n \times 1 \times n$ bzw. $n \times n \times 1$) Schicht. Außerdem betrachten wir ein einfacheres Drehpuzzle in Form eines $n \times n \times 1$ Quaders, das wir als $n \times n$ Rubik's Square bezeichnen. Hier bewegt ein Zug jeweils eine $n \times 1 \times 1$ Zeile oder eine $1 \times n \times 1$ Spalte.

3.1 Der Rubik's Square

Ein Rubik's Square besteht aus $n \times n$ Einheitswürfeln, die wir hier als Würfelchen bezeichnen. Auf jeder Fläche eines solchen Würfelchens, die sich auf der Außenseite des Rubik's Square befindet, ist ein Aufkleber in einer von sechs Farben (Weiß, Gelb, Rot, Blau, Orange, Grün). Das Ziel des Puzzles ist es durch eine Folge von Zügen die Würfelchen so anzuordnen, dass die Aufkleber auf jeder Seite des Rubik's Square jeweils einfarbig sind. Ein Zug ist eine Rotation einer Zeile oder Spalte um 180° wie in Abbildung 3.1 dargestellt.

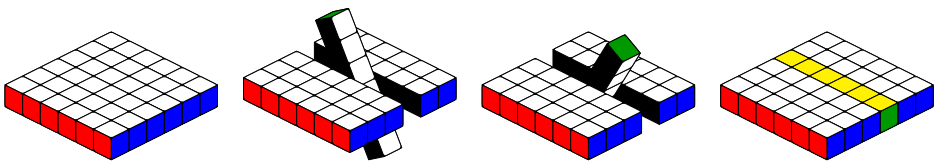


Abbildung 3.1: Ein Zug eines 6×6 Rubik's Square

Dazu definieren wir das folgende Entscheidungsproblem:

Definition 3.1.1. Das Entscheidungsproblem RUBIK'S SQUARE ist wie folgt definiert:

RS := $\{\langle C, k\rangle \mid C$ ist eine Konfiguration eines $n \times n$ Rubik's Square für ein $n \in \mathbb{Z}_{>0}$, die in maximal $k \in \mathbb{Z}_{\geq 0}$ Zügen gelöst werden kann.$\}$

3.2 Der Rubik's Cube

Ein Rubik's Cube besteht aus $n \times n \times n$ Einheitswürfeln, die wir hier als Würfelchen bezeichnen. Auf jeder Fläche eines solchen Würfelchens, die sich auf der Außenseite des Rubik's Cube befindet, ist ein Aufkleber in einer von sechs Farben (Weiß, Gelb, Rot, Blau, Orange, Grün). Das Ziel des Puzzles ist es, genau wie beim Rubik's Square, durch eine Folge von Zügen die Würfelchen so anzuordnen, dass die Aufkleber auf jeder Seite des Rubik's Cube jeweils einfarbig sind. Es gibt für den Rubik's Cube verschiedene Definitionen von Zügen. Solche Definitionen von Zügen werden als Zugmetriken bezeichnet. Wir betrachten zwei der am weitesten verbreiteten Zugmetriken, die sich für $n > 3$ generalisieren lassen. In der Slice Turn Metric (STM) ist eine Rotation einer Schicht um ein Vielfaches von 90° ein Zug. In der Slice Quarter Turn Metric (SQTM) ist eine Rotation einer Schicht um 90° in eine der beiden Richtungen ein Zug. Ein beispielhafter SQTM-Zug ist in Abbildung 3.2 dargestellt.

Dazu definieren wir die folgenden Entscheidungsprobleme:

Definition 3.2.1. Das Entscheidungsproblem STM RUBIK'S CUBE ist wie folgt definiert:

STMRC := $\{\langle C, k\rangle \mid C$ ist eine Konfiguration eines $n \times n \times n$ Rubik's Cube für ein $n \in \mathbb{Z}_{>0}$, die in maximal $k \in \mathbb{Z}_{\geq 0}$ STM-Zügen gelöst werden kann.$\}$

Definition 3.2.2. Das Entscheidungsproblem SQTM RUBIK'S CUBE ist wie folgt definiert:

SQTMRC := $\{\langle C, k\rangle \mid C$ ist eine Konfiguration eines $n \times n \times n$ Rubik's Cube für ein $n \in \mathbb{Z}_{>0}$, die in maximal $k \in \mathbb{Z}_{\geq 0}$ SQTM-Zügen gelöst werden kann.$\}$

Weil jeder SQTM-Zug auch ein STM-Zug ist, aber nicht jeder STM-Zug auch ein SQTM-Zug ist, ist es zuerst einmal nicht offensichtlich, dass diese beiden Probleme die gleiche Schwere haben. Daher werden wir uns mit beiden Problemen beschäftigen, um letztendlich zu zeigen, dass dies tatsächlich der Fall ist. Daraus lässt sich die Intuition gewinnen, dass die Schwere der Probleme mehr von dem Drehpuzzle abhängt als von einer speziellen Metrik. Dass die entsprechenden Probleme für andere denkbare Metriken auch NP-vollständig sind, wurde allerdings noch nicht gezeigt.

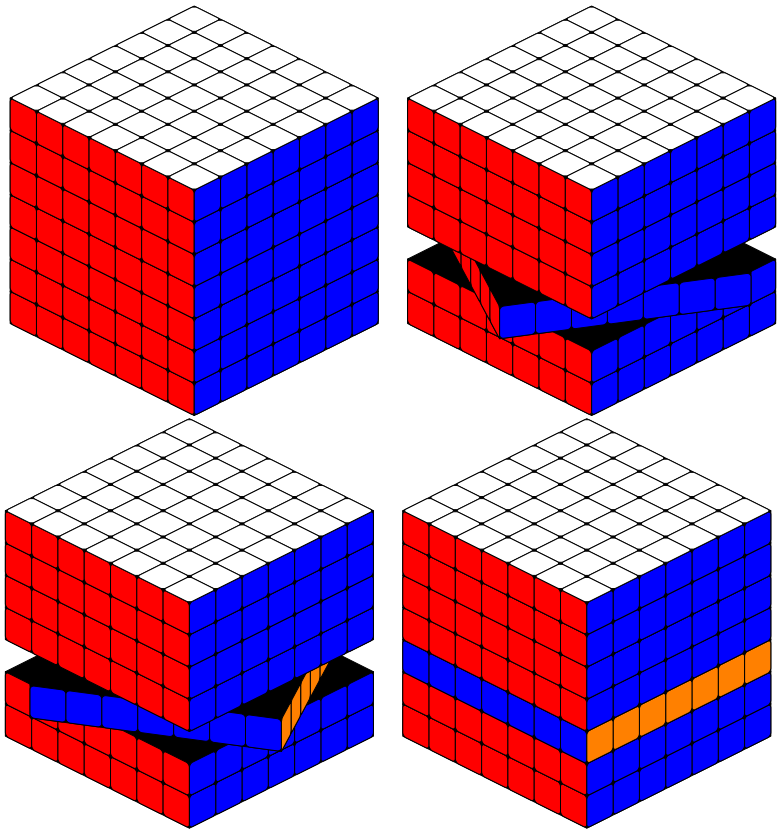


Abbildung 3.2: Ein Zug eines $7 \times 7 \times 7$ Rubik's Cube

3.3 Nomenklatur

Zuerst legen wir fest, wie wir einzelne Würfelchen und einzelne Aufkleber identifizieren. Für die Würfelchen des Rubik's Square reicht es aus, die x- und y-Koordinaten anzugeben, bei dem Rubik's Cube müssen hingegen die x-, y- und z-Koordinaten angegeben werden, um ein einzelnes Würfelchen eindeutig zu identifizieren. Um einen Aufkleber zu identifizieren, geben wir die Seite des Drehpuzzles, auf der sich der Aufkleber befindet (z. B. "$+x$"), und die verbleibenden Koordinaten in die anderen Richtungen (z. B. die y- und z-Koordinaten für einen Aufkleber auf der $+x$-Seite eines Rubik's Cube) an.

Wenn $n = 2a+1$ ungerade ist, lassen wir die Koordinaten über die Menge $\{-a, -a+1, \ldots, a-1, a\}$ laufen. Wenn $n = 2a$ stattdessen gerade ist, lassen wir die Koordinaten über die Menge $\{-a, -a+1, \ldots, a-1, a\} \setminus \{0\}$ laufen. Dadurch ist gewährleistet, dass die Koordinaten nur ganze Zahlen annehmen und dass sich die Koordinaten von Würfelchen und Aufklebern bei einem Zug (oder auch einer beliebigen Folge von Zügen) nur durch die Permutation der Komponenten und Negation einzelner Komponenten ändern.

Bei dem Rubik's Square bezeichnen wir Züge, die eine Spalte bewegen, als x-Züge und Züge, die eine Zeile bewegen, als y-Züge. Bei einem x-Zug sind alle Würfelchen betroffen, die sich eine bestimmte x-Koordinate teilen. Den Betrag dieser Koordinate bezeichnen wir als Index des Zugs. Bei y-Zügen bezeichnen wir entsprechend den Betrag der y-Koordinate als Index. Jeder Zug lässt sich dann eindeutig durch die Angabe, ob es ein x- oder y-Zug ist, das Vorzeichen und den Index identifizieren. Z. B. bewegt ein negativer x-Zug mit Index 3 oder auch $-x$-Zug mit Index 3 oder auch $x = -3$-Zug alle Würfelchen, deren x-Koordinate gleich -3 ist.

Analog dazu haben bei einem STM- oder SQTM-Zug eines Rubik's Cube alle betroffenen Würfelchen eine gemeinsame Koordinate. Wenn dies eine x-Koordinate (bzw. y-Koordinate bzw. z-Koordinate) ist, bezeichnen wir die Würfelchen zusammen als x-Schicht (bzw. y-Schicht bzw. z-Schicht). Hier bezeichnen wir den Betrag der gemeinsamen Koordinate als Index und nennen das Vorzeichen getrennt. Dadurch lassen sich alle Schichten eindeutig identifizieren (z. B. die positive y-Schicht mit Index 2 oder auch die $+y$-Schicht mit Index 2 oder auch $y = 2$-Schicht). Wir bezeichnen die Schichten an den sechs Außenseiten des Würfels auch als Außenschichten (z. B. die $+z$-Außenschicht).

Um einen Zug eines Rubik's Cube eindeutig zu identifizieren, müssen zusätzlich zu der Schicht noch die Drehrichtung und der Drehwinkel angegeben werden. Dadurch, dass wir zur Identifikation von Zügen fünf Teilinformationen (gemeinsame Koordinate, Betrag der Koordinate, Index, Drehrichtung und Drehwinkel) haben, können wir außerdem interessante Mengen von Zügen betrachten, indem wir nicht alle fünf angeben. Wie bei den Schichten bezeichnen wir z. B. einen positiven x-Zug auch als $+x$-Zug. Einen Zug, der eine Außenseite bewegt, nennen wir Außenseitenzug. Diese Konventionen übertragen wir auch auf den Rubik's Square.

Einen Zug mit einem Drehwinkel von 90° bezeichnen wir als Drehung und einen Zug mit einem Drehwinkel von 180° bezeichnen wir als Wendung. Bei Drehungen geben wir die Drehrichtung als im Uhrzeigersinn oder gegen den Uhrzeigersinn an. Dazu legen wir fest, dass die Richtung einer x-Drehung (bzw. y-Drehung bzw. z-Drehung) von positiver x-Richtung (bzw. y-Richtung bzw. z-Richtung) aus betrachtet wird. Bei Wendungen ist es nicht notwendig, die Drehrichtung anzugeben, weil das Resultat davon unabhängig ist.

3.4 Der gruppentheoretische Ansatz

Wir definieren RS_n als die Gruppe der Permutationen der Aufkleber des $n \times n$ Rubik's Square, die durch Zugfolgen vom gelösten Zustand aus erreichbar sind, und RC_n als die Gruppe der Permutationen der Aufkleber des $n \times n \times n$ Rubik's Cube, die durch Zugfolgen vom gelösten Zustand aus

erreichbar sind. Die dazugehörige Verknüpfung ist jeweils die Komposition der Permutationen.

Hierbei handelt es sich um Gruppen, weil die Komposition von Permutationen assoziativ ist, es jeweils ein Einselement gibt, nämlich die Permutation, bei der alle Aufkleber an ihrem Platz bleiben, und alle Permutationen ein Inverses haben, weil sich die dazugehörige Zugfolge umkehren lässt.

Anmerkung. Es ist zu beachten, dass RS_n für jedes $n \in \mathbb{Z}_{>0}$ eine Gruppe ist, während RS ein Entscheidungsproblem ist.

Jeder einzelne Zug des $n \times n$ Rubik's Square bzw. $n \times n \times n$ Rubik's Cube permutiert die Aufkleber und entspricht damit einem Element in RS_n bzw. RC_n.

Für den Rubik's Square sei $x_i \in RS_n$ die Permutation, die einer Wendung der Spalte mit x-Koordinate i entspricht, und $y_i \in RS_n$ die Permutation, die einer Wendung der Zeile mit y-Koordinate i entspricht. Weil alle Permutationen in RS_n in einer endlichen Anzahl an Zügen lösbar und damit auch erreichbar sind, ist $\bigcup_{i \in I} \{x_i, y_i\}$ ein Erzeugendensystem von RS_n, wobei $I \subset \mathbb{Z}$ die Menge der möglichen Indizes ist.

Für den Rubik's Cube sei analog dazu $x_i \in RC_n$ bzw. $y_i \in RC_n$ bzw. $z_i \in RC_n$ die Permutationen, die einer Drehung der Schicht mit x-Koordinate bzw. y-Koordinate bzw. z-Koordinate i im Uhrzeigersinn entspricht. $\bigcup_{i \in I} \{x_i, y_i, z_i\}$ ist ein Erzeugendensystem von RC_n, wobei $I \subset \mathbb{Z}$ die Menge der möglichen Indizes ist.

Außerdem definieren wir RSC_n als Menge der lösbaren Konfigurationen des $n \times n$ Rubik's Square und RCC_n als Menge der lösbaren Konfigurationen des $n \times n \times n$ Rubik's Cube. Dabei seien $C_0 \in RSC_n$ bzw. $C_0 \in RCC_n$ die gelösten Konfigurationen des Rubik's Square bzw. Rubik's Cube. In den gelösten Konfigurationen sind die Aufkleber wie folgt angeordnet: Die $-x$-Außenseite ist grün, die $+x$-Außenseite ist blau, die $-y$-Außenseite ist orange, die $+y$-Außenseite ist rot, die $-z$-Außenseite (oder auch Oberseite) ist weiß und die $+z$-Außenseite (oder auch Unterseite) ist gelb. Wir können nun die Gruppen RS_n bzw. RC_n auf den jeweiligen Mengen RSC_n bzw. RCC_n operieren lassen, indem wir sie die Würfelchen so umordnen lassen, dass sich die Positionen der Aufkleber entsprechend der Permutationen verändern. Dadurch können wir jeder Permutation aus RS_n bzw. RC_n eine Konfiguration aus RSC_n bzw. RCC_n zuordnen, indem wir die Permutation auf die gelöste Konfiguration anwenden. Für jede Permutation $t \in RS_n$ oder $t \in RC_n$ benennen wir die zugeordnete Konfiguration $C_t := t \circ C_0$.

Es ist zu beachten, dass das Farbschema hier von den in [DER17] verwendeten Farbschemata abweicht. Diese Änderung hat den Sinn, dass wir hier für den Rubik's Square und den Rubik's Cube dasselbe Farbschema statt zweier unterschiedlicher verwenden.

Mit diesem neuen Ansatz definieren wir nun folgende Probleme:

Definition 3.4.1. Das Entscheidungsproblem GROUP RUBIK'S SQUARE ist wie folgt definiert:

GRS := $\{\langle t, k\rangle \mid t \in RS_n$ für ein $n \in \mathbb{Z}_{>0}$ und t^{-1} lässt sich als ein Produkt von höchstens $k \in \mathbb{Z}_{\geq 0}$ Permutationen aus RS_n darstellen, die jeweils einzelnen Zügen entsprechen.$\}$

Definition 3.4.2. Das Entscheidungsproblem GROUP STM RUBIK'S CUBE ist wie folgt definiert:

GSTMRC := $\{\langle t, k\rangle \mid t \in RC_n$ für ein $n \in \mathbb{Z}_{>0}$ und t^{-1} lässt sich als ein Produkt von höchstens $k \in \mathbb{Z}_{\geq 0}$ Permutationen aus RC_n darstellen, die jeweils einzelnen STM-Zügen entsprechen.$\}$

Definition 3.4.3. Das Entscheidungsproblem GROUP SQTM RUBIK'S CUBE ist wie folgt definiert:

GSQTMRC := $\{\langle t, k\rangle \mid t \in RC_n$ für ein $n \in \mathbb{Z}_{>0}$ und t^{-1} lässt sich als ein Produkt von höchstens $k \in \mathbb{Z}_{\geq 0}$ Permutationen aus RC_n darstellen, die jeweils einzelnen SQTM-Zügen entsprechen.$\}$

Diese Probleme sind den Rubik's Square- und Rubik's Cube-Problemen sehr ähnlich. Der Unterschied besteht darin, dass die gruppentheoretischen Probleme eine Lösung (in einer gewissen Anzahl an Zügen) fordern, bei der alle Aufkleber an ihren ursprünglichen Platz zurückkehren, während die vorherigen Probleme nur fordern, dass die Außenseiten einfarbig sind. Die gruppentheoretischen Probleme können als schwierigere Varianten angesehen werden. Die strengeren Anforderungen können auch praktische Anwendungen haben, da sie zum Beispiel Puzzles, bei denen die Aufkleber mit Bildern bedruckt sind, besser beschreiben.

Wir formalisieren die Beobachtung, dass die gruppentheoretischen Probleme schwieriger sind, wie folgt:

Lemma 3.4.4. *Wenn $\langle t, k\rangle \in GRS$ ist, dann ist $\langle C_t, k\rangle \in RS$.*

Beweis. Wenn $\langle t, k\rangle \in$ GRS ist, dann lässt sich t^{-1} als ein Produkt von höchstens k Permutationen aus RS_n darstellen, die jeweils einzelnen Zügen entsprechen. Das Anwenden dieser Züge auf C_t liefert daher

$$t^{-1} \circ C_t = t^{-1} \circ t \circ C_0 = 1 \circ C_0 = C_0.$$

Es ist also möglich, C_t in höchstens k Zügen zu lösen und damit ist $\langle C_t, k\rangle \in$ RS. □

Lemma 3.4.5. *Wenn $\langle t, k\rangle \in GSTMRC$ bzw. $GSQTMRC$ ist, dann ist $\langle C_t, k\rangle \in STMRC$ bzw. $SQTMRC$.*

Beweis. Der Beweis verläuft analog zum Beweis für den Rubik's Square. □

An dieser Stelle ist noch anzumerken, dass das Lösen von Rubik's Cube nach der SQTM schwieriger als nach der STM ist, wie wir in folgendem Lemma festhalten:

Lemma 3.4.6. *Wenn $\langle C, k\rangle \in SQTMRC$ ist, dann ist $\langle C, k\rangle \in STMRC$. Wenn $\langle t, k\rangle \in GSQTMRC$ ist, dann ist $\langle t, k\rangle \in GSTMRC$.*

Beweis. Jeder SQTM-Zug ist auch ein legaler STM-Zug. Wenn eine Konfiguration C in höchstens k SQTM-Zügen gelöst werden kann, kann sie auch in höchstens k STM-Zügen gelöst werden. Ebenso kann eine Permutation t mit höchstens k Permutationen, die jeweils einzelnen STM-Zügen entsprechen, invertiert werden, wenn sie mit höchstens k Permutationen, die jeweils einzelnen SQTM-Zügen entsprechen, invertiert werden kann. □

3.5 Mitgliedschaft in NP

Satz 3.5.1. *Die Probleme RS, STMRC, SQTMRC, GRS, GSTMRC und GSQTMRC liegen in NP.*

Beweis. In [Dem+11] wurde gezeigt, dass die Gotteszahl (auch God's Number, maximale Länge einer optimalen Lösung) von $n \times n$ Rubik's Square und von $n \times n \times n$ Rubik's Cube mit einer Funktion in $\Theta\left(\frac{n^2}{\log n}\right)$ wächst. Daraus folgt, dass es ein Polynom $p(n)$ gibt, sodass jede Konfiguration bzw. jede Permutation in RSn_n oder RC_n in höchstens $p(n)$ Zügen (nach der jeweilige Metrik) gelöst werden kann.

Daher können wir einen nichtdeterministischen Algorithmus für die Probleme angeben. Die Eingabe besteht bei den sechs Problemen aus einer Startkonfiguration oder einer Permutation und einem k. Der Algorithmus führt nun nichtdeterministisch bis zu $\min\{k, p(n)\}$ Züge aus und überprüft, ob die Zugfolge die Konfiguration bzw. die Permutation löst.

Wenn ein Ausführungszweig einen akzeptierenden Zustand annimmt, dann gibt es eine Lösung mit höchstens k Zügen und dann ist die Eingabe eine "Ja"-Instanz des Problems. Wenn umgekehrt die Eingabe eine "Ja"-Instanz des Problems ist, dann gibt es eine Folge von Zügen mit einer Länge bis zu k und bis zu $p(n)$, weil jede Permutation in höchstens $p(n)$ Zügen gelöst werden kann. Daher gibt es auch einen Ausführungszweig, der einen akzeptierenden Zustand erreicht. Der Algorithmus für jedes der Probleme ist also korrekt und seine Laufzeit ist durch ein Polynom beschränkt. Daraus folgt, dass die Probleme in NP liegen. □

Kapitel 4

Hamiltonkreise und Hamiltonwege

Um die NP-Schwere der in Kapitel 3 eingeführten Probleme zu zeigen, müssen wir uns zunächst mit einigen graphentheoretischen Problemen befassen. Hierbei ist zu beachten, dass in [DER17] Promise-Probleme verwendet wurden. Weil dies aber noch weitere Definitionen benötigt, verwenden wir hier stattdessen gewöhnliche Entscheidungsprobleme. Um trotzdem in den Reduktionen die Anzahl der Fallunterscheidungen gering zu halten, gehen wir davon aus, dass am Anfang von Reduktionsfunktionen jeweils ein Parser in Polynomialzeit triviale "Nein"-Instanzen erkennt und auf eine festgelegte "Nein"-Instanz abbildet, bevor der beschriebene Algorithmus die anderen Instanzen behandelt.

Definition 4.0.1. GRID GRAPH HAMILTONIAN CYCLE

GGHamCyc := $\{\langle G \rangle \mid G$ ist ein Gittergraph, der keine Knoten, von denen genau eine Kante ausgeht, und der einen Hamiltonkreis enthält.$\}$

Satz 4.0.2. *GGHamCyc ist NP-vollständig.*

Beweis. Der Satz wurde in [IPS82] bewiesen. □

Wir werden diesen Satz verwenden, um die NP-Schwere von folgendem Problem zu beweisen.

Definition 4.0.3. GRID GRAPH HAMILTONIAN PATH

GGHamPath := $\{\langle G, s, t \rangle \mid G = (V, E)$ ist ein Gittergraph, der keine Knoten, von denen genau eine Kante ausgeht, und der einen Hamiltonweg von $s \in V$ nach $t \in V$ enthält.$\}$

Weil es nicht einfach ist, Gittergraphen mit Rubik's Square oder Rubik's Cube in Verbindung zu bringen, benutzen wir kubische Graphen als Zwischenschritt. Kubische Graphen lassen sich leichter mit Rubik's Square und Rubik's Cube in Verbindung bringen. Zusätzlich lassen sich alle Gittergraphen in entsprechende kubische Graphen überführen.

Definition 4.0.4. CUBICAL HAMILTONIAN PATH

CHamPath := $\{\langle l_1, l_2, \ldots, l_n\rangle \mid l_1, l_2, \ldots l_n$ sind Bitstrings der Länge $m \in \mathbb{Z}_{>0}$, $l_n = 00...0$ und der kubische Graph $G = (V, E)$ mit $G = \{l_1, l_2, \ldots, l_n\}$ enthält einen Hamiltonweg von l_1 nach $l_n\}$

Anmerkung. Die Frage, ob es einen solchen Hamiltonweg gibt, ist identisch zu der Frage, ob sich die Bitstrings so umordnen lassen, dass jeder einen Hamming-Abstand von 1 zum nächsten hat. Dies liegt daran, dass Bitstringpaare mit einem Hamming-Abstand von 1 genau den Kanten im kubischen Graph entsprechen.

Im Rest dieses Kapitels beweisen wir die NP-Schwere dieser beiden Probleme.

4.1 NP-Schwere von GGHamPath

Zuerst reduzieren wir das Entscheidungsproblem GGHamCyc, von dem wir jetzt wissen, dass es NP-schwer ist, auf GGHamPath, um zu zeigen, dass auch GGHamPath NP-schwer ist.

Lemma 4.1.1. *GGHamPath ist NP-schwer.*

Beweis. Es ist zu beachten, dass dieser Beweis dadurch, dass die Probleme hier ohne Promise definiert sind, im Vergleich zu dem Beweis in [DER17] etwas einfacher ist.

Es sei $\langle G\rangle$ eine Instanz des Problems GGHamCyc. Außerdem sei v der linkeste Knoten in der obersten Reihe von Knoten in G. Wenn dieser Knoten weniger als zwei Nachbarknoten hat, kann der Graph keinen Hamiltonkreis enthalten. Unsere Reduktionsfunktion bildet diesen Graph auf eine feste "Nein"-Instanz von GGHamPath ab. Ansonsten muss v einen Nachbarknoten unter sich und einen rechts von sich haben, weil links und oben von v keine Knoten sind und von v mindestens zwei Kanten ausgehen. Es sei v' dieser rechte Nachbarknoten. Dann bildet unsere Reduktionsfunktion $\langle G\rangle$ auf $\langle G, v, v'\rangle$ ab. Ein Beispiel dazu ist in Abbildung 4.1 zu sehen.

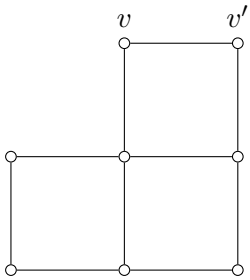


Abbildung 4.1: Ein Gittergraph G mit den beiden Knoten v und v'

Jetzt bleibt noch zu zeigen, dass $\langle G, v, v' \rangle$ genau dann eine "Ja"-Instanz von GGHamPath ist, also G einen Hamiltonweg von v nach v' enthält, wenn $\langle G \rangle$ eine "Ja"-Instanz von GGHamCyc ist, also G einen Hamiltonkreis enthält.

Wenn G einen Hamiltonkreis enthält, dann enthält dieser die Kante von v nach v', weil von v genau 2 Kanten ausgehen und in einem Kreis für jeden Knoten zwei ausgehende Kanten enthalten sind. G enthält also auch einen Hamiltonweg von v nach v', der genau dem Hamiltonkreis ohne diese eine Kante entspricht.

Wenn G hingegen einen Hamiltonweg von v nach v' enthält, dann kann dieser Weg nicht die Kante von v nach v' enthalten, weil er ansonsten die anderen Knoten nicht besuchen würde. Durch Hinzufügen dieser Kante erhalten wir einen Hamiltonkreis in G.

Wir haben also eine Reduktionsfunktion angegeben, die in Polynomialzeit arbeitet. Es gilt also, dass GGHamCyc auf GGHamPath in Polynomialzeit m-reduzierbar ist. Weil zusätzlich GGHamCyc nach Satz 4.0.2 NP-vollständig und damit auch NP-schwer ist, folgt dass GGHamPath NP-schwer ist. □

Anmerkung. Eine ähnliche Reduktion funktioniert für die Probleme HAMPATH und HAMCIRC für allgemeine Graphen nicht, weil es keine offensichtliche Methode für beliebige Graphen, die einen Hamiltonkreis enthalten, gibt, in Polynomialzeit zwei Knoten so zu wählen, dass sie garantiert in diesem Hamiltonkreis direkt aufeinander folgen.

4.2 NP-Schwere von CHamPath

Als nächstes reduzieren wir das Entscheidungsproblem GGHamPath, von dem wir jetzt wissen, dass es NP-schwer ist, auf CHamPath, um zu zeigen, dass auch CHamPath NP-schwer ist.

Lemma 4.2.1. *CHamPath ist NP-schwer.*

Beweis. Es sei $\langle G, s, t \rangle$ eine Instanz des Problems GGHamPath. Außerdem seien m_R die Anzahl der Reihen, m_S die Anzahl der Spalten und n die Anzahl der Knoten in $G = (V, E)$.

Jetzt benennen wir die Reihen von oben nach unten mit folgenden m_R Bitstrings der Länge $m_R - 1$: 000...0, 100...0, 110...0, ..., 111...1. Analog dazu benennen wir die Spalten von links nach rechts mit folgenden m_S Bitstrings der Länge $m_S - 1$: 000...0, 100...0, 110...0, ..., 111...1. Dies nutzen wir, um jedem Knoten einen Bitstring der Länge $m = m_R + m_S - 2$ zuzuweisen, der aus der Konkatenation des Reihenbitstrings und des Spaltenbitstrings besteht.

Daraus folgt, dass die Bitstrings zweier Knoten in G genau dann einen Hamming-Abstand von 1 haben, wenn die Reihenbitstrings gleich

sind und die Spaltenbitstrings einen Hamming-Abstand von 1 haben oder wenn es andersherum ist. Zwei Reihen-/Spaltenbitstrings sind genau dann gleich, wenn sie zur gleichen Reihe/Spalte gehören, und zwei Reihen-/Spaltenbitstrings haben einen Hamming-Abstand von 1 genau dann, wenn die zugehörigen Reihen/Spalten direkt über-/nebeneinander liegen. Daher haben sie einen Hamming-Abstand von 1 genau dann, wenn sie in G benachbart sind.

Wir haben jetzt G als kubischen Graph dargestellt, indem wir jedem Knoten in G einen Bitstring zugewiesen haben. Es seien die Knoten $V = \{v_1, v_2, \ldots, v_n\}$, sodass $v_1 = s$ und $v_n = t$ sind. Für alle $i \in I := \{1, 2, \ldots, n\}$ sie l'_i der dem Knoten v_i zugewiesene Bitstring.

Außerdem definieren wir noch für alle $i \in I$ den Bitstring $l_i := l'_i \oplus l'_n$. Für alle $i, j \in I$ ist der Hamming-Abstand von l_i und l_j der gleiche wie der von l'_i und l'_j. Die Bistrings l_i lassen sich in Polynomialzeit berechnen. Jetzt ist der kubische Graph G' durch die Knotenmenge $\{l_1, l_2, \ldots, l_n\}$ eindeutig bestimmt und isomorph zu G.

Weil die Bitstrings l_i alle die gleiche Länge haben und $l_n = l'_n \oplus l'_n = 00...0$ ist, ist $\langle l_1, l_2, \ldots, l_n \rangle$ genau dann ein "Ja"-Instanz von CHamPath, wenn es einen Hamiltonweg von l_1 nach l_n gibt. Weil G' und G isomorph sind und l_1 dabei s und l_n dabei t entspricht, ist dies genau dann der Fall, wenn G einen Hamiltonweg von s nach t enthält, also wenn $\langle G, s, t \rangle$ eine "Ja"-Instanz von GGHamPath ist. Damit ist die Korrektheit der in diesem Beweis beschriebenen Reduktionsfunktion gezeigt.

Wir haben eine Reduktionsfunktion angegeben, die in Polynomialzeit arbeitet. Es gilt also, dass GGHamPath auf CHamPath in Polynomialzeit m-reduzierbar ist. Weil wir aus Lemma 4.1.1 bereits wissen, dass GGHamPath NP-schwer ist, folgt, dass CHamPath NP-schwer ist. □

Kapitel 5

Die NP-Vollständigkeit der Rubik's-Square-Probleme

5.1 Die Reduktionen

Wir zeigen die NP-Schwere von RS und GRS mittels Reduktion von CHamPath, dessen NP-Schwere wir in Abschnitt 4.2 gezeigt haben.

Die Eingabe ist eine Instanz von CHamPath, die aus n Bitstrings $l_1, l_2, \ldots, l_n$ der Länge m besteht, wobei $l_n = \underbrace{00...0}_{m}$ gilt. Daraus berechnen wir die maximal erlaubte Anzahl an Zügen k und die Permutation $t \in RS_s$.

Den Wert k berechnen wir direkt mit $k = 2n - 1$. Um die Permutation $t \in RS_s$ anzugeben, berechnen wir zuerst s mit $s = 2(\max\{m, n\} + 2n)$. Dadurch ist s so bestimmt, dass wir im Korrektheitsbeweis in Abschnitt 5.5 ausreichend Schichten zur Verfügung haben. Zudem definieren wir für $1 \leq i \leq n$ Folgendes:

- $(l_i)_1, (l_i)_2, \ldots, (l_i)_m$ sind die Bits des Bitstrings l_i.
- $a_i := (x_1)^{(l_i)_1} \circ (x_2)^{(l_i)_2} \circ \cdots \circ (x_m)^{(l_i)_m}$
- $b_i := (a_i)^{-1} \circ y_i \circ a_i$
- $t := a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$

Die Ausgabe der Reduktionsfunktion nach GRS ist dann $\langle t, k \rangle$. Die Ausgabe der Reduktionsfunktion nach RS ist $\langle C_t, k \rangle = \langle t \circ C_0, k \rangle$. Beide Reduktionsfunktionen arbeiten in Polynomialzeit.

5.2 Intuition für die Korrektheit

Die Idee hinter der Reduktion basiert darauf, dass die Permutationen b_i für $i \in \{1, 2, \ldots, n\}$ alle kommutieren. Wenn die b_i in der Definition von

t so umgeordnet werden, dass sie einem Hamiltonweg im von $l_1, l_2, \ldots, l_n$ spezifizierten kubischen Graphen entsprechen, dann heben sich die meisten x_j und y_i auf, sodass noch genau k von ihnen übrig bleiben. Weil wir dann t als Produkt von k, x_j und y_i ausdrücken können, können wir auch t^{-1} als Produkt von k, x_j und y_i ausdrücken. Wenn es also im von $l_1, l_2, \ldots, l_n$ spezifizierten kubischen Graphen einen Hamiltonweg gibt, dann ist $\langle t, k\rangle \in$ GRS.

Um deutlicher zu sehen, wie sich Terme in t aufheben, betrachten wir nur einen Teil: $b_i \circ b_{i'}$. Dieser Teil ist gleich $(a_i)^{-1} \circ y_i \circ a_i \circ (a_{i'})^{-1} \circ b_{i'} \circ a_{i'}$. Das Interessante daran ist, dass sich in $a_i \circ (a_{i'})^{-1}$ alles bis auf ein x_j aufhebt. Dies können wir sehen, indem wir in der ausgeschriebenen Form

$$\begin{aligned} a_i \circ (a_{i'})^{-1} = {} & (x_1)^{(l_i)_1} \circ (x_2)^{(l_i)_2} \circ \cdots \circ (x_m)^{(l_i)_m} \\ & \circ (x_1)^{-(l_{i'})_1} \circ (x_2)^{-(l_{i'})_2} \circ \cdots \circ (x_m)^{-(l_{i'})_m} \end{aligned}$$

Terme wie folgt zusammenfassen:

$$(x_1)^{(l_i)_1-(l_{i'})_1} \circ (x_2)^{(l_i)_2-(l_{i'})_2} \circ \cdots \circ (x_m)^{(l_i)_m-(l_{i'})_m}$$

Weil b_i und $b_{i'}$ benachbarten Knoten l_i und $l_{i'}$ entsprechen, die einen Hamming-Abstand von 1 haben, ist $(l_i)_j - (l_{i'})_j = 0$ für alle j bis auf eines, für das $(l_i)_j - (l_{i'})_j = \pm 1$ ist. Daher ist $a_i \circ (a_{i'})^{-1} = (x_j)^{\pm 1}$ für ein bestimmtes j. Weil außerdem $x_j = (x_j)^{-1}$ ist, haben wir gezeigt, dass $a_i \circ (a_{i'})^{-1} = x_j$ für ein bestimmtes j gilt.

Diese Intuition formalisieren wir im nächsten Abschnitt in einen Beweis.

5.3 Die Hinrichtung des Korrektheitsbeweises

Lemma 5.3.1. *Die Permutationen b_i kommutieren miteinander.*

Beweis. Eine Permutation b_i lässt sich auch als $(a_i)^{-1} \circ y_i \circ a_i$ darstellen. Für alle Würfelchen, die nicht von dem Term y_i bewegt werden, ist die Auswirkung der Permutation zu $(a_i)^{-1} \circ a_i = 1$ identisch. In anderen Worten ausgedrückt beeinflusst y_i nur Würfelchen, die von dem Term y_i bewegt werden. Aber y_i beeinflusst nur Würfelchen mit der y-Koordinate i. In einem Rubik's Square gilt generell, dass Würfelchen, die zu einem gewissen Zeitpunkt die y-Koordinate i haben, immer die y-Koordinate $\pm i$ haben. Daher befinden sich alle Würfelchen, die von b_i beeinflusst werden, zu jedem Zeitpunkt in den Zeilen $\pm i$.

Daraus folgt, dass es keine Würfelchen gibt, die sowohl von b_i als auch von b_j für ein $j \neq i$ beeinflusst werden. Die Permutationen b_i kommutieren also. □

Satz 5.3.2. *Wenn $\langle l_1, l_2, \ldots, l_n\rangle \in$ CHamPath ist, dann ist $\langle t, k\rangle \in$ GRS.*

Beweis. Es seien $\langle l_1, l_2, \ldots, l_n\rangle \in$ CHamPath und m die Länge der l_i. Daraus folgt direkt, dass $l_n = 00...0$ ist, dass es eine Anordnung der Bitstrings $l_{i_1}, l_{i_2}, \ldots l_{i_n}$ gibt, sodass aufeinander folgende Bitstrings einen Hamming-Abstand von 1 haben, und dass $i_1 = 1$ und $i_n = n$ ist.

Aus dem Lemma 5.3.1 wissen wir, dass wir $t = a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ zu $t = a_1 \circ b_{i_1} \circ b_{i_2} \circ \cdots \circ b_{i_n}$ umstellen können. Durch Einsetzen der Definition der b_i erhalten wir

$$t = a_1 \circ ((a_{i_1})^{-1} \circ y_{i_1} \circ a_{i_1}) \circ ((a_{i_2})^{-1} \circ y_{i_2} \circ a_{i_2}) \circ \cdots \circ ((a_{i_n})^{-1} \circ y_{i_n} \circ a_{i_n})$$

und durch Verwendung der Assoziativität

$$t = (a_1 \circ (a_{i_1})^{-1}) \circ y_{i_1} \circ (a_{i_1} \circ (a_{i_2})^{-1}) \circ y_{i_2} \\ \circ (a_{i_2} \circ (a_{i_3})^{-1}) \circ \cdots \circ (a_{i_{n-1}} \circ (a_{i_n})^{-1}) \circ y_{i_n} \circ (a_{i_n}).$$

Wir wissen, dass $i_1 = 1$ ist, und damit auch, dass $a_1 \circ (a_{i_1})^{-1} = a_1 \circ (a_1)^{-1} = 1$, die Identität, ist. Außerdem wissen wir, dass $i_n = n$ ist, und damit, dass $a_{i_n} = a_n = (x_1)^{(l_n)_1} \circ (x_2)^{(l_n)_2} \circ \cdots \circ (x_m)^{(l_n)_m} = (x_1)^0 \circ (x_2)^0 \circ \cdots \circ (x_m)^0 = 1$, die Identität, ist.

Daher ist

$$t = y_{i_1} \circ (a_{i_1} \circ (a_{i_2})^{-1}) \circ y_{i_2} \circ (a_{i_2} \circ (a_{i_3})^{-1}) \circ \cdots \circ (a_{i_{n-1}} \circ (a_{i_n})^{-1}) \circ y_{i_n}.$$

Dabei betrachten wir jetzt $a_{i_p} \circ (a_{i_{p+1}})^{-1}$ für ein $p \in \{1, 2, \ldots, n-1\}$. Durch Einsetzen der Definition der a_i erhalten wir

$$a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1} \circ (x_2)^{(l_{i_p})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m} \\ \circ ((x_1)^{(l_{i_{p+1}})_1} \circ (x_2)^{(l_{i_{p+1}})_2} \circ \cdots \circ (x_m)^{(l_{i_{p+1}})_m})^{-1}$$

und durch Umformen erhalten wir

$$a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1} \circ (x_2)^{(l_{i_p})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m} \\ \circ (x_m)^{-(l_{i_{p+1}})_m} \circ (x_{m-1})^{-(l_{i_{p+1}})_{m-1}} \circ \cdots \circ (x_1)^{-(l_{i_{p+1}})_1}.$$

Weil x_u und x_v immer miteinander kommutieren, können wir dies weiter als

$$a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1 - (l_{i_{p+1}})_1} \\ \circ (x_2)^{(l_{i_p})_2 - (l_{i_{p+1}})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m - (l_{i_{p+1}})_m}$$

zusammenfassen.

Da sich l_{i_p} und $l_{i_{p+1}}$ nur in einer Stelle unterscheiden, die wir j_p nennen, gilt, dass $(l_{i_p})_j - (l_{i_{p+1}})_j$ für $j \in \{1, 2, \ldots, m\} \setminus \{j_p\}$ gleich 0 ist und für $j = j_p$ gleich ± 1 ist. Dies reicht aus, um zu zeigen, dass $a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_{j_p})^{\pm 1} = x_{j_p}$ ist.

Dies setzen wir in unsere Gleichung für t ein und erhalten

$$t = y_{i_1} \circ x_{j_1} \circ y_{i_2} \circ x_{j_2} \circ \cdots \circ x_{j_{n-1}} \circ y_{i_n}.$$

Daraus folgt

$$\begin{aligned} 1 &= t^{-1} \circ t \\ &= (y_{i_1} \circ x_{j_1} \circ y_{i_2} \circ x_{j_2} \circ \cdots \circ x_{j_{n-1}} \circ y_{i_n})^{-1} \circ t \\ &= (y_{i_n})^{-1} \circ (x_{j_{n-1}})^{-1} \circ (y_{i_{n-1}})^{-1} \circ (x_{j_{n-2}})^{-1} \circ \cdots \circ (x_{j_1})^{-1} \circ (y_{i_1})^{-1} \circ t \\ &= y_{i_n} \circ x_{j_{n-1}} \circ y_{i_{n-1}} \circ x_{j_{n-2}} \circ \cdots \circ x_{j_1} \circ y_{i_1} \circ t. \end{aligned}$$

Wir haben gezeigt, dass t in $k = 2n - 1$ Permutationen, die Zügen der Form x_j oder y_i entsprechen, invertiert werden kann, und damit, dass $\langle t, k \rangle \in$ GRS ist. □

Korollar 5.3.3. *Wenn $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist, dann ist $\langle C_t, k \rangle \in$ RS.*

Beweis. Dies folgt direkt aus Satz 5.3.2, nach dem $\langle t, k \rangle \in$ RS ist, und Lemma 3.4.4, nach dem dann $\langle C_t, k \rangle \in$ RS ist. □

5.4 Die Farben der Aufkleber von C_t

Um die Rückrichtung des Beweises zu zeigen, ist es hilfreich, die Farben der Aufkleber auf der Ober- und Unterseite des Rubik's Square zu kennen. Dafür definieren wir zuerst $b := b_1 \circ b_2 \circ \cdots \circ b_n$, sodass $t = a_1 \circ b$ gilt und betrachten die Farben der Aufkleber auf der Ober- und Unterseite in der Konfiguration $C_b := b \circ C_0$.

Wir verwenden im Weiteren die Beispielinstanz $I := \langle l_1, l_2, l_3, l_4, l_5 \rangle \in$ CHamPath mit $n = 5$ und $m = 3$, wobei die l_i wir folgt definiert sind:

$$\begin{aligned} l_1 &= 011 \\ l_2 &= 110 \\ l_3 &= 111 \\ l_4 &= 100 \\ l_5 &= 000 \end{aligned}$$

Für dieses Beispiel gilt $s = 2(\max\{3, 5\} + 2 \cdot 5) = 30$ und somit ist C_0 ein 30×30 Rubik's Square.

Um die Konfiguration C_b beschreiben zu können, müssen wir die Auswirkung einer Permutation b_i kennen. Die Abbildung 5.1 zeigt die Oberseite eines Rubik's Square in den Konfigurationen C_0, $a_2 \circ C_0$, $y_2 \circ a_2 \circ C_0$ und $b_2 \circ C_0 = (a_2)^{-1} \circ y_2 \circ a_2 \circ C_0$.

Das exakte Verhalten eines beliebigen Rubik's Square unter einer Permutation b_i wird durch folgendes Lemma beschrieben:

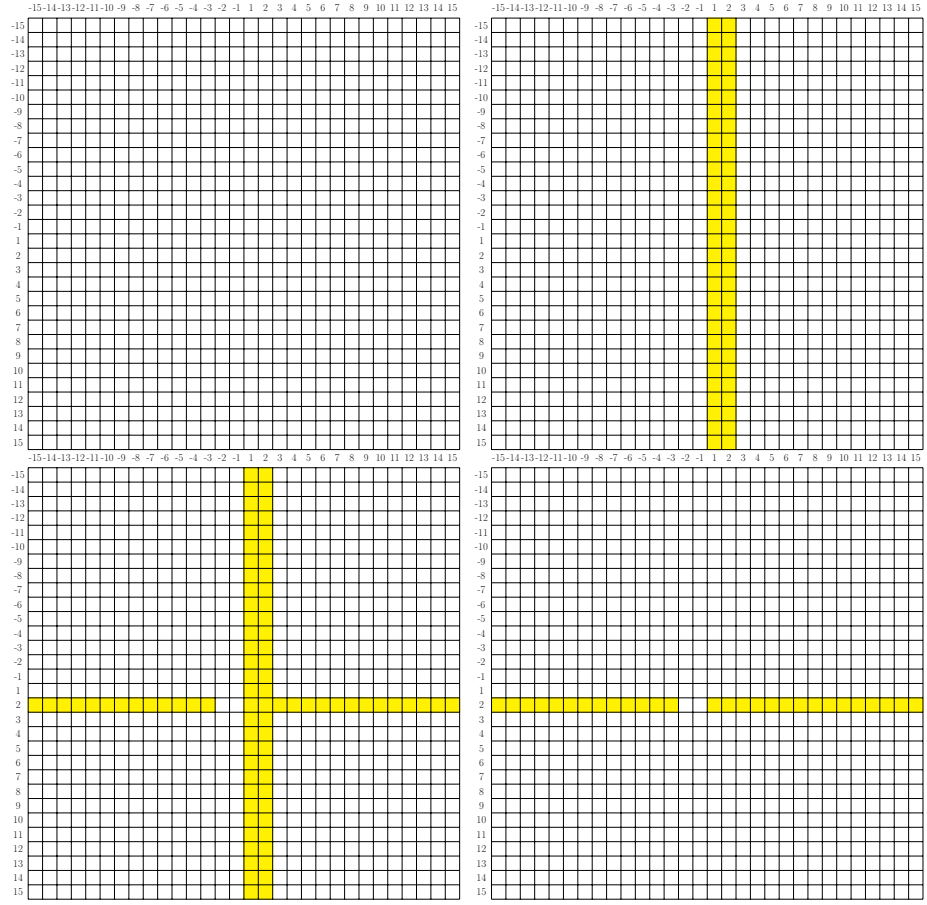


Abbildung 5.1: Schrittweise Auswirkung von b_2 auf C_0 (von oben betrachtet)

Lemma 5.4.1. *Es seien $i \in \{1, 2, \ldots, n\}$ und $c, r \in \{1, 2, \ldots, \frac{s}{2}\}$. Dann gilt:*

1. *Wenn $r = i$, $c \leq m$ und $(l_i)_c = 1$ ist, dann vertauscht b_i die Würfelchen an den Positionen $(c, -r)$ und $(-c, r)$, ohne sie zu wenden.*

2. *Wenn $r = i$ und entweder $c > m$ oder $c \leq m$ und $(l_i)_c = 0$ ist, dann vertauscht b_i die Würfelchen an den Positionen (c, r) und $(-c, r)$ und wendet beide.*

3. *Alle anderen Würfelchen sind nicht von b_i betroffen.*

Beweis. Im Beweis des Lemmas 5.3.1 haben wir bereits festgestellt, dass ein Würfelchen genau dann von $b_i = (a_i)^{-1} \circ y_i \circ a_i$ betroffen ist, wenn es von dem Term y_i bewegt wird.

Außerdem bewegt $(a_i)^{-1} = a_i$ nur Würfelchen aus Spalten c, für die $(l_i)_c = 1$ gilt, nur innerhalb ihrer Spalten. Daher kann ein Würfelchen nur von a_i bewegt werden, wenn seine x-Koordinate positiv ist. Ein Würfelchen, dass

von dem Term y_i bewegt wird, hat danach eine x-Koordinate mit anderem Vorzeichen als zuvor. Deshalb kann ein solches Würfelchen nicht von dem Term $(a_i)^{-1}$ und dem Term a_i bewegt werden.

Es gibt also für Würfelchen, die von b_i bewegt werden, drei mögliche Fälle: (1) das Würfelchen wird nur von y_i bewegt, (2) das Würfelchen wird von a_i und dann von y_i bewegt und (3) das Würfelchen wird von y_i und dann von $(a_i)^{-1}$ bewegt.

Zuerst betrachten wir ein beliebiges Würfelchen vom Typ (1), dessen Koordinaten die Beträge c und r haben. Weil es von y_i bewegt wird, wissen wir, dass $r = i$ ist. Weil das Würfelchen weder von a_i noch von $(a_i)^{-1}$ bewegt wird, wissen wir, dass sein Spaltenindex kein von a_i beeinflusster Spaltenindex ist. Es kann also nicht gelten, dass $(l_i)_c = 1$ ist. Zudem gilt noch, dass das Würfelchen genau einmal gewendet wird. Wenn also $c \in \{1, 2, \ldots, \frac{s}{2}\}$, $r = i$ ist und $(l_i)_c$ entweder nicht existiert oder nicht gleich 1 ist, dann vertauscht b_i die beiden Würfelchen an den Positionen (c, r) und $(-c, r)$ und wendet sie beide.

Als nächstes betrachten wir ein beliebiges Würfelchen vom Typ (2), dessen Koordinaten die Beträge c und r haben. Weil es zuerst von a_i und dann von y_i bewegt wird, wissen wir, dass $r = i$, $c \leq m$ und $(l_i)_c = 1$ ist. Außerdem muss das Würfelchen erst von a_i von der Position $(c, -r)$ in die Position (c, r) und dann von y_i in die Position $(-c, r)$ bewegt werden. Es wird dabei zweimal gewendet, sodass es am Ende insgesamt nicht gewendet ist.

Zuletzt betrachten wir noch ein beliebiges Würfelchen vom Typ (3), dessen Koordinaten die Beträge c und r haben. Weil es zuerst von y_i und dann von $(a_i)^{-1}$ bewegt wird, wissen wir, dass $r = i$, $c \leq m$ und $(l_i)_c = 1$ ist. Außerdem muss das Würfelchen erst von a_i von der Position $(-c, r)$ in die Position (c, r) und dann von y_i in die Position $(c, -r)$ bewegt werden. Es wird dabei zweimal gewendet, sodass es am Ende insgesamt nicht gewendet ist.

Wenn also $r = i$ ist und $(l_i)_c = 1$ ist, dann vertauscht b_i die beiden Würfelchen an den Positionen $(c, -r)$ und $(-c, r)$, ohne sie zu wenden.

Damit haben wir alle Würfelchen abgedeckt, die von b_i bewegt werden. Alle anderen Würfelchen sind also nicht betroffen. □

Diese Erkenntnisse können wir jetzt verwenden, um die Auswirkung der Permutation $b = b_1 \circ b_2 \circ \cdots \circ b_n$ auf C_0 zu verstehen und damit die Farben der Aufkleber der Konfiguration C_b.

Satz 5.4.2. *In C_b hat ein Würfelchen genau dann einen gelben Aufkleber auf der Oberseite, wenn es sich in der Position (c, r) befindet, sodass $r \in \{1, 2, \ldots, n\}$ und entweder $|c| > m$ oder $|c| \leq m$ und $(l_r)_{|c|} = 0$ ist.*

Beweis. In C_0 sind die Aufkleber auf der Oberseite alle weiß. Ein Würfelchen hat in $C_b = b \circ C_0$ genau dann einen gelben Aufkleber auf der Oberseite,

wenn es von der Permutation $b = b_1 \circ b_2 \circ \cdots \circ b_n$ eine ungerade Anzahl oft gewendet wird. Jede Permutation b_i beeinflusst eine disjunkte Menge an Würfelchen. Von allen Würfelchen, die von einer bestimmten Permutation b_i bewegt werden, sind die einzigen, die am Ende einen gelben Aufkleber auf der Oberseite haben, diejenigen, die von b_i gewendet werden. Nach Lemma 5.4.1 sind dies die Würfelchen mit den Koordinaten (c, i), sodass $(l_i)_{|c|}$ nicht gleich 1 ist. Wenn wir alle diese Würfelchen für $i \in \{1, 2, \ldots, n\}$ zusammenfügen, erhalten wir genau die Menge an Würfelchen, die im Satz beschrieben ist. □

Damit haben wir die Farben der Aufkleber von C_b ausreichend bestimmt. Um die Farben der Konfiguration C_t zu bestimmen, die in der Reduktion tatsächlich erzeugt wird, müssen wir die Transformation a_1 auf die Farben von C_b anwenden.

Wenn wir den Satz 5.4.2 auf unser Beispiel anwenden, finden wir heraus, dass die Konfiguration C_b wie in Abbildung 5.2 aussieht. Dabei fällt auf, dass die $m \times n$-Matrix, die sich aus den Bitstrings $l_1, l_2, \ldots, l_n$ zusammensetzt, direkt in den Farben der Aufkleber eines entsprechenden Gebiets auf der Oberseite des Rubik's Square kodiert ist. Zudem ist in Abbildung 5.2 die Konfiguration C_t für dasselbe Beispiel zu sehen.

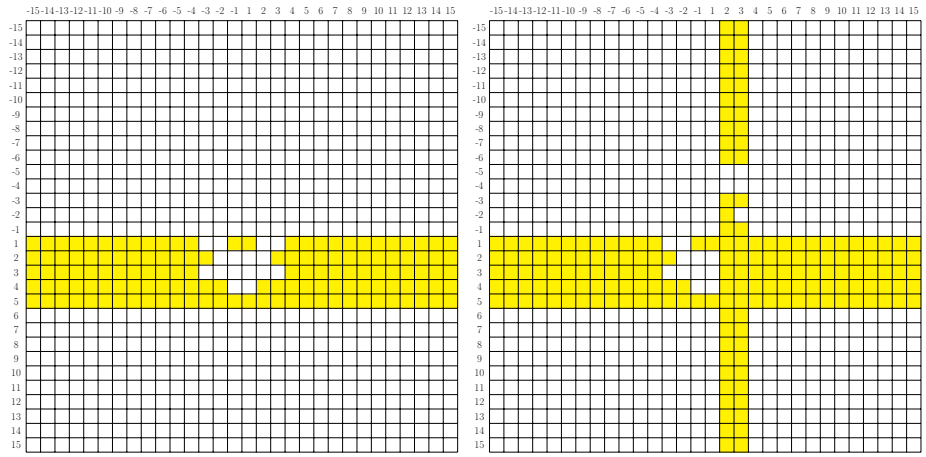


Abbildung 5.2: Die Konfigurationen C_b und C_t für die Beispielinstanz $\langle l_1, l_2, l_3, l_4, l_5 \rangle$ (von oben betrachtet)

5.5 Die Rückrichtung des Korrektheitsbeweises

In diesem Abschnitt beweisen wir den folgenden Satz:

Satz 5.5.1. *Wenn $\langle C_t, k \rangle \in RS$ ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in CHamPath$.*

Beweis. Es sei $\langle C_t, k \rangle \in$ RS. Es existiert also eine Folge von Rubik's Square-Zügen $m_1, m_2, \ldots m_{k'}$ mit $k' \leq k$, sodass $C' := m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ C_t$ eine

gelöste Konfiguration des Rubik's Square ist. In diesem Beweis werden wir nur die Tatsache, dass diese Zugfolge die Ober- und Unterseite des Rubik's Square in der Konfiguration C_t löst, verwenden.

Der Beweis setzt sich aus drei Schritten zusammen. Im ersten Schritt werden wir in Lemma 5.5.2 zeigen, dass $m_1, m_2, \dots m_{k'}$ eine Zeile i genau dann eine ungerade Anzahl oft wenden muss, wenn $i \in \{1, 2, \dots, n\}$ ist.

Dann definieren wir $E \subseteq \{1, 2, \dots, n\}$ als Menge der Indizes i, für die die Zugfolge genau einen y-Zug mit Index i enthält. Weil die Zugfolge die Konfiguration C_t löst, muss sie aus Gründen der Parität für jedes $i \in \{1, 2, \dots, n\}$ einen $y = i$-Zug und null $y = -i$-Züge enthalten. Im zweiten Schritt des Beweises werden wir in Lemma 5.5.4 zeigen, dass für $i_1, i_2 \in E$ die Anzahl der x-Züge zwischen dem $y = i_1$-Zug und dem $y = i_2$-Zug mindestens der Hamming-Abstand von l_{i_1} und l_{i_2} sein muss.

Im letzten Schritt argumentieren wir durch Abzählen. Es gibt vier Typen von Zügen in $m_1, m_2, \dots m_{k'}$:

1. y-Züge mit Index i mit $i \in E$ (die alle $y = i$-Züge sind)
2. y-Züge mit Index i mit $i \in \{1, 2, \dots, n\} \setminus E$
3. x-Züge
4. y-Züge mit Index i mit $i \notin \{1, 2, \dots, n\}$

Für jedes $i \in E$ gibt es nach der Definition von E genau einen y-Zug mit Index i. Daher ist die Anzahl an Typ-1-Zügen gleich $|E|$.

Für jedes $i \in \{1, 2, \dots, n\} \setminus E$ ist die Anzahl der y-Züge mit Index i aufgrund der Parität ungerade. Außerdem ist sie nach Definition von E nicht gleich 1. Die Anzahl dieser Züge ist also für jedes $i \in \{1, 2, \dots, n\} \setminus E$ mindestens 3. Daher ist die Anzahl an Typ-2-Zügen mindestens $3\left(\left|\{1, 2, \dots, n\} \setminus E\right|\right) = 3(n - |E|)$.

Jetzt betrachten wir die $y = i$-Züge mit $i \in E$. Weil die Bitstrings l_i alle voneinander unterschiedlich sind, muss zwischen jedem aufeinanderfolgenden Paar von solchen y-Zügen mindestens ein x-Zug liegen. Daher ist die Anzahl der Typ-3-Züge mindestens $|E| - 1$. Diese Anzahl ist genau dann gleich $|E| - 1$, wenn zwischen jedem solchen Paar von y-Zügen genau ein x-Zug liegt. Dies ist genau dann der Fall, wenn die zugehörigen Bitstrings l_i einen Hamming-Abstand von genau 1 haben. Wenn wir die Bitstrings also entsprechend der Reihenfolge der zugehörigen y-Züge in der Zugfolge anordnen, dann ist die Anzahl der Typ-3-Züge genau dann gleich $|E| - 1$, wenn die Bitstrings jeweils von einem zum nächsten einen Hamming-Abstand von 1 haben.

Über die Anzahl der Typ-4-Züge können wir im Moment noch nichts aussagen, außer dass sie mindestens 0 ist.

Wenn wir all diese unteren Schranken zusammenaddieren, finden wir heraus, dass die Zugfolge mindestens

$$|E| + 3(n - |E|) + (|E| - 1) + E = 3n - 1 - |E| = k + (n - |E|)$$

Züge enthält. Weil $n - |E| \geq 0$ ist und es maximal k Züge sein können, wissen wir jetzt, dass $|E| = n$ sein muss und dass die Anzahl der Züge genau die errechnete untere Schranke ist. Weil $|E| = n$ ist, ist $E = \{1, 2, \ldots, n\}$. Aufgrund der Bedingung für die Minimalität der Typ-3-Züge, wissen wir außerdem, dass die Bitstrings l_i für $i \in E = \{1, 2, \ldots, n\}$ in der Reihenfolge, in der die entsprechenden $y = i$-Züge in der Zugfolge vorkommen, jeweils von einem zum nächsten einen Hamming-Abstand von 1 haben. Weil eine solche Anordnung der Bitstrings $l_1, l_2, \ldots, l_n$ existiert, enthält der kubische Graph, der durch sie bestimmt ist, einen Hamiltonweg und damit ist $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath. □

Lemma 5.5.2. *Die Zugfolge $m_1, m_2, \ldots m_{k'}$ muss eine Zeile i genau dann eine ungerade Anzahl oft wenden, wenn $i \in \{1, 2, \ldots, n\}$ ist.*

Beweis. Wir betrachten die Permutation

$$m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ t = m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n.$$

Diese Permutation ist nicht notwendigerweise die Identität, aber sie muss die Konfiguration C_0 in eine gelöste Konfiguration C' transformieren.

Unter den $2n = k + 1$ Indizes

$$\max\{m, n\} + 1,\ \max\{m, n\} + 2,\ \ldots,\ \max\{m, n\} + 2n$$

muss es mindestens einen Index i geben, für den die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keinen Zug mit Index i enthält. Es sei u ein solcher Index.

Jetzt betrachten wir die Auswirkung der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ auf das Würfelchen an der Position (u, u). Wenn wir $t = a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ als Produkt von Permutationen x_j und y_i nach den Definitionen der Permutationen a_i und b_i schreiben, dann können wir sehen, dass jeder Zug in t nur Zeilen und Spalten mit einem Index von maximal $\max\{m, n\}$ wendet. Daher wendet kein Term in $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ die Zeile oder Spalte u. Das Würfelchen an der Position (u, u) wird also von dieser Permutation nicht bewegt. Durch Anwenden dieser Permutation auf C_0 erhalten wir C'. Weil das Würfelchen in der Konfiguration C_0 einen weißen Aufkleber auf der Oberseite hat, hat es auch in der Konfiguration C' einen weißen Aufkleber auf der Oberseite. Weil C' außerdem eine gelöste Konfiguration ist, muss die gesamte obere Seite des Rubik's Square in Konfiguration C' weiß sein.

Als nächstes betrachten wir das Würfelchen in der Position (u, r) für ein $r \in \left\{-\frac{s}{2}, -\frac{s}{2} + 1, \ldots, \frac{s}{2}\right\} \setminus \{0\}$. Weil keine Zeile oder Spalte mit dem Index u jemals von der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ gewendet wird, wird dieses Würfelchen nur von $y = r$-Zügen bewegt. Außerdem wendet jeder $y = r$-Zug das Würfelchen und tauscht dadurch die Farben auf der Ober- und Unterseite. Weil sowohl in der Konfiguration C_0 als auch in der

Konfiguration C' die obere Seite weiß ist, muss die Permutation eine gerade Anzahl an $y = r$-Zügen enthalten.

Für alle $i \in \{1, 2, \ldots, n\}$ enthält die Permutation $a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$, wenn sie in Permutationen $y_{i'}$ und x_j ausgeschrieben wird, genau eine Permutation y_i. Daher muss die Zugfolge $m_1, m_2, \ldots, m_{k'}$ jede Permutation y_i eine ungerade Anzahl oft enthalten. Für alle $i \notin \{1, 2, \ldots, n\}$ enthält die Permutation $a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$, wenn sie in Permutationen $y_{i'}$ und x_j ausgeschrieben wird, keine Permutation y_i. Daher muss die Zugfolge $m_1, m_2, \ldots, m_{k'}$ jede Permutation y_i eine gerade Anzahl oft enthalten. □

Lemma 5.5.3. *Wenn $i_1, i_2 \in E$ sind, $i_1 \neq i_2$ ist und $j \in \{1, 2, \ldots, m\}$ ist, sodass die Aufkleber auf der Oberseite der Würfelchen in den Positionen (j, i_1) und (j, i_2) unterschiedliche Farben haben, dann muss es in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ mindestens einen x-Zug mit Index j zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug geben.*

Beweis. Wir führen einen Widerspruchsbeweis durch. Dafür nehmen wir an, dass die Aussage falsch wäre, also dass $i_1, i_2 \in E$ und $j \in \{1, 2, \ldots, m\}$ existierten, sodass die Farben der Aufkleber auf der Oberseite der Würfelchen in den Positionen (j, i_1) und (j, i_2) in der Konfiguration C_b unterschiedlich wären und zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ kein x-Zug mit Index j gemacht würde.

Wir betrachten jetzt diese beiden Würfelchen. Aus der Konfiguration C_b erreichen wir die Konfiguration C' durch Anwenden der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 = m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ (x_1)^{(l_1)_1} \circ (x_2)^{(l_1)_2} \circ \cdots \circ (x_m)^{(l_1)_m}$. Diese Permutation ist das Produkt mancher der Permutationen $x_1, x_2, \ldots, x_m$ und der Zugfolge $m_1, m_2, \ldots, m_{k'}$.

Weil die beiden Würfelchen in den Positionen (j, i_1) und (j, i_2) anfangen, sind die einzigen Züge, die sie jemals bewegen können, von einer der Formen x_j, x_{-j}, y_{i_1}, y_{-i_1}, y_{i_2} und y_{-i_1}. Außerdem treten nach der Definition von E keine Züge der Form y_{-i_1} oder y_{-i_2} auf und treten die Züge der Formen y_{i_1} und y_{i_2} jeweils genau einmal auf. Letztlich treten nach der Annahme keine Züge der Form x_j oder x_{-j} zwischen den Zügen der Formen y_{i_1} und y_{i_2} auf.

Insgesamt hat die Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ auf diese beiden Würfelchen also die gleiche Auswirkung wie eine Zugfolge, die wie folgt abläuft: (1) einige Züge der Formen x_j und x_{-j} gefolgt von (2) den beiden Zügen der Formen y_{i_1} und y_{i_2} in beliebiger Reihenfolge gefolgt von (3) einigen Zügen der Formen x_j und x_{-j}.

In Schritt (1) wendet jeder der x-Züge mit Index j jeweils entweder beide Würfelchen oder keines von beiden, weil sie anfangs beide in der Spalte j sind. Sie werden also beide gleich oft gewendet. Außerdem ist das Vorzeichen der y-Koordinate der beiden Würfelchen zu jedem Zeitpunkt gleich. In Schritt (2) werden entweder beide Würfelchen genau einmal gewendet (wenn das Vorzeichen positiv ist) oder nicht gewendet (wenn das Vorzeichen negativ

ist). Sie werden also wieder beide gleich oft gewendet. Schließlich werden die Würfelchen auch in Schritt (3) analog zu Schritt (1) beide gleich oft gewendet, weil sie am Anfang in derselben Spalte sind. Sie werden also von der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ beide gleich oft gewendet.

Weil die beiden Würfelchen also in der Konfiguration C_b auf der Oberseite verschiedenfarbige Aufkleber haben, haben sie auch nach Anwendung der Permutation auf der Oberseite verschiedenfarbige Aufkleber. Die resultierende Konfiguration ist aber C', in der alle Aufkleber auf der Oberseite weiß sind. Wir haben also einen Widerspruch erreicht und damit gezeigt, dass die Aussage dieses Lemmas wahr ist. □

Lemma 5.5.4. *Wenn $i_1, i_2 \in E$ sind und $i_1 \neq i_2$ ist, dann muss die Anzahl der x-Züge zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug in der Zugfolge $m_1, m_2, \ldots m_{k'}$ mindestens der Hamming-Abstand von l_{i_1} und l_{i_2} sein.*

Beweis. Aus dem Satz 5.5.1 wissen wir, dass für ein $i \in \{1, 2, \ldots, n\}$ und ein $j \in \{1, 2, \ldots, m\}$ gilt, dass der Aufkleber auf der Oberseite des Würfelchens an der Position (j, i) in der Konfiguration C_b genau dann weiß ist, wenn $(l_i)_j = 1$ ist. Wenn sich also die Bitstrings l_{i_1} und l_{i_2} in Bit j unterscheiden, dann hat eines der beiden Würfelchen in den Positionen (j, i_1) und (j, i_2) einen weißen Aufkleber auf der Oberseite und das andere einen gelben. Mit Lemma 5.5.3 folgt daraus, dass in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug mindestens ein x-Zug mit dem Index j sein muss. Weil dieser x-Zug den Index j hat, gibt es für jeden Unterschied zwischen l_{i_1} und l_{i_2} mindestens einen unterschiedlichen x-Zug zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug. Wir haben also gezeigt, dass die Anzahl der x-Züge zwischen dem einzigen $y = i_1$-Zug und dem einzigen $y = i_2$-Zug mindestens der Hamming-Abstand von l_{i_1} und l_{i_2} ist. □

Korollar 5.5.5. *Wenn $\langle t, k \rangle \in GRS$ ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in CHam-Path$.*

Beweis. Dies folgt direkt aus Lemma 3.4.4, nach dem $\langle C_t, k \rangle \in$ RS ist, und Satz 5.5.1, nach dem dann $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist. □

5.6 Fazit

Satz 5.6.1. *RS und GRS sind NP-vollständig.*

Beweis. Nach Korollar 5.3.3 und Satz 5.5.1 ist die in Abschnitt 5.1 beschriebene Reduktionsfunktion für RS korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch RS NP-schwer. Weil RS außerdem nach Satz 3.5.1 in NP liegt, ist RS NP-vollständig.

Nach Satz 5.3.2 und Korollar 5.5.5 ist die in Abschnitt 5.1 beschriebene Reduktionsfunktion für GRS korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch GRS NP-schwer. Weil GRS außerdem nach Satz 3.5.1 in NP liegt, ist GRS NP-vollständig. □

Kapitel 6

Die NP-Vollständigkeit der Rubik's Cube-Probleme

6.1 Die Reduktionen

In diesem Abschnitt werden wir die Reduktionsfunktionen für die Rubik's Cube-Probleme beschreiben. Diese sind denen für die Rubik's Square-Probleme generell recht ähnlich und die Intuition dazu ist dieselbe. Weil die Terme b_i kommutieren, können sie bei einer "Ja"-Instanz von CHamPath so umgeordnet werden, dass sich die t so vereinfachen lässt, dass nur k Züge übrig bleiben. Dann kann t in k Zügen sowohl angewendet als auch rückgängig gemacht werden.

Es gibt jedoch auch einige Unterschiede. Der erste Unterschied ist, dass die Züge x_i, y_i und z_i beim Rubik's Cube nur Drehungen und keine Wendungen sind. Die Züge sind also nicht ihr eigenes Inverses. Ein weiterer Unterschied ist, dass wir beim Rubik's Square die Auswirkungen von Zeilen- und Spaltenzügen relativ getrennt voneinander betrachten konnten. Beim Rubik's Cube können jedoch Züge der Außenseiten ganze Reihen von Aufklebern von einer Achsenausrichtung zu einer anderen bewegen. Um zu vermeiden, dass dadurch eine Lösung entsteht, obwohl die entsprechende Instanz eine "Nein"-Instanz von CHamPath ist, werden wir den Schichten, die die Funktionen der Zeilen 1 bis n und der Spalten 1 bis m übernehmen, komplett unterschiedliche Indizes zuweisen.

Wir zeigen die NP-Schwere von STMRC, SQTMRC, GSTMRC und GSQTMRC mittels Reduktion von CHamPath, dessen NP-Schwere wir in Abschnitt 4.2 gezeigt haben.

Die einzig erheblichen Unterschiede im Vergleich zu der Reduktionsfunktion für den Rubik's Square sind, dass s anders berechnet wird, und, dass t aus x- und z-Zügen statt aus x- und y-Zügen besteht.

Die Eingabe ist eine Instanz von CHamPath, die aus n Bitstrings

$l_1, l_2, \ldots, l_n$ der Länge m besteht, wobei $l_n = \underbrace{00...0}_{m}$ gilt. Daraus berechnen wir die maximal erlaubte Anzahl an Zügen k und die Permutation $t \in RS_s$.

Den Wert k berechnen wir direkt mit $k = 2n - 1$. Um die Permutation $t \in RS_s$ anzugeben, berechnen wir zuerst s mit $s = 6n + 2m$. Dadurch ist s so bestimmt, dass wir im Korrektheitsbeweis in Abschnitt 6.4 ausreichend Schichten zur Verfügung haben. Zudem definieren wir für $1 \leq i \leq n$ Folgendes:

- $(l_i)_1, (l_i)_2, \ldots, (l_i)_m$ sind die Bits des Bitstrings l_i.
- $a_i := (x_1)^{(l_i)_1} \circ (x_2)^{(l_i)_2} \circ \cdots \circ (x_m)^{(l_i)_m}$
- $b_i := (a_i)^{-1} \circ z_{m+i} \circ a_i$
- $t := a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$

Die Ausgabe der Reduktionsfunktion nach GSTMRC und GSQTMRC ist dann $\langle t, k \rangle$. Die Ausgabe der Reduktionsfunktion nach STMRC und SQTMRC ist $\langle C_t, k \rangle = \langle t \circ C_0, k \rangle$. Diese Reduktionsfunktionen arbeiten wieder in Polynomialzeit.

6.2 Die Hinrichtung des Korrektheitsbeweises

In diesem Abschnitt beweisen wir, dass "Ja"-Instanzen von CHamPath auf "Ja"-Instanzen der Rubik's Cube-Probleme abgebildet werden. Der Beweis ist dem Beweis für die Rubik's Square-Probleme in Abschnitt 5.3 sehr ähnlich. Die Unterschiede sind lediglich Kleinigkeiten, die aus den oben genannten Gründen geändert werden mussten.

Lemma 6.2.1. *Die Permutationen b_i kommutieren miteinander.*

Beweis. Eine Permutation b_i lässt sich auch als $(a_i)^{-1} \circ z_{m+i} \circ a_i$ darstellen. Für alle Würfelchen, die nicht von dem Term z_{m+i} bewegt werden, ist die Auswirkung der Permutation zu $(a_i)^{-1} \circ a_i = 1$ identisch. In anderen Worten ausgedrückt beeinflusst y_i nur Würfelchen, die von dem Term z_{m+i} bewegt werden.

Aber z_{m+i} beeinflusst nur Würfelchen mit der z-Koordinate $(m + i)$. Ein solches Würfelchen wurde also entweder von a_i in diese Position bewegt oder war schon dort. a_i besteht aus x-Drehungen im Uhrzeigersinn, die alle disjunkte Mengen an Würfelchen bewegen. Wenn das Würfelchen also von a_i bewegt wird, wird es von genau einer der x-Drehungen bewegt. Daraus folgt, dass es vor der Drehung an der $+z$-Außenseite oder der $-z$-Außenseite gewesen sein und die y-Koordinate $\pm(m + i)$ gehabt haben muss.

Weil außerdem z_{m+i} nicht die Drehung einer Außenseite ist, muss ein von b_i bewegtes Würfelchen entweder die y-Koordinate $\pm(m + i)$ haben und auf

einer der $\pm z$-Außenseiten liegen oder die z-Koordinate $(m+i)$ haben und auf einer der anderen vier Außenseiten liegen. Die Mengen der Würfelchen, die von b_i und b_j für $i, j \in \{1, 2, \ldots, n\}$ und $i \neq j$ bewegt werden, sind also disjunkt. Daher kommutieren die Permutationen b_i alle. □

Satz 6.2.2. *Wenn $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist, dann ist $\langle t, k \rangle \in$ GSQTMRC.*

Beweis. Es seien $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath und m die Länge der l_i. Daraus folgt direkt, dass $l_n = 00...0$ ist, dass es eine Anordnung der Bitstrings $l_{i_1}, l_{i_2}, \ldots l_{i_n}$ gibt, sodass aufeinander folgende Bitstrings einen Hamming-Abstand von 1 haben, und dass $i_1 = 1$ und $i_n = n$ ist.

Aus dem Lemma 6.2.1 wissen wir, dass wir $t = a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ zu $t = a_1 \circ b_{i_1} \circ b_{i_2} \circ \cdots \circ b_{i_n}$ umstellen können. Durch Einsetzen der Definition der b_i erhalten wir

$$t = a_1 \circ ((a_{i_1})^{-1} \circ z_{m+i_1} \circ a_{i_1}) \circ ((a_{i_2})^{-1} \circ z_{m+i_2} \circ a_{i_2}) \circ \cdots \circ ((a_{i_n})^{-1} \circ z_{m+i_n} \circ a_{i_n})$$

und durch Verwendung der Assoziativität

$$\begin{aligned} t = (a_1 \circ (a_{i_1})^{-1}) \circ z_{m+i_1} \circ (a_{i_1} \circ (a_{i_2})^{-1}) \circ z_{m+i_2} \\ \circ (a_{i_2} \circ (a_{i_3})^{-1}) \circ \cdots \circ (a_{i_{n-1}} \circ (a_{i_n})^{-1}) \circ z_{m+i_n} \circ (a_{i_n}). \end{aligned}$$

Wir wissen, dass $i_1 = 1$ ist, und damit auch, dass $a_1 \circ (a_{i_1})^{-1} = a_1 \circ (a_1)^{-1} = 1$, die Identität, ist. Außerdem wissen wir, dass $i_n = n$ ist, und damit, dass $a_{i_n} = a_n = (x_1)^{(l_n)_1} \circ (x_2)^{(l_n)_2} \circ \cdots \circ (x_m)^{(l_n)_m} = (x_1)^0 \circ (x_2)^0 \circ \cdots \circ (x_m)^0 = 1$, die Identität, ist.

Daher ist

$$t = z_{m+i_1} \circ (a_{i_1} \circ (a_{i_2})^{-1}) \circ z_{m+i_2} \circ (a_{i_2} \circ (a_{i_3})^{-1}) \circ \cdots \circ (a_{i_{n-1}} \circ (a_{i_n})^{-1}) \circ z_{m+i_n}.$$

Dabei betrachten wir jetzt $a_{i_p} \circ (a_{i_{p+1}})^{-1}$ für ein $p \in \{1, 2, \ldots, n-1\}$. Durch Einsetzen der Definition der a_i erhalten wir

$$\begin{aligned} a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1} \circ (x_2)^{(l_{i_p})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m} \\ \circ ((x_1)^{(l_{i_{p+1}})_1} \circ (x_2)^{(l_{i_{p+1}})_2} \circ \cdots \circ (x_m)^{(l_{i_{p+1}})_m})^{-1} \end{aligned}$$

und durch Umformen erhalten wir

$$\begin{aligned} a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1} \circ (x_2)^{(l_{i_p})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m} \\ \circ (x_m)^{-(l_{i_{p+1}})_m} \circ (x_{m-1})^{-(l_{i_{p+1}})_{m-1}} \circ \cdots \circ (x_1)^{-(l_{i_{p+1}})_1}. \end{aligned}$$

Weil x_u und x_v immer miteinander kommutieren, können wir dies weiter als

$$\begin{aligned} a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_1)^{(l_{i_p})_1 - (l_{i_{p+1}})_1} \\ \circ (x_2)^{(l_{i_p})_2 - (l_{i_{p+1}})_2} \circ \cdots \circ (x_m)^{(l_{i_p})_m - (l_{i_{p+1}})_m} \end{aligned}$$

zusammenfassen.

Da sich l_{i_p} und $l_{i_{p+1}}$ nur in einer Stelle unterscheiden, die wir j_p nennen, gilt, dass $(l_{i_p})_j - (l_{i_{p+1}})_j$ für $j \in \{1, 2, \ldots, m\} \setminus \{j_p\}$ gleich 0 ist und für $j = j_p$ gleich ± 1 ist. Dies reicht aus, um zu zeigen, dass $a_{i_p} \circ (a_{i_{p+1}})^{-1} = (x_{j_p})^{s_p}$ ist, wobei $s_p = \pm 1$ ist.

Dies setzen wir in unsere Gleichung für t ein und erhalten

$$t = z_{m+i_1} \circ (x_{j_1})^{s_1} \circ z_{m+i_2} \circ (x_{j_2})^{s_2} \circ \cdots \circ (x_{j_{n-1}})^{s_{n-1}} \circ z_{m+i_n}.$$

Daraus folgt

$$\begin{aligned} 1 &= t^{-1} \circ t \\ &= (z_{m+i_1} \circ (x_{j_1})^{s_1} \circ z_{m+i_2} \circ (x_{j_2})^{s_2} \circ \cdots \circ (x_{j_{n-1}})^{s_{n-1}} \circ z_{m+i_n})^{-1} \circ t \\ &= (z_{m+i_n})^{-1} \circ (x_{j_{n-1}})^{-s_{n-1}} \circ (z_{m+i_{n-1}})^{-1} \\ &\quad \circ (x_{j_{n-2}})^{-s_{n-2}} \circ \cdots \circ (x_{j_1})^{-1} \circ (z_{m+i_1})^{-1} \circ t. \end{aligned}$$

Wir haben gezeigt, dass t in $k = 2n - 1$ Permutationen, die SQTM-Zügen der Form $(z_i)^{-1}$, x_j oder $(x_j)^{-1}$ entsprechen, invertiert werden kann, und damit, dass $\langle t, k \rangle \in$ GSQTMRC ist. □

Korollar 6.2.3. *Wenn $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist, dann ist $\langle t, k \rangle \in$ GSTMRC.*

Beweis. Dies folgt direkt aus Satz 6.2.2, nach dem $\langle t, k \rangle \in$ GSQTMRC ist, und Lemma 3.4.6, nach dem $\langle t, k \rangle \in$ GSTMRC ist. □

Korollar 6.2.4. *Wenn $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist, dann ist $\langle C_t, k \rangle \in$ SQTMRC.*

Beweis. Dies folgt direkt aus Satz 6.2.2, nach dem $\langle t, k \rangle \in$ GSQTMRC ist, und Lemma 3.4.5, nach dem $\langle C_t, k \rangle \in$ SQTMRC ist. □

Korollar 6.2.5. *Wenn $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist, dann ist $\langle C_t, k \rangle \in$ STMRC.*

Beweis. Dies folgt direkt aus Korollar 6.2.3, nach dem $\langle t, k \rangle \in$ GSTMRC ist, und Lemma 3.4.5, nach dem $\langle C_t, k \rangle \in$ STMRC ist. □

6.3 Die Farben der Aufkleber von C_t

Auch für den Rubik's Cube wird es für die Rückrichtung des Beweises hilfreich sein, die Farben der Aufkleber in der Konfiguration C_t zu kennen. Dafür definieren wir wieder $b := b_1 \circ b_2 \circ \cdots \circ b_n$, sodass $t = a_1 \circ b$ gilt, und bestimmen zunächst die Farben der Aufkleber in der Konfiguration $C_b := b \circ C_0$.

Wir verwenden wieder dieselbe Beispielinstanz, die in CHamPath liegt, wie bei dem Rubik's Square. Es gilt also für die Beispielinstanz $n = 5$, $m = 3$, sowie Folgendes:

$$l_1 = 011$$
$$l_2 = 110$$
$$l_3 = 111$$
$$l_4 = 100$$
$$l_5 = 000$$

Diese Beispielinstanz wird von der Reduktionsfunktion auf eine Konfiguration eines $s \times s \times s$ Rubik's Cube abgebildet, wobei $s = 2m + 6n = 36$ ist. Außerdem ist die Anordnung der Aufkleber in der Konfiguration C_b in Abbildung 6.1 zu sehen. Es ist direkt zu erkennen, dass die Bitstrings $l_1, l_2, \ldots, l_n$ in den Farben der Aufkleber eines $n \times m$ Rechtecks auf jeder Seite des Rubik's Cube kodiert sind.

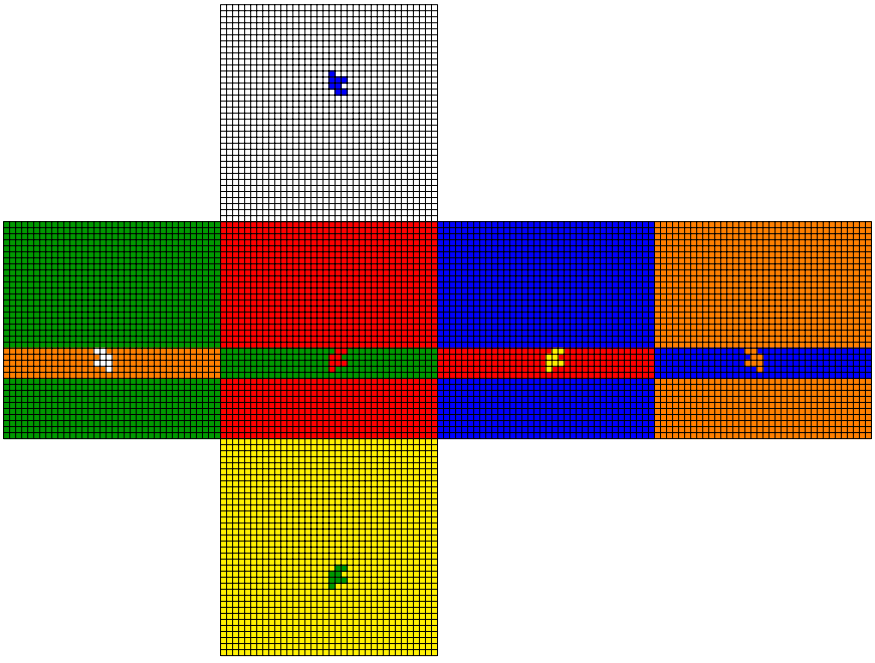


Abbildung 6.1: Die Konfiguration C_b für die Beispielinstanz $\langle l_1, l_2, l_3, l_4, l_5 \rangle$ (als Würfelnetz dargestellt)

In diesem Abschnitt beweisen wir den Satz 6.3.4, der das Muster der Farben der Aufkleber in der Konfiguration C_b genau beschreibt. Dafür ist allerdings noch etwas Vorarbeit notwendig. Wir beschreiben zuerst die Auswirkung eines b_i auf den Rubik's Cube in den Lemmata 6.3.1, 6.3.2

und 6.3.3. Die Abbildung 6.2 zeigt die $+x$- $+y$- und $-z$-Außenseiten eines Rubik's Cube in den Konfigurationen C_0, $a_2 \circ C_0$, $z_{m+2} \circ a_2 \circ C_0$ und $b_2 \circ C_0 = (a_2)^{-1} \circ z_{m+2} \circ a_2 \circ C_0$.

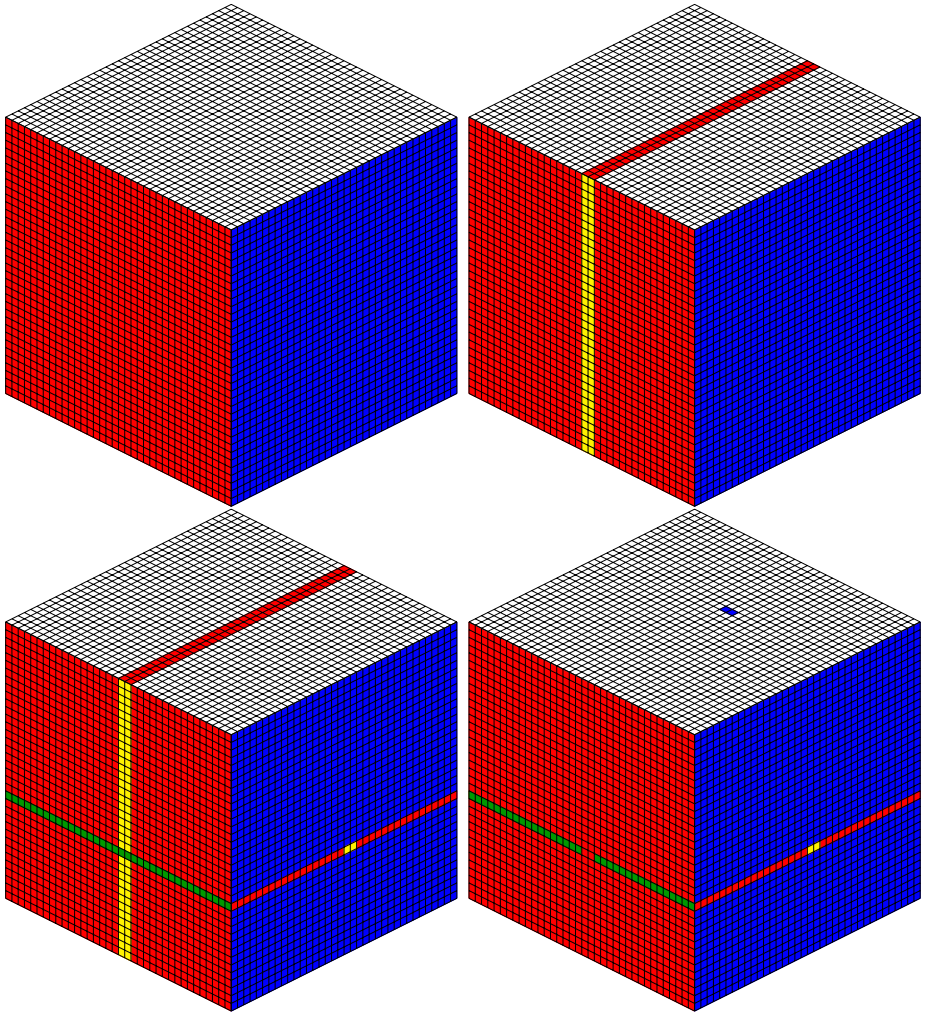


Abbildung 6.2: Schrittweise Auswirkung von b_2 auf C_0

Lemma 6.3.1. *Die Permutation b_i für ein $i \in \{1, 2, \ldots, n\}$ hat auf die Aufkleber auf den $\pm z$-Außenseiten eines Rubik's Cube folgende Auswirkungen:*

- *Wenn $(l_i)_j$ existiert und gleich 1 ist, dann landet ein Aufkleber der $-z$-Außenseite mit den (x, y)-Koordinaten $(j, -(m + i))$ auf der $-x$-Außenseite mit den (y, z)-Koordinaten $(-j, (m + i))$.*
- *Wenn $(l_i)_j$ existiert und gleich 1 ist, dann landet ein Aufkleber der $+z$-Außenseite mit den (x, y)-Koordinaten $(j, -(m + i))$ auf der $+x$-Außenseite mit den (y, z)-Koordinaten $(-j, (m + i))$.*

- *Alle anderen Aufkleber der $\pm z$-Außenseiten bleiben, wo sie sind.*

Beweis. Wie im Beweis von Lemma 6.2.1 angemerkt wurde, wird ein Aufkleber genau dann von $b_i = (a_i)^{-1} \circ z_{m+i} \circ a_i$ bewegt, wenn er von dem Term z_{m+i} bewegt wird.

Wir betrachten die Aufkleber, die sich ursprünglich auf der $-z$-Außenseite befinden. b_i beginnt mit der Permutation a_i, die die x-Schichten mit den x-Koordinaten j für alle j, für die gilt, dass $(l_i)_j$ existiert und gleich 1 ist, bewegt. Es werden also alle Aufkleber der $-z$-Seite mit solchen x-Koordinaten zur $-y$-Außenseite bewegt, während sich die anderen Aufkleber jener Seite nicht bewegen. Die einzigen von der $-z$-Außenseite kommenden Aufkleber, die von dem Term z_{m+i} bewegt werden, sind die, die sich jetzt auf der $-y$-Außenseite befinden und die z-Koordinate $(m+i)$ haben. Dies sind genau die Aufkleber, die ursprünglich die (x,y)-Koordinaten $(j,-(m+i))$ für ein j für das gilt, dass $(l_i)_j$ existiert und gleich 1 ist, hatten.

Die anderen Aufkleber der $-z$-Außenseite werden nicht von dem Term z_{m+i} bewegt und somit auch nicht von b_i. Jetzt betrachten wir einen solchen Aufkleber der $-z$-Außenseite, der von b_i bewegt wird und zu Beginn die (x,y)-Koordinaten $(j,-(m+i))$ hat. Zuerst wird er von a_i zu den (x,z)-Koordinaten $(j,(m+i))$ auf der $-y$-Außenseite bewegt. Dann wird er von z_{m+i} zu den (y,z)-Koordinaten $(-y,(m+i))$ auf der $-x$-Außenseite bewegt. Schließlich wird er nicht von $(a_i)^{-1}$ bewegt, weil er sich auf der $-x$-Außenseite befindet und $(a_i)^{-1}$ nur aus Drehungen von x-Schichten besteht.

Wenn also $(l_i)_j$ existiert und gleich 1 ist, dann landet ein Aufkleber der $-z$-Außenseite mit den (x,y)-Koordinaten $(j,-(m+i))$ auf der $-x$-Außenseite mit den (y,z)-Koordinaten $(-j,(m+i))$. Alle anderen Aufkleber der $-z$-Außenseite bleiben, wo sie sind.

Der Beweis für Aufkleber der $+z$-Außenseite verläuft analog hierzu. □

Lemma 6.3.2. *Die Permutation b_i für ein $i \in \{1,2,\ldots,n\}$ hat auf die Aufkleber auf den $\pm y$-Außenseiten eines Rubik's Cube folgende Auswirkungen:*

- *Wenn $(l_i)_j$ nicht existiert oder gleich 0 ist, dann landet ein Aufkleber der $-y$-Außenseite mit den (x,z)-Koordinaten $(j,(m+i))$ auf der $-x$-Außenseite mit den (y,z)-Koordinaten $(-j,(m+i))$.*

- *Wenn $(l_i)_j$ nicht existiert oder gleich 0 ist, dann landet ein Aufkleber der $+y$-Außenseite mit den (x,z)-Koordinaten $(j,(m+i))$ auf der $+x$-Außenseite mit den (y,z)-Koordinaten $(-j,(m+i))$.*

- *Alle anderen Aufkleber der $\pm y$-Außenseiten bleiben, wo sie sind.*

Beweis. Wie im Beweis von Lemma 6.2.1 angemerkt wurde, wird ein Aufkleber genau dann von $b_i = (a_i)^{-1} \circ z_{m+i} \circ a_i$ bewegt, wenn er von dem Term z_{m+i} bewegt wird.

Wir betrachten die Aufkleber, die sich ursprünglich auf der $-y$-Außenseite befinden. b_i beginnt mit der Permutation a_i, die die x-Schichten mit den x-Koordinaten j für alle j, für die gilt, dass $(l_i)_j$ existiert und gleich 1 ist, bewegt. Es werden also alle Aufkleber der $-y$-Seite mit solchen x-Koordinaten zur $+z$-Außenseite bewegt, während sich die anderen Aufkleber jener Seite nicht bewegen. Die einzigen von der $-y$-Außenseite kommenden Aufkleber, die von dem Term z_{m+i} bewegt werden, sind die, die sich jetzt immer noch auf der $-y$-Außenseite befinden und die z-Koordinate $(m+i)$ haben. Dies sind genau die Aufkleber, die ursprünglich die (x,y)-Koordinaten $(j,-(m+i))$ für ein j für das gilt, dass $(l_i)_j$ nicht existiert oder gleich 0 ist, hatten.

Die anderen Aufkleber der $-y$-Außenseite werden nicht von dem Term z_{m+i} bewegt und somit auch nicht von b_i. Jetzt betrachten wir einen solchen Aufkleber der $-y$-Außenseite, der von b_i bewegt wird und zu Beginn die (x,y)-Koordinaten $(j,-(m+i))$ hat. Ein solcher Aufkleber wird nicht von a_i bewegt. Dann wird er von z_{m+i} zu den (y,z)-Koordinaten $(-y,(m+i))$ auf der $-x$-Außenseite bewegt. Schließlich wird er nicht von $(a_i)^{-1}$ bewegt, weil er sich auf der $-x$-Außenseite befindet und $(a_i)^{-1}$ nur aus Drehungen von x-Schichten besteht.

Wenn also $(l_i)_j$ nicht existiert oder gleich 0 ist, dann landet ein Aufkleber der $-y$-Außenseite mit den (x,z)-Koordinaten $(j,-(m+i))$ auf der $-x$-Außenseite mit den (y,z)-Koordinaten $(-j,(m+i))$. Alle anderen Aufkleber der $-y$-Außenseite bleiben, wo sie sind.

Der Beweis für Aufkleber der $+y$-Außenseite verläuft analog hierzu. □

Lemma 6.3.3. *Die Permutation b_i für ein $i \in \{1,2,\ldots,n\}$ hat auf die Aufkleber auf den $\pm x$-Außenseiten eines Rubik's Cube folgende Auswirkungen:*

- *Wenn $(l_i)_j$ existiert und gleich 1 ist, dann landet ein Aufkleber der $-x$-Außenseite mit den (y,z)-Koordinaten $(j,(m+i))$ auf der $+z$-Außenseite mit den (x,y)-Koordinaten $(j,-(m+i))$.*

- *Wenn $(l_i)_j$ nicht existiert oder gleich 0 ist, dann landet ein Aufkleber der $-x$-Außenseite mit den (y,z)-Koordinaten $(j,(m+i))$ auf der $+y$-Außenseite mit den (x,z)-Koordinaten $(j,(m+i))$.*

- *Wenn $(l_i)_j$ existiert und gleich 1 ist, dann landet ein Aufkleber der $+x$-Außenseite mit den (y,z)-Koordinaten $(j,(m+i))$ auf der $-z$-Außenseite mit den (x,y)-Koordinaten $(j,-(m+i))$.*

- *Wenn $(l_i)_j$ nicht existiert oder gleich 0 ist, dann landet ein Aufkleber der $+x$-Außenseite mit den (y,z)-Koordinaten $(j,(m+i))$ auf der $-y$-Außenseite mit den (x,z)-Koordinaten $(j,(m+i))$.*

- *Alle anderen Aufkleber der $\pm x$-Außenseiten bleiben, wo sie sind.*

Beweis. Wie im Beweis von Lemma 6.2.1 angemerkt wurde, wird ein Aufkleber genau dann von $b_i = (a_i)^{-1} \circ z_{m+i} \circ a_i$ bewegt, wenn er von dem Term z_{m+i} bewegt wird.

Wir betrachten die Aufkleber, die sich ursprünglich auf der $-x$-Außenseite befinden. b_i beginnt mit der Permutation a_i, die keine Aufkleber der $-x$-Außenseite bewegt. Der Term z_{m+i} bewegt dann genau die Aufkleber der $-x$-Außenseite, die die z-Koordinate $(m + i)$ haben. Es werden also genau diese Aufkleber von b_i bewegt.

Jetzt betrachten wir einen solchen Aufkleber der $-x$-Außenseite, der von b_i bewegt wird und zu Beginn die (y, z)-Koordinaten $(j, (m+i))$ hat. Er wird von a_i nicht bewegt und von z_{m+i} zu den (x, z)-Koordinaten $(j, (m+i))$ auf der $+y$-Außenseite bewegt. Dann gibt es zwei Fälle:

Fall 1: Wenn $(l_i)_j$ nicht existiert oder gleich 0 ist, dann wird der Aufkleber nicht von $(a_i)^{-1}$ bewegt. In diesem Fall wird also ein Aufkleber von b_i von den (y, z)-Koordinaten $(j, (m + i))$ auf der $-x$-Außenseite zu den (x, z)-Koordinaten $(j, (m + i))$ auf der $+y$-Außenseite bewegt.

Fall 2: Wenn $(l_i)_j$ existiert und gleich 1 ist, dann wird der Aufkleber von $(a_i)^{-1}$ zu den (x, y)-Koordinaten $(j, -(m+i))$ auf der $+z$-Außenseite bewegt. In diesem Fall wird also ein Aufkleber von b_i von den (y, z)-Koordinaten $(j, (m + i))$ auf der $-x$-Außenseite zu den (x, y)-Koordinaten $(j, -(m + i))$ auf der $+z$-Außenseite bewegt.

Damit haben wir alle Aufkleber der $-x$-Außenseite behandelt und die Aussagen des Lemmas über sie bewiesen.

Der Beweis für Aufkleber der $+x$-Außenseite verläuft analog hierzu. □

Jetzt können wir diese Lemmata anwenden, um die Auswirkung der Permutation $b = b_1 \circ b_2 \circ \cdots \circ b_n$ auf die Konfiguration C_0 zu beschreiben und damit die Farben der Aufkleber der Konfiguration C_b anzugeben.

Satz 6.3.4. *In C_b haben die Aufkleber folgende Farben:*

$-x$: *Die Aufkleber auf der $-x$-Außenseite mit den (y, z)-Koordinaten $(-j, (m + i))$, für ein $i \in \{1, 2, \ldots n\}$ und ein j, für das gilt, dass $(l_i)_j$ existiert und gleich 1 ist, sind alle weiß. Alle anderen Aufkleber auf dieser Seite mit der z-Koordinate $(m + i)$ für ein $i \in \{1, 2, \ldots n\}$ sind orange. Alle anderen Aufkleber auf dieser Seite sind grün.*

$+x$: *Die Aufkleber auf der $+x$-Außenseite mit den (y, z)-Koordinaten $(-j, (m + i))$, für ein $i \in \{1, 2, \ldots n\}$ und ein j, für das gilt, dass $(l_i)_j$ existiert und gleich 1 ist, sind alle gelb. Alle anderen Aufkleber auf dieser Seite mit der z-Koordinate $(m + i)$ für ein $i \in \{1, 2, \ldots n\}$ sind rot. Alle anderen Aufkleber auf dieser Seite sind blau.*

$-y$: *Die Aufkleber auf der $-y$-Außenseite mit den (x, z)-Koordinaten $(j, (m + i))$, für ein $i \in \{1, 2, \ldots n\}$ und ein j, für das gilt, dass $(l_i)_j$*

existiert und gleich 1 ist, sind alle orange. Alle anderen Aufkleber auf dieser Seite mit der z-Koordinate $(m+i)$ *für ein* $i \in \{1, 2, \dots n\}$ *sind blau. Alle anderen Aufkleber auf dieser Seite sind orange.*

$+y$**:** *Die Aufkleber auf der* $+y$*-Außenseite mit den* (x, z)*-Koordinaten* $(j, (m+i))$*, für ein* $i \in \{1, 2, \dots n\}$ *und ein* j*, für das gilt, dass* $(l_i)_j$ *existiert und gleich 1 ist, sind alle rot. Alle anderen Aufkleber auf dieser Seite mit der z-Koordinate* $(m+i)$ *für ein* $i \in \{1, 2, \dots n\}$ *sind grün. Alle anderen Aufkleber auf dieser Seite sind rot.*

$-z$**:** *Die Aufkleber auf der* $-z$*-Außenseite mit den* (x, y)*-Koordinaten* $(j, -(m+i))$*, für ein* $i \in \{1, 2, \dots n\}$ *und ein* j*, für das gilt, dass* $(l_i)_j$ *existiert und gleich 1 ist, sind alle blau. Alle anderen Aufkleber auf dieser Seite sind weiß.*

$+z$**:** *Die Aufkleber auf der* $+z$*-Außenseite mit den* (x, y)*-Koordinaten* $(j, -(m+i))$*, für ein* $i \in \{1, 2, \dots n\}$ *und ein* j*, für das gilt, dass* $(l_i)_j$ *existiert und gleich 1 ist, sind alle grün. Alle anderen Aufkleber auf dieser Seite sind gelb.*

Beweis. Es gilt $C_b = b \circ C_0 = b_1 \circ b_2 \circ \dots \circ b_n \circ C_0$. Außerdem wissen wir aus dem Beweis von Lemma 6.2.1, dass die Mengen der Aufkleber, die von den Permutationen b_i bewegt werden, disjunkt sind. Da wir jetzt die Auswirkung eines b_i auf eine Konfiguration eines Rubik's Cube kennen, können wir zeigen, dass die Aussagen des Satzes die Farben der Aufkleber der Konfiguration C_b korrekt beschreiben.

Wir betrachten beispielhaft die Aufkleber, die sich nach Anwenden der Permutation auf der $+z$-Außenseite befinden. Nach Lemma 6.3.3 gilt für jedes $i \in \{1, 2, \dots, n\}$, dass ein Aufkleber der $-x$-Außenseite mit den (y, z)-Koordinaten $(j, (m+i))$ von b_i auf der zu der Position auf der $+z$-Außenseite mit den (x, y)-Koordinaten $(j, -(m+i))$ bewegt wird, wenn $(l_i)_j$ existiert und gleich 1 ist. Weil die Mengen der Aufkleber, die von den Permutationen b_i bewegt werden, disjunkt sind, befinden sich alle Aufkleber, die in der Konfiguration C_b auf der $+z$-Außenseite sind und die (x, y)-Koordinaten $(j, -(m+i))$ für ein $i \in \{1, 2, \dots, n\}$ und ein j, für das gilt, dass $(l_i)_j$ existiert und gleich 1 ist, haben, in C_0 auf der $-x$-Außenseite. Weil diese Außenseite in C_0 grün ist, sind auch die Aufkleber alle grün. Wir wissen außerdem aus den Lemmata 6.3.1, 6.3.2 und 6.3.3, dass ansonsten keine Aufkleber von einem b_i auf die $+z$-Außenseite bewegt werden. Daher werden alle diese anderen Aufkleber nicht von b bewegt und haben somit dieselbe Farbe, wie in C_0, also gelb. Damit haben wir die Aussagen über die Aufkleber auf der $+z$-Außenseite gezeigt.

Der Beweis für die anderen fünf Außenseiten verläuft analog hierzu. □

Damit haben wir die Farben der Aufkleber in der Konfiguration C_b komplett beschrieben. Die Farben der Aufkleber in der Konfiguration

$C_t = a_1 \circ C_b$, die von der Reduktionsfunktion erzeugt wird, werden durch Anwenden der Permutationen a_1 erhalten. Dies ist für das Beispielinstanz von Anfang dieses Abschnitts in Abbildung 6.3 dargestellt.

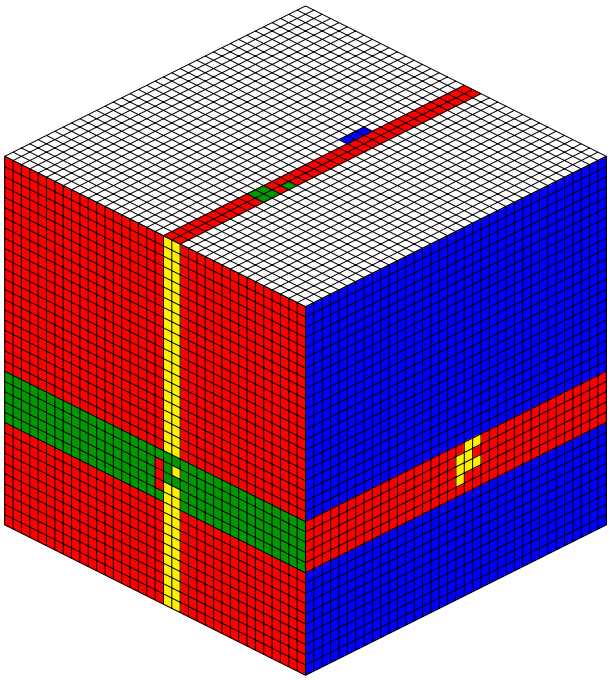


Abbildung 6.3: Die Konfiguration C_t für die Beispielinstanz $\langle l_1, l_2, l_3, l_4, l_5 \rangle$

6.4 Beweisskizze der Rückrichtung des Korrektheitsbeweises

In diesem Abschnitt werden wir den Beweis für den folgenden Satz skizzieren, den wir im Rest dieses Kapitels vervollständigen werden:

Satz 6.4.1. *Wenn $\langle C_t, k \rangle \in STMRC$ ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in CHam-Path$.*

Die Idee hinter dem Beweis ist generell ähnlich zu der für den Rubik's Square in Abschnitt 5.5. Der Beweis ist aber komplexer, weil Rubik's Cube aufgrund der weiteren Dimension mehr Freiheitsgrade haben. So ist es z. B. durch Außenseitenzüge möglich, dass eine Reihe von Aufklebern während einer Lösung eines Rubik's Cube in verschiedene Richtungen zeigt.

Daher enthält der Beweis einige Schritte, die wir hier nur oberflächlich beschreiben und dann in den folgenden Abschnitten genau betrachten werden.

Beweis. Es sei $\langle C_t, k\rangle \in$ STMRC. Es existiert also eine Folge von STM-Rubik's Cube-Zügen $m_1, m_2, \ldots, m_{k'}$ für ein $k' \leq k$, sodass $C' := m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ C_t$ eine gelöste Konfiguration des Rubik's Cube ist.

Eine Idee, die im Laufe dieses Beweises mehrfach verwendet wird, ist es, einen Index u zu betrachten, für den gilt, dass keiner der Züge m_i für $i \in \{1, 2, \ldots, k'\}$ ein Zug mit Index u ist.

Definition 6.4.2. Es sei $u \in \{m+n+1, m+n+2, \ldots, m+n+2n\}$ ein Index, sodass die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keinen Zug mit Index u enthält.

Es muss ein solches u geben, weil es aus einer Menge von $2n = k + 1 > k \geq k'$ Indizes ausgewählt wird und jeder der k' Züge der Zugfolge höchstens einen Index ausschließt.

Schritt 1 besteht aus einer vorläufigen Charakterisierung der möglichen Züge mit Index $(m + i)$ für ein $i \in \{1, 2, \ldots, n\}$ in der Zugfolge $m_1, m_2, \ldots, m_{k'}$.

Definition 6.4.3. Wir partitionieren die Menge {1, 2, ..., n} in die vier (möglicherweise leeren) Teilmengen N, E, Z und M wie folgt:

- $i \in N$ genau dann, wenn $m_1, m_2, \ldots, m_{k'}$ genau null Züge mit Index $(m + i)$ enthält.
- $i \in E$ genau dann, wenn $m_1, m_2, \ldots, m_{k'}$ genau einen Zug mit Index $(m + i)$ enthält.
- $i \in Z$ genau dann, wenn $m_1, m_2, \ldots, m_{k'}$ genau zwei Züge mit Index $(m + i)$ enthält.
- $i \in M$ genau dann, wenn $m_1, m_2, \ldots, m_{k'}$ mehr als zwei Züge mit Index $(m + i)$ enthält.

In Abschnitt 6.5 werden wir folgende Aussagen beweisen, die die Menge der möglichen Züge mit Index $(m + i)$ für ein $i \in \{1, 2, \ldots, n\}$ aus $m_1, m_2, \ldots, m_{k'}$ einschränken:

- N ist leer.
- Wenn $i \in E$ ist, dann muss der einzige Zug mit Index $(m + i)$ eine z-Drehung gegen den Uhrzeigersinn sein.
- Wenn $i \in Z$ ist, dann müssen die beiden Züge mit Index $(m + i)$ eine z-Drehung im Uhrzeigersinn und eine z-Wendung sein.
- Wenn $i \in E \cup Z$ ist, dann muss jeder positive z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem die $\pm x$- und $\pm y$-Außenseiten jeweils um 0° gedreht sind, und jeder negative z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem diese Außenseiten um 180° gedreht sind.

In Schritt 2 verwenden wir das Konzept der gekuppelten Aufkleber:

Definition 6.4.4. Es seien $p_1, p_2, q \in \left\{1, 2, \ldots, \frac{s}{2} - 1\right\}$ paarweise verschiedene Indizes. Wir bezeichnen zwei Aufkleber genau dann als (p_1, p_2, q)-**gekuppelt**, wenn sich die Aufkleber in demselben Quadranten einer Außenseite befinden, einer der beiden Aufkleber die Koordinaten $\pm q$ und $\pm p_1$ auf dieser Außenseite hat und der andere Aufkleber die Koordinaten $\pm q$ und $\pm p_2$ auf dieser Außenseite hat.

In Abschnitt 6.6 werden wir folgende Eigenschaften gekuppelter Aufkleber beweisen:

- Wenn zwei Aufkleber (p_1, p_2, q)-gekuppelt sind, dann bleiben sie dies nach einem Zug, außer es handelt sich bei dem Zug um einen Zug mit Index p_1 oder Index p_2, der einen der Aufkleber bewegt.
- Es seien $i_1, i_2 \in E$ und $j \in \{1, 2, \ldots, m\}$. Wir betrachten ein beliebiges Paar von Aufklebern, die in C_b $(m+i_1, m+i_2, j)$-gekuppelt sind. Wenn die Zugfolge $m_1, m_2, \ldots m_{k'}$ zwischen dem Zug mit Index $(m+i_1)$ und dem Zug mit Index $(m+i_2)$ keine $\pm x$- oder $\pm y$-Außenseitenzüge und keine Züge mit Index j, die einen der Aufkleber bewegen, enthält, dann bleiben die beiden Aufkleber auch in C' (p_1, p_2, q)-gekuppelt.

In Schritt 3 werden wir die möglichen Züge in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ durch Abzählen deutlich einschränken. Dafür klassifizieren wir sie in folgende disjunkte Typen:

- "E-Züge": Züge mit Index $(m+i)$ für ein $i \in E$
- "Z-Züge": Züge mit Index $(m+i)$ für ein $i \in Z$
- "M-Züge": Züge mit Index $(m+i)$ für ein $i \in M$
- "J-Züge": Züge mit Index j für ein $j \in J := \{1, 2, \ldots, m\}$
- "Züge vertikaler Außenseiten": Züge der $\pm x$- oder $\pm y$-Außenseiten
- "andere Züge": alle anderen Züge

In Abschnitt 6.7 werden wir mithilfe der Resultate aus den Schritten 1 und 2 zeigen, dass zwischen jedem Paar von E-Zügen in $m_1, m_2, \ldots, m_{k'}$ ein J-Zug oder zwei Züge vertikaler Außenseiten sein müssen. Dies erlaubt es uns, die Anzahl der Züge von jedem Typ wie folgt abzuzählen:

Es seien $c_E, c_Z, c_M, c_J, c_{\text{vertikal}}$ und c_{andere} die Anzahlen der Züge der entsprechenden Typen. Dann erhalten wir folgen Einschränkungen:

- $c_E = |E|$
- $c_Z = 2|Z|$

- $c_M \geq 3|M|$
- $c_J + \frac{1}{2}c_{\text{vertikal}} \geq |E| - 1$
- $c_{\text{andere}} \geq 0$

Wenn wir diese Anzahlen jetzt zusammenrechnen, erhalten wir:

$$\begin{aligned}
k' &= c_E + c_Z + c_M + c_{\text{vertikal}} + c_J + c_{\text{andere}} \\
&= c_E + c_Z + c_M + \left(c_J + \frac{1}{2}c_{\text{vertikal}}\right) + \frac{1}{2}c_{\text{vertikal}} + c_{\text{andere}} \\
&\geq |E| + 2|Z| + 3|M| + (|E| - 1) + \frac{1}{2}c_{\text{vertikal}} + 0 \\
&= 2|E| + 2|Z| + 3|M| - 1 + \frac{1}{2}c_{\text{vertikal}} \\
&= 2(|E| + |Z| + |M|) + |M| - 1 + \frac{1}{2}c_{\text{vertikal}} \\
&= 2n - 1 + |M| + \frac{1}{2}c_{\text{vertikal}} \\
&= k + |M| + \frac{1}{2}c_{\text{vertikal}} \\
&\geq k
\end{aligned}$$

Jetzt können wir sehen, dass $k' \geq k$ ist und wissen bereits, dass $k' \leq k$ ist. Daher muss $k' = k$ sein und somit auch in jedem Schritt der obigen Rechnung Gleichheit vorliegen. Daraus ergibt sich, dass $c_M = |M| = c_{\text{vertikal}} = c_{\text{andere}} = 0$ ist und es gelten weiterhin $c_E = |E|$, $c_Z = |Z|$ und $c_J = |E| - 1$. Wir haben also gezeigt, dass die Zugfolge $m_1, m_2, \ldots, m_{k'}$ außer E- und Z-Zügen nur $|E| - 1$ viele J-Züge enthält, die jeweils zwischen den E-Zügen sind.

In Schritt 4 schränken wir dies weiter ein. Insbesondere werden wir in Abschnitt 6.8 folgende Aussagen über die Zugfolge $m_1, m_2, \ldots, m_{k'}$ zeigen:

- Weil es keine Außenseitenzüge gibt, kann der Zug mit Index $(m + i)$ für ein $i \in E$ nur eine positive z-Drehung gegen den Uhrzeigersinn sein. Ähnlich dazu können die beiden Züge mit Index $(m + i)$ für ein $i \in Z$ nur eine positive z-Drehung im Uhrzeigersinn und eine positive z-Wendung sein.

- Wir betrachten die Elemente $i \in E$ in der Reihenfolge, in der die entsprechenden E-Züge passieren. Wenn i_1 und i_2 in dieser Reihenfolge direkt aufeinander folgen, dann müssen l_{i_1} und l_{i_2} einen Hamming-Abstand von eins haben.

- Der eine J-Zug zwischen zwei aufeinanderfolgenden E-Zügen mit den Indizes $(m + i_1)$ und $(m + i_2)$ muss ein positiver x-Zug mit Index j sein, wobei j der eindeutig bestimmte Index ist, sodass $(l_{i_1})_j \neq (l_{i_2})_j$ gilt.

Wir betrachten weiter die Elemente $i \in E$ in der Reihenfolge, in der die entsprechenden E-Züge passieren. Wie wir in Schritt 4 gezeigt haben, haben die entsprechenden Bitstrings l_i in derselben Reihenfolge die Eigenschaft, dass aufeinanderfolgende l_i den Hamming-Abstand eins haben.

In Schritt 5 in Abschnitt 6.9 werden wir mithilfe des Konzepts der gekuppelten Aufkleber zeigen, dass Z leer ist. Daraus folgt, dass $E = \{1, 2, \ldots, n\}$ ist. Weil die obige Anordnung der Bitstrings l_i eine Anordnung ist, bei der aufeinanderfolgende l_i den Hamming-Abstand eins haben, und sie außerdem alle l_i für $i \in \{1, 2, \ldots, n\}$ enthält, haben wir so gezeigt, dass $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath ist. □

Korollar 6.4.5. *Wenn $\langle C_t, k \rangle \in$ SQTMRC ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath.*

Beweis. Dies folgt direkt aus Lemma 3.4.6 und Satz 6.4.1. □

Korollar 6.4.6. *Wenn $\langle t, k \rangle \in$ GSTMRC ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath.*

Beweis. Dies folgt direkt aus Lemma 3.4.5 und Satz 6.4.1. □

Korollar 6.4.7. *Wenn $\langle t, k \rangle \in$ GSQTMRC ist, dann ist $\langle l_1, l_2, \ldots, l_n \rangle \in$ CHamPath.*

Beweis. Dies folgt direkt aus Lemma 3.4.5 und Korollar 6.4.5. □

6.5 Schritt 1: Einschränkungen der möglichen Züge mit Index $(m + i)$

In diesem Abschnitt werden wir, wie in der Beweisskizze in Abschnitt 6.4 angekündigt, folgende Aussagen beweisen:

- N ist leer.
- Wenn $i \in E$ ist, dann muss der einzige Zug mit Index $(m + i)$ eine z-Drehung gegen den Uhrzeigersinn sein.
- Wenn $i \in Z$ ist, dann müssen die beiden Züge mit Index $(m + i)$ eine z-Drehung im Uhrzeigersinn und eine z-Wendung sein.
- Wenn $i \in E \cup Z$ ist, dann muss jeder positive z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem die $\pm x$- und $\pm y$-Außenseiten jeweils um 0° gedreht sind, und jeder negative z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem diese Außenseiten um 180° gedreht sind.

Dafür befassen wir uns zuerst mit den Farben der Aufkleber in der Konfiguration $C' = m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ C_t$.

Lemma 6.5.1. *Die Außenseiten des Rubik's Cube haben in der gelösten Konfiguration C' dieselben Farben wie in C_0.*

Beweis. Wir betrachten den Aufkleber, der in der Konfiguration C_0 auf einer beliebigen Außenseite die Koordinaten (u, u) hat. Aus der Definition von u folgt, dass die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keine Züge mit Index u enthält. Außerdem enthält $t = a_1 \circ b_1 \circ b_2 \circ \cdots \circ b_n$ auch keine Züge mit Index u, weil die Definition nur Züge von Schichten mit einem Index von maximal $(m+n)$ enthält und $u > m + n$ ist. Der Aufkleber wird also von der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ t$ niemals zu einer anderen Außenseite bewegt. Es gilt aber $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ t \circ C_0 = C'$ und somit befindet sich der Aufkleber in C_0 und C' auf der gleichen Außenseite. Weil wir die Außenseite beliebig gewählt haben und C_0 und C' beide gelöste Konfigurationen sind, müssen alle Außenseiten in der Konfiguration C' dieselben Farben haben wie in C_0. □

Lemma 6.5.2. *N ist leer.*

Beweis. Wir führen einen Widerspruchsbeweis durch und nehmen dafür an, es gäbe ein $i \in \{1, 2, \ldots, n\}$, für das die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keinen Zug mit Index $(m + i)$ enthielte. Wir betrachten den Aufkleber, der in der Konfiguration C_b auf der $+y$-Außenseite die (x, z)-Koordinaten $(u, m+i)$ hat. Es gilt $C' = m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1 \circ C_b$. Die Zugfolge $m_1, m_2, \ldots, m_{k'}$ enthält aber keinen Zug mit Index $(m + i)$ oder mit Index u. Außerdem enthält $a_1 = (x_1)^{(l_1)_1} \circ (x_2)^{(l_1)_2} \circ \cdots \circ (x_m)^{(l_1)_m}$ für alle $j > m$ keine Züge mit Index j. Weil sowohl $(m + i)$ als auch u größer als m sind, enthält auch $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ keine Züge mit Index $(m + i)$ oder Index u. Der Aufkleber wird also von dieser Permutation nicht zu einer anderen Außenseite bewegt.

Der Aufkleber, der in der Konfiguration C_b auf der $+y$-Außenseite die (x, z)-Koordinaten $(u, m + i)$ hat, befindet sich also in der Konfiguration C' auf der $+y$-Außenseite. Nach Satz 6.3.4 hat der Aufkleber in der Konfiguration C_b die Farbe grün. Die $+y$-Außenseite hat aber in der Konfiguration C' dieselbe Farbe wie in C_0, nämlich rot. Wir haben also einen Widerspruch erreicht und damit gezeigt, dass die Zugfolge $m_1, m_2 m \ldots, m_{k'}$ für alle $i \in \{1, 2, \ldots, n\}$ einen Zug mit Index $(m + i)$ enthalten muss, also dass N leer ist. □

Die restlichen Aussagen, die wir zeigen wollen, beziehen sich auf Züge mit Index $(m + i)$ für ein $i \in E \cup Z$. Dabei können wir für jedes solche i die Aufkleber, die wir betrachten, auf im Folgenden definierte spezielle Aufkleber einschränken.

Definition 6.5.3. Für jedes $i \in E \cup Z$ sind die 48 **speziellen Aufkleber** diejenigen, die in der Konfiguration C_b auf einer der Außenseiten die Koordinaten $\pm u$ und $\pm(m + i)$ haben (8 pro Außenseite).

Aus Satz 6.3.4 folgt, dass alle dieser speziellen Aufkleber bis auf 8 (jeweils 2 pro $\pm x$- und $\pm y$-Außenseite) dieselbe Farbe wie die entsprechende Außenseite in C_0 haben.

Definition 6.5.4. Wir bezeichnen die 40 speziellen Aufkleber, die dieselbe Farbe wie die entsprechende Außenseite in C_0 haben, als **korrekt platzierte Aufkleber** und die anderen 8 speziellen Aufkleber als **falsch platzierte Aufkleber**.

Von diesen falsch platzierten Aufklebern haben die beiden auf der $-x$-Außenseite die Farbe der $-y$-Außenseite in C_0, die beiden auf der $-y$-Außenseite die Farbe der $+x$-Außenseite in C_0, die beiden auf der $+x$-Außenseite die Farbe der $+y$-Außenseite in C_0 und die beiden auf der $+y$-Außenseite die Farbe der $-x$-Außenseite in C_0. Die falsch platzierten Aufkleber müssen aus der Konfiguration C_b also um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden, um auf den Außenseiten anzukommen, die in C_0 dieselbe Farbe wie die jeweiligen Aufkleber haben.

Als nächstes betrachten wir die Auswirkung der Zugfolge $m_1, m_2, \ldots, m_{k'}$ auf die speziellen Aufkleber.

Lemma 6.5.5. *Wenn die Zugfolge $m_1, m_2, \ldots, m_{k'}$ auf die Konfiguration C_b angewendet wird, muss sie die falsch platzierten Aufkleber um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegen und die korrekt platzierten Aufkleber so bewegen, dass sie am Ende wieder auf den Außenseiten sind, auf denen sie am Anfang waren.*

Beweis. Die Konfiguration C', die nach Lemma 6.5.1 dasselbe Farbschema wie C_0 hat, kann der Konfiguration C_b durch Anwenden der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ erreicht werden. Die falsch platzierten Aufkleber müssen also um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden und die korrekt platzierten Aufkleber auf ihrer Außenseite bleiben. Die einzigen Züge, die spezielle Aufkleber auf andere Außenseiten bewegen, sind Züge mit Index u und mit Index $(m + i)$. Die einzigen anderen Züge, die spezielle Aufkleber bewegen, sind Außenseitenzüge. Weil a_1 keine Züge einer dieser drei Arten enthält, bewegt a_1 keine speziellen Aufkleber.

Die Auswirkung der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ auf die speziellen Aufkleber ist also dieselbe wie die Auswirkung der Zugfolge $m_1, m_2, \ldots, m_{k'}$. Daher bewegt die Zugfolge die speziellen Aufkleber wie beschrieben. □

Jetzt können wir damit die nächsten beiden Aussagen zeigen.

Lemma 6.5.6. *Wenn $i \in E$ ist, dann muss der einzige Zug mit Index $(m+i)$ eine z-Drehung gegen den Uhrzeigersinn sein.*

Beweis. Wir betrachten das Resultat einer Anwendung der Zugfolge $m_1, m_2, \ldots, m_{k'}$ auf die Konfiguration C_b. Wir haben dazu in Lemma 6.5.5

gezeigt, dass die 8 falsch platzierten Aufkleber um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden und die korrekt platzierten Aufkleber so bewegt werden, dass sie am Ende wieder auf den Außenseiten sind, auf denen sie am Anfang waren. Außerdem sind die einzigen Züge, die spezielle Aufkleber auf andere Außenseiten bewegen, Züge mit Index u und mit Index $(m+i)$. Weil die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keine Züge mit Index u und für ein $i \in E$ genau einen Zug mit Index $(m+i)$ enthält, können die speziellen Aufkleber nur von diesem Zug von einer Außenseite zu einer anderen bewegt werden.

Jede Schicht mit Index $(m+i)$ enthält genau 8 spezielle Aufkleber. Der einzige Zug mit Index $(m+i)$ muss also genau 8 spezielle Aufkleber zu einer anderen Außenseite bewegen. Dies müssen genau die 8 falsch platzierten Aufkleber sein, weil sie sonst auf der falschen Außenseite blieben. Weil sich die falsch platzierten Aufkleber auf den $\pm x$- und $\pm y$-Außenseiten befinden und um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden müssen, muss dieser eine Zug eine z-Drehung gegen den Uhrzeigersinn sein. □

Lemma 6.5.7. *Wenn $i \in Z$ ist, dann müssen die beiden Züge mit Index $(m+i)$ eine z-Drehung im Uhrzeigersinn und eine z-Wendung sein.*

Beweis. Wir betrachten erneut das Resultat einer Anwendung der Zugfolge $m_1, m_2, \ldots, m_{k'}$ auf die Konfiguration C_b. Es gilt, wie wir in Lemma 6.5.5 gezeigt haben, immer noch, dass die 8 falsch platzierten Aufkleber um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden und die korrekt platzierten Aufkleber so bewegt werden, dass sie am Ende wieder auf den Außenseiten sind, auf denen sie am Anfang waren. Die einzigen Züge, die spezielle Aufkleber auf andere Außenseiten bewegen, sind Züge mit Index u und mit Index $(m+i)$. Weil die Zugfolge $m_1, m_2, \ldots, m_{k'}$ keine Züge mit Index u und für ein $i \in Z$ genau zwei Züge mit Index $(m+i)$ enthält, können die speziellen Aufkleber nur von diesen beiden Zügen von einer Außenseite zu einer anderen bewegt werden.

Jede Schicht mit Index $(m+i)$ enthält genau 8 spezielle Aufkleber. Die beiden Züge mit Index $(m+i)$ müssen also jeweils genau 8 spezielle Aufkleber zu einer anderen Außenseite bewegen. Dazu betrachten wir verschieden Fälle:

- Wenn genau einer der beiden Züge mit Index $(m+i)$ ein x-Zug oder ein y-Zug wäre, dann würde mindestens einer der korrekt platzierten Aufkleber der $+z$-Außenseite wegbewegt und nicht wieder dorthin bewegt werden. Dies steht im Widerspruch dazu, dass korrekt platzierte Aufkleber so bewegt werden, dass sie am Ende wieder auf den Außenseiten sind, auf denen sie am Anfang waren.

- Wenn es sich bei beiden Züge mit Index $(m+i)$ um x-Züge handelte, dann würden die falsch platzierten Aufkleber der x-Außenseiten diese

nie verlassen. Dies steht im Widerspruch dazu, dass falsch platzierte Aufkleber zu einer anderen Außenseite bewegt werden.

- Wenn es sich bei beiden Züge mit Index $(m + i)$ um y-Züge handelte, dann würden die falsch platzierten Aufkleber der y-Außenseiten diese nie verlassen. Dies steht im Widerspruch dazu, dass falsch platzierte Aufkleber zu einer anderen Außenseite bewegt werden.

- Wenn es sich bei dem ersten der beiden Züge mit Index $(m+i)$ um einen x-Zug und bei dem zweiten um einen y-Zug handelte, dann würde jeder falsch platzierte Aufkleber der x-Außenseiten auf einer x-Außenseite oder einer z-Außenseite landen. Dies steht im Widerspruch dazu, dass falsch platzierte Aufkleber der x-Außenseiten zu einer y-Außenseite bewegt werden.

- Wenn es sich bei dem ersten der beiden Züge mit Index $(m+i)$ um einen y-Zug und bei dem zweiten um einen x-Zug handelte, dann würde jeder falsch platzierte Aufkleber der y-Außenseiten auf einer y-Außenseite oder einer z-Außenseite landen. Dies steht im Widerspruch dazu, dass falsch platzierte Aufkleber der y-Außenseiten zu einer x-Außenseite bewegt werden.

- Weil alle anderen Fälle zu Widersprüchen führen, muss es sich bei beiden Zügen mit Index $(m + i)$ um z-Züge handeln.

Um einen weiteren Widerspruch zu erreichen, nehmen wir an, dass die Mengen der speziellen Aufkleber, die jeweils von den beiden Zügen mit Index $(m + i)$ bewegt werden, nicht gleich wären. Jeder Aufkleber, der von genau einem dieser Züge bewegt wird, landet auf einer anderen Außenseite und muss daher ein falsch platzierter Aufkleber sein. Ein solcher Aufkleber muss um eine Seite gegen den Uhrzeigersinn um die z-Achse bewegt werden. Weil beide Züge mit Index $(m + i)$ jeweils mindestens einen speziellen Aufkleber bewegen, der nicht von dem anderen Zug bewegt wird, müssen beide Züge z-Drehungen gegen den Uhrzeigersinn sein. Daraus folgt, dass jeder Aufkleber, der von beiden Zügen bewegt wird, insgesamt um zwei Seiten gegen den Uhrzeigersinn um die z-Achse bewegt wird. Dies ist aber bei keinem der speziellen Aufkleber der Fall. Es kann also keinen Aufkleber geben, der von beiden Zügen bewegt wird. Jetzt haben wir also genau 16 unterschiedliche Aufkleber, die von genau einem der beiden Züge mit Index $(m + i)$ bewegt werden. Alle diese 16 Aufkleber werden also auf andere Außenseiten bewegt. Dies steht im Widerspruch dazu, dass nur genau 8 der speziellen Aufkleber falsch platzierte Aufkleber sind.

Aus diesem Widerspruch folgt, dass die beiden Züge dieselben 8 Aufkleber bewegen müssen. Die einzige Möglichkeit, mit zwei Zügen insgesamt eine Drehung gegen den Uhrzeigersinn zu erreichen, ist, dass einer der Züge eine Drehung im Uhrzeigersinn ist und der andere eine Wendung ist. Bei den

beiden Zügen mit Index $(m+i)$ für ein $i \in Z$ handelt es sich also um eine z-Drehung im Uhrzeigersinn und eine z-Wendung. □

Lemma 6.5.8. *Wenn $i \in E \cup Z$ ist, dann muss jeder positive z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem die $\pm x$- und $\pm y$-Außenseiten jeweils um $0°$ gedreht sind, und jeder negative z-Zug mit Index $(m+i)$ zu einem Zeitpunkt passieren, an dem diese Außenseiten um $180°$ gedreht sind.*

Beweis. Wir betrachten erneut das Resultat der Zugfolge $m_1, m_2, \ldots, m_{k'}$ auf die Konfiguration C_b. Die 8 falsch platzierten Aufkleber müssen jeweils um eine Außenseite gegen den Uhrzeigersinn um die z-Achse bewegt werden, während die korrekt platzierten Aufkleber auf ihrer jeweiligen Außenseite bleiben müssen. Die speziellen Aufkleber werden nur von Zügen mit Index $(m+i)$ oder mit Index u auf eine andere Außenseite bewegt, aber auch von Außenseitenzügen bewegt. Die einzigen Züge der Zugfolge $m_1, m_2, \ldots, m_{k'}$, die spezielle Aufkleber zu anderen Außenseiten bewegen, sind der eine oder die zwei Züge mit Index $(m+i)$, weil $i \in E \cup Z$ ist. Außerdem wissen wir aus den Beweisen der Lemmata 6.5.6 und 6.5.7, dass die speziellen Aufkleber, die von diesen Zügen bewegt werden, genau die falsch platzierten sind. Die einzigen Züge der Zugfolge, die die korrekt platzierten Aufkleber bewegen, sind also Außenseitenzüge.

Es sei m_j ein Zug mit Index $(m+i)$ der Zugfolge $m_1, m_2, \ldots, m_{k'}$. Aus den Lemmata 6.5.6 und 6.5.7 folgt, dass m_j ein z-Zug ist.

Wir betrachten im Weiteren die sechs korrekt platzierten Aufkleber auf einer der $\pm x$- oder $\pm y$-Außenseiten. Weil diese Aufkleber nur von Außenseitenzügen bewegt werden, sind ihre Positionen zu jedem Zeitpunkt komplett von der gesamten bisherigen Rotation dieser Außenseite bestimmt. Wenn die gesamte Rotation $0°$ ist, dann befinden sich die sechs korrekt platzierten Aufkleber auf der Außenseite an den Koordinaten $\pm u$ und $\pm(m+i)$, wobei $z \neq (m+i)$ gilt. Wenn die gesamte Rotation $90°$ ist, dann befinden sich die sechs korrekt platzierten Aufkleber auf der Außenseite an den Koordinaten $\pm u$ und $\pm(m+i)$, wobei $x \neq -(m+i)$ gilt, wenn es sich um eine $\pm y$-Außenseite handelt, und $y \neq (m+i)$ gilt, wenn es sich um eine $\pm x$-Außenseite handelt. Wenn die gesamte Rotation $180°$ ist, dann befinden sich die sechs korrekt platzierten Aufkleber auf der Außenseite an den Koordinaten $\pm u$ und $\pm(m+i)$, wobei $z \neq -(m+i)$ gilt. Wenn die gesamte Rotation $270°$ ist, dann befinden sich die sechs korrekt platzierten Aufkleber auf der Außenseite an den Koordinaten $\pm u$ und $\pm(m+i)$, wobei $x \neq (m+i)$ gilt, wenn es sich um eine $\pm y$-Außenseite handelt, und $y \neq -(m+i)$ gilt, wenn es sich um eine $\pm x$-Außenseite handelt.

Wenn m_j ein positiver z-Zug ist, dann kann er diese Aufkleber nur dann nicht bewegen, wenn sie sich in den Positionen mit $z \neq (m+i)$ befinden, also wenn die gesamte bisherige Rotation $0°$ ist. Wenn m_j ein negativer z-Zug ist, dann kann er diese Aufkleber nur dann nicht bewegen, wenn sie

sich in den Positionen mit $z \neq -(m+i)$ befinden, also wenn die gesamte bisherige Rotation 180° ist. Dies gilt für alle $\pm x$- und $\pm y$-Außenseiten. Wir haben also gezeigt, dass die $\pm x$- und $\pm y$-Außenseiten jeweils um 0° gedreht sein müssen, wenn m_j ein positiver Zug mit Index $(m+i)$ ist, und dass die $\pm x$- und $\pm y$-Außenseiten jeweils um 180° gedreht sein müssen, wenn m_j ein negativer Zug mit Index $(m+i)$ ist. □

6.6 Schritt 2: Eigenschaften gekuppelter Aufkleber

In diesem Abschnitt werden wir, wie in der Beweisskizze in Abschnitt 6.4 angekündigt, einige Eigenschaften gekuppelter Aufkleber betrachten.

Lemma 6.6.1. *Wenn zwei Aufkleber (p_1, p_2, q)-gekuppelt sind, dann bleiben sie dies nach einem Zug, außer es handelt sich bei dem Zug um einen Zug mit Index p_1 oder Index p_2, der einen der Aufkleber bewegt.*

Beweis. Wir betrachten für die Auswirkung eines beliebigen Zugs auf die beiden Aufkleber folgende Fälle:

- Wenn der Zug keinen der beiden Aufkleber bewegt, dann verändern sich ihre Positionen nicht. Daher bleiben sie (p_1, p_2, q)-gekuppelt.
- Wenn der Zug beide Aufkleber bewegt, dann werden sie beide gleich weit gedreht. Relativ zu den Aufklebern ist die Auswirkung die gleiche, als wenn sich der gesamte restliche Rubik's Cube drehte, während die Schicht mit den beiden Aufklebern stillstünde. Aus diesem Blickwinkel betrachtet werden die beiden Aufkleber nicht bewegt. Daher bleiben sie genau wie im ersten Fall auch wieder (p_1, p_2, q)-gekuppelt.
- Wenn der Zug einen der beiden Aufkleber bewegt, dann sind sie nach dem Zug nicht mehr (p_1, p_2, q)-gekuppelt.

Die Züge, die die Aufkleber bewegen, sind Außenseitenzüge und Züge mit den Indizes q, p_1 und p_2. Außenseitenzüge und Züge mit Index q bewegen entweder keinen der Aufkleber oder beide. Die einzige Möglichkeit zwei (p_1, p_2, q)-gekuppelte Aufkleber zu trennen, ist also mit einem Zug mit Index p_1 oder p_2, der einen der beiden Aufkleber bewegt. □

Hiermit beweisen wir jetzt folgendes Lemma:

Lemma 6.6.2. *Es seien $i_1, i_2 \in E$ und $j \in \{1, 2, \ldots, m\}$. Wir betrachten ein beliebiges Paar von Aufklebern, die in C_b $(m+i_1, m+i_2, j)$-gekuppelt sind. Wenn die Zugfolge $m_1, m_2, \ldots m_{k'}$ zwischen dem Zug mit Index $(m+i_1)$ und dem Zug mit Index $(m+i_2)$ keine $\pm x$- oder $\pm y$-Außenseitenzüge und keine Züge mit Index j, die einen der Aufkleber bewegen, enthält, dann bleiben die beiden Aufkleber auch in C' (p_1, p_2, q)-gekuppelt.*

Beweis. Wir betrachten zwei in der Konfiguration C_b $(m + i_1, m + i_2, j)$-gekuppelte Aufkleber. Außerdem nehmen wir an, dass die Zugfolge $m_1, m_2, \ldots m_{k'}$ zwischen den E-Zügen mit Index $(m + i_1)$ oder $(m + i_2)$ keine $\pm x$- oder $\pm y$-Außenseitenzüge und keine Züge mit Index j, die einen der Aufkleber bewegen, enthält. Es seien m_α der E-Zug mit Index $(m + i_1)$ und m_β der E-Zug mit Index $(m + i_2)$. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass m_α vor m_β stattfindet.

Weil es zwischen m_α und m_β keine $\pm x$- oder $\pm y$-Außenseitenzüge gibt, muss die Rotation dieser Außenseiten zu den Zeitpunkten der beiden Züge identisch sein. Aus den Ergebnissen aus Schritt 1 folgt, dass m_α und m_β entweder beide positive Drehungen gegen den Uhrzeigersinn oder beide negative Drehungen gegen den Uhrzeigersinn sind.

Die Konfiguration C' kann aus der Konfiguration C_b durch Anwendung der Permutation $m_{k'} \circ m_{k'-1} \circ \cdots \circ m_1 \circ a_1$ erhalten werden. Weil a_1 aus einer gewissen Anzahl von x-Drehungen besteht, lässt sich diese Permutation auch als Zugfolge darstellen. Da wir wissen, dass die Aufkleber in C_b $(m+i_1, m+i_2, j)$-gekuppelt sind, müssen sie bis zu m_α $(m + i_1, m + i_2, j)$-gekuppelt bleiben. Wir werden jetzt zeigen, dass sie aufgrund unserer Annahmen in allen Fällen direkt nach m_β wieder $(m + i_1, m + i_2, j)$-gekuppelt sind.

Der erste Fall ist, dass sich die beiden Aufkleber direkt vor m_α auf der $-z$- oder der $+z$-Außenseite befinden. In diesem Fall bewegt m_α, der ein z-Zug ist, keinen der beiden Aufkleber. Sie sind also auch nach m_α noch immer $(m+i_1, m + i_2, j)$-gekuppelt. Abgesehen von m_α und m_β sind die einzigen Züge der Zugfolge $m_1, m_2, \ldots, m_{k'}$, die die Aufkleber zu einer anderen Außenseite bewegen, Züge mit Index j. Nach der Annahme gibt es aber zwischen m_α und m_β keine Züge mit Index j, die die Aufkleber bewegen. Die Aufkleber werden also direkt vor m_β immer noch $(m + i_1, m + i_2, j)$-gekuppelt sein und sich immer noch auf der $-z$- oder $+z$-Außenseite befinden. Daher wird m_β die Aufkleber auch nicht bewegen. Sie werden also auch direkt nach m_β $(m + i_1, m + i_2, j)$-gekuppelt sein.

Der zweite Fall ist, dass sich die beiden Aufkleber direkt vor m_α auf der $-x$-, $-y$-, $+x$- oder $+y$-Außenseite befinden. Die einzigen Züge zwischen m_α und m_β, die die Aufkleber bewegen, sind Außenseitenzüge und Züge mit Index j. Egal wie m_α die beiden Aufkleber bewegt, bleiben sie beide auf den vier $-x$-, $-y$-, $+x$- und $+y$-Außenseiten. Nach der Annahme wird bis m_β keiner der Aufkleber von einem Zug mit Index j bewegt. Weil sie sich auf den vier Außenseiten befinden, folgt außerdem aus der Annahme, dass keiner der Aufkleber bis m_β von einem Außenseitenzug bewegt wird. Der nächste Zug, der einen der Aufkleber bewegt, ist also m_β.

Es ist zu beachten, dass aus der Definition der $(m + i_1, m + i_2, j)$-gekuppelten Aufkleber folgt, dass der erste Aufkleber direkt vor m_α genau dann die z-Koordinate $(m+i_1)$ hat, wenn der zweite die z-Koordinate $(m+i_2)$ hat. Analog dazu hat der erste Aufkleber genau dann die z-Koordinate $-(m+i_1)$, wenn der zweite die z-Koordinate $-(m+i_2)$ hat. Wir wissen, dass

m_α und m_β zusammen entweder die positiven z-Schichten mit den Indizes $(m + i_1)$ und $(m + i_2)$ einen Zug gegen den Uhrzeigersinn drehen oder die negativen z-Schichten mit den Indizes $(m+i_1)$ und $(m+i_2)$ einen Zug gegen den Uhrzeigersinn drehen. Insgesamt werden die Aufkleber also von den Zügen von m_α bis m_β beide entweder um einen Zug gegen den Uhrzeigersinn oder überhaupt nicht bewegt. Aus der Sichtweise der Aufkleber entspricht eine solche Drehung aber wieder einer Drehung des restlichen Rubik's Cube, bei der sie sich nicht bewegen. Die Aufkleber bleiben also auch in diesem Fall direkt nach m_β $(m + i_1, m + i_2, j)$-gekuppelt.

Die beiden Aufkleber sind also in beiden Fällen direkt nach m_β $(m + i_1, m+i_2, j)$-gekuppelt. Weil außerdem nach m_β keine Züge mit Index $(m+i_1)$ oder $(m + i_2)$ stattfinden, bleiben sie auch bis zum Ende der Zugfolge und damit bis C' $(m + i_1, m + i_2, j)$-gekuppelt. □

6.7 Schritt 3: Klassifizierung möglicher Züge durch Abzählen

In diesem Abschnitt werden wir, wie in der Beweisskizze in Abschnitt 6.4 angekündigt, die möglichen Züge in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ durch Abzählen einschränken.

Zuerst zeigen wir Folgendes:

Lemma 6.7.1. *Zwischen jedem Paar von E-Zügen in $m_1, m_2, \ldots, m_{k'}$ müssen ein J-Zug oder zwei Züge vertikaler Außenseiten sein.*

Beweis. Wir betrachten ein beliebiges Paar von E-Zügen m_α und m_β, die in dieser Reihenfolge passieren. Es seien m_α ein Zug mit Index $(m+i_1)$ und m_β ein Zug mit Index $(m + i_2)$. Außerdem sei j ein Index, für den $(l_{i_1})_j \neq (l_{i_2})_j$ gilt.

Es ist zu beachten, dass die $(m + i_1, m + i_2, j)$-gekuppelten Aufkleber auf der $+y$-Außenseite mit den (x, z)-Koordinaten $(j, m+i_1)$ und $(j, m+i_2)$ in der Konfiguration C_b nach Satz 6.3.4 unterschiedliche Farben haben. Sie dürfen also in C' nicht mehr $(m + i_1, m + i_2, j)$-gekuppelt sein, weil C' eine gelöste Konfiguration ist. Aus der Kontraposition von Lemma 6.6.2 folgt jetzt, dass zwischen m_α und m_β mindestens ein Zug mit Index j, der einen der Aufkleber bewegt, oder mindestens ein $\pm x-$ oder $\pm y$-Außenseitenzug stattfinden muss.

Aus Lemma 6.5.8 aus Schritt 1 wissen wir außerdem, dass zu den Zeitpunkten der Züge m_α und m_β die vier $\pm x$- und $\pm y$-Außenseiten entweder eine gesamte Rotation von 0° oder 180° haben müssen. Zwischen den beiden Zügen muss sich also entweder die Rotation aller vier Außenseiten verändern oder jede Rotation einer Außenseite muss auch wieder rückgängig gemacht werden. Daher ist es nicht möglich, dass zwischen zwei solcher Züge genau eine Drehung einer $\pm x$- oder $\pm y$-Außenseite stattfindet.

Wir haben also gezeigt, dass zwischen m_α und m_β mindestens ein Zug mit Index j oder mindestens zwei $\pm x$- oder $\pm y$-Außenseitenzüge sein müssen. □

Korollar 6.7.2. *Wenn m_α und m_β E-Züge mit Index $(m + i_1)$ und mit Index $(m + i_2)$ sind, $(l_{i_1})_j \neq (l_{i_2})_j$ gilt und zwischen m_α und m_β keine $\pm x$- oder $\pm y$-Außenseitenzüge sind, dann muss zwischen m_α und m_β ein J-Zug mit Index j sein.*

Beweis. Aus dem Beweis für Lemma 6.7.1 wissen wir bereits, dass zwischen m_α und m_β ein J-Zug mit Index j oder zwei $\pm x$- oder $\pm y$-Außenseitenzüge sein müssen. Da wir jetzt zusätzlich die Vorraussetzung haben, dass zwischen m_α und m_β keine $\pm x$- oder $\pm y$-Außenseitenzüge sind, folgt daraus, dass zwischen m_α und m_β ein J-Zug mit Index j sein muss. □

Jetzt können wir die Anzahlen der Züge der verschiedenen Typen wie folgt abzählen:

Für jedes $i \in E$ gibt es genau einen E-Zug, nämlich den Zug mit Index $(m + i)$. Daher ist also $c_E = |E|$.

Für jedes $i \in Z$ gibt es genau zwei Z-Züge, nämlich die beiden Züge mit Index $(m + i)$. Daher ist also $c_Z = 2|Z|$.

Für jedes $i \in M$ gibt es mindestens drei M-Züge, nämlich die Züge mit Index $(m + i)$. Daher ist also $c_M \geq 3|M|$.

Wir betrachten die E-Züge der Reihe nach. Zwischen den $c_E = |E|$ verschiedenen E-Zügen gibt es $|E| - 1$ Zwischenräume. Wie wir in Lemma 6.7.1 gezeigt haben, muss jeder dieser Zwischenräume mindestens einen J-Zug oder mindestens zwei $\pm x$- oder $\pm y$-Außenseitenzüge enthalten. Es gilt also $c_J + \frac{1}{2}c_{\text{vertikal}} \geq |E| - 1$.

Zuletzt gilt noch $c_{\text{andere}} \geq 0$.

Wenn wir dies jetzt zusammensetzen erhalten wir:

$$\begin{aligned}
k' &= c_E + c_Z + c_M + c_{\text{vertikal}} + c_J + c_{\text{andere}} \\
&= c_E + c_Z + c_M + \left(c_J + \frac{1}{2}c_{\text{vertikal}}\right) + \frac{1}{2}c_{\text{vertikal}} + c_{\text{andere}} \\
&\geq |E| + 2|Z| + 3|M| + (|E| - 1) + \frac{1}{2}c_{\text{vertikal}} + 0 \\
&= 2|E| + 2|Z| + 3|M| - 1 + \frac{1}{2}c_{\text{vertikal}} \\
&= 2(|E| + |Z| + |M|) + |M| - 1 + \frac{1}{2}c_{\text{vertikal}} \\
&= 2n - 1 + |M| + \frac{1}{2}c_{\text{vertikal}} \\
&= k + |M| + \frac{1}{2}c_{\text{vertikal}} \\
&\geq k
\end{aligned}$$

Wir haben also gezeigt, dass $k' \geq k$ ist, aber wir wissen bereits, dass $k' \leq k$ ist. Daher muss in jedem Schritt Gleichheit gelten. Insbesondere müssen $c_M = 3|M|$, $c_J + \frac{1}{2}c_{\text{vertikal}} = |E| - 1$, $c_{\text{andere}} = 0$ und $|M| + \frac{1}{2}c_{\text{vertikal}} = 0$ sein.

Da $|M| + \frac{1}{2}c_{\text{vertikal}} = 0$ ist, muss sowohl $|M|$ als auch c_{vertikal} gleich 0 sein. Daraus folgt außerdem $c_m = |M| = 0$. Insgesamt haben wir also gezeigt, dass $c_E = |E|$, $c_Z = |Z|$, $c_J = |E| - 1$ und $c_M = c_{\text{vertikal}} = c_{\text{andere}} = 0$ sind.

6.8 Schritt 4: Weitere Einschränkung der möglichen Züge

In diesem Abschnitt werden wir, wie in der Beweisskizze in Abschnitt 6.4 angekündigt, die möglichen Züge in der Zugfolge $m_1, m_2, \ldots, m_{k'}$ weiter einschränken.

Lemma 6.8.1. *Für ein $i \in E$ kann der einzige Zug mit Index $(m + i)$ in der Zugfolge $m_1, m_2, \ldots m_{k'}$ nur eine positive z-Drehung gegen den Uhrzeigersinn sein.*

Beweis. Wir haben bereits gezeigt, dass der Zug eine z-Drehung mit Index $(m + i)$ gegen den Uhrzeigersinn ist. Außerdem wissen wir, dass es sich genau dann um eine positive Drehung handelt, wenn die vier $\pm x$- und $\pm y$-Außenseiten jeweils eine gesamte Rotation von 0° haben. Da wir jetzt zusätzlich gezeigt haben, dass die Zugfolge $m_1, m_2, \ldots m_{k'}$ keine Außenseitenzüge enthält, die gesamte Rotation aller Außenseiten also immer gleich 0° ist, muss es sich bei dem Zug um eine positive z-Drehung gegen den Uhrzeigersinn handeln. □

Lemma 6.8.2. *Für ein $i \in Z$ können die beiden Züge mit Index $(m + i)$ in der Zugfolge $m_1, m_2, \ldots m_{k'}$ nur eine positive z-Drehung im Uhrzeigersinn und eine positive z-Wendung sein.*

Beweis. Dieser Beweise ist analog zum letzten Beweis. □

Lemma 6.8.3. *Wenn m_α und m_β zwei positive E-Züge mit Indizes $(m+i_1)$ und $(m + i_2)$, zwischen denen keine anderen E-Züge stattfinden, sind, dann müssen sich die Bitstrings l_{i_1} und l_{i_2} genau in einem Bit unterscheiden.*

Beweis. Wir haben bereits gesehen, dass es zwischen m_α und m_β mindestens einen J-Zug gibt. Tatsächlich muss es sogar genau einer sein, weil in den $|E| - 1$ Zwischenräumen zwischen den E-Zügen jeweils nur ein J-Zug sein kann.

Aus Korollar 6.7.2 wissen wir, dass zwischen m_α und m_β für jedes $j \in \{1, 2, \ldots, m\}$, für das gilt, dass sich l_{i_1} und l_{i_2} im Bit j unterscheiden, ein J-Zug mit Index j sein muss. Die Bitstrings l_{i_1} und l_{i_2} unterscheiden sich

also höchstens in einem Bit j. Weil die Bitstrings zudem alle unterschiedlich sind, müssen sie sich genau in einem Bit unterscheiden. □

Lemma 6.8.4. *Wenn m_α und m_β zwei positive E-Züge mit Indizes $(m+i_1)$ und $(m+i_2)$, zwischen denen keine anderen E-Züge stattfinden, sind und sich l_{i_1} und l_{i_2} im Bit j unterscheiden, dann muss der eine J-Zug zwischen m_α und m_β ein x-Zug mit Index j sein.*

Beweis. Wir wissen, dass der J-Zug ein Zug mit Index j ist, und wollen zeigen, dass er ein positiver x-Zug mit Index j ist.

Dazu betrachten wir ein Paar von Aufklebern, das sich in der Konfiguration C_b auf der $+y$-Außenseite an den (x,z)-Koordinaten $(j, m+i_1)$ und $(j, m+i_2)$ befindet, und ein Paar von Aufklebern, das sich in der Konfiguration C_b auf der $+z$-Außenseite an den (y,z)-Koordinaten $(j, -(m+i_1))$ und $(j, -(m+i_2))$ befindet. Diese beiden Paare von Aufklebern sind jeweils $(m+i_1, m+i_2, j)$-gekuppelt. Außerdem enthalten beide Paare nach Satz 6.3.4 jeweils Aufkleber zwei verschiedener Farben.

Um von der Konfiguration C_b in die Konfiguration C' zu gelangen, wenden wir die Permutation $m_k \circ m_{k-1} \circ \cdots \circ m_1 \circ a_1$ an. Wir wenden also eine Zugfolge an, die zuerst aus einigen x-Zügen, aus denen sich a_i zusammensetzt, und dann der Zugfolge $m_1, m_2, \ldots, m_k$ besteht. Weil diese Zugfolge keine Außenseitenzüge enthält, sind die einzigen Züge vor m_α in ihr, die die vier Aufkleber bewegen können, positive x-Drehungen mit Index j. Unabhängig davon, wie oft und wie weit diese x-Schicht gedreht wird, befindet sich immer eins der beiden Paare von Aufklebern auf einer der $\pm z$-Außenseiten.

Wir betrachten jetzt nur noch dieses Paar. Der Zug m_α ist ein z-Zug und bewegt deshalb keinen der beiden Aufkleber des Paars. Weil die beiden Aufkleber unterschiedliche Farben haben, können sie in der gelösten Konfiguration C' nicht $(m+i_1, m+i_2, j)$-gekuppelt sein. Da außerdem m_β der einzige andere Zug mit Index $(m+i_1)$ oder $(m+i_2)$ ist, folgt aus Lemma 6.6.1, dass einer der beiden Aufkleber von m_β bewegt werden muss. Damit dies aber der Fall sein kann, muss der einzige J-Zug zwischen m_α und m_β das Paar von Aufklebern von der $\pm z$-Außenseite wegbewegen. Weil dieser J-Zug ein Zug mit Index j ist und die Zugfolge keine Außenseitenzüge enthält, ist die einzige Möglichkeit, dass er ein positiver x-Zug mit Index j ist. □

6.9 Schritt 5: Z ist leer

In diesem Abschnitt werden wir, wie in der Beweisskizze in Abschnitt 6.4 angekündigt, zeigen, dass Z leer ist und damit den Beweis vollenden.

Lemma 6.9.1. *Wenn die Zugfolge $a_1, m_1, m_2, \ldots, m_k$ auf C_b angewendet wird, dann gilt für alle $i \in E$, dass sich die Aufkleber, die sich direkt nach*

dem E-Zug mit Index $(m+i)$ *an den Koordinaten* $z=i$ *und* $1 \leq x \leq n$ *auf der* $+y$*-Außenseite befinden, in der Konfiguration* C_b *an den Koordinaten* $z=i$ *und* $1 \leq -y \leq n$ *auf der* $+x$*-Außenseite befinden.*

Beweis. Es seien $i \in E$ und m_α der E-Zug mit Index $(m+i)$.

Wir betrachten die Aufkleber, die sich direkt nach dem E-Zug mit Index $(m+i)$ an den Positionen mit den Koordinaten $z=i$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden. Diese Aufkleber wurden dorthin durch m_α von den Positionen mit den Koordinaten $z=i$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite bewegt, weil m_α ein positiver Zug mit Index $(m+i)$ ist.

Alle E- und Z-Züge vor m_α beeinflussen nur z-Schichten, deren Index nicht i ist. Alle J-Züge und alle Züge, aus denen sich a_1 zusammensetzt, beeinflussen nur x-Schichten, die nicht die Außenschicht sind, also nicht die x-Außenseite. Kein Zug in $a_1, m_1, m_2, \ldots, m_k$ vor m_α beeinflusst also die Aufkleber mit den Koordinaten $z=i$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite. Die Aufkleber in diesen Positionen direkt vor m_α und in C_b sind also dieselben.

Damit haben wir gezeigt, dass sich die Aufkleber, die sich direkt nach dem E-Zug mit Index $(m+i)$ an den Koordinaten $z=i$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden, in der Konfiguration C_b an den Koordinaten $z=i$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite befinden. □

Lemma 6.9.2. *Wenn die Zugfolge* $a_1, m_1, m_2, \ldots, m_k$ *auf* C_b *angewendet wird, dann gilt für alle* $i \in Z$*, dass sich die Aufkleber, die sich direkt nach dem zweiten Z-Zug mit Index* $(m+i)$ *an den Koordinaten* $z=i$ *und* $1 \leq x \leq n$ *auf der* $+y$*-Außenseite befinden, in der Konfiguration* C_b *an den Koordinaten* $z=i$ *und* $1 \leq -y \leq n$ *auf der* $+x$*-Außenseite befinden.*

Beweis. Es seien $i \in Z$ und m_α und m_β die beiden (positiven) Z-Züge mit Index $(m+i)$ in der Reihenfolge, in der sie in der Zugfolge vorkommen.

Wir betrachten die Aufkleber, die sich direkt nach m_β an den Positionen mit den Koordinaten $z=i$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden. Diese Aufkleber wurden dorthin durch m_β entweder von den Positionen mit den Koordinaten $z=i$ und $1 \leq y \leq n$ auf der $-x$-Außenseite oder von den Positionen mit den Koordinaten $z=i$ und $1 \leq -x \leq n$ auf der $-y$-Außenseite bewegt. Ersteres ist der Fall, wenn m_β eine Drehung im Uhrzeigersinn ist, Zweiteres, wenn m_β eine Wendung ist.

In keinem der beiden Fälle kann einer der Züge zwischen m_α und m_β einen der Aufkleber bewegen, weil diese Züge entweder E- oder Z-Züge, also z-Züge, mit anderen Indizes oder positive J-Züge, also positive x-Züge, mit Indizes zwischen 1 und n. Deshalb waren diese Aufkleber direkt vor m_α an den Positionen mit den Koordinaten $z=i$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite. Da es wieder kein Züge vor m_α gibt, die diese Aufkleber bewegen können, müssen die Aufkleber auch in der Konfiguration C_b in diesen Positionen gewesen sein.

Wir haben also gezeigt, dass sich die Aufkleber, die sich direkt nach dem m_β an den Koordinaten $z = i$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden, in der Konfiguration C_b an den Koordinaten $z = i$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite befinden. □

Satz 6.9.3. *Z ist leer.*

Beweis. Zuerst ist anzumerken, dass E nicht leer sein kann, da die Anzahl der J-Züge ansonsten $|E| - 1 = |\varnothing| - 1 = -1$ wäre.

Für einen Widerspruchsbeweis nehmen wir an, dass es ein $i_1 \in Z$ gäbe. Wir bezeichnen den zweiten Z-Zug mit Index $(m + i_1)$ in der Zugfolge $a_1, m_1, m_2, \ldots, m_k$ als m_α. Es kann nicht sein, dass zwischen m_α und jedem beliebigen E-Zug mindestens ein J-Zug liegt, weil es ansonsten zwei J-Züge gäbe, zwischen denen kein E-Zug liegt. Es muss also einen E-Zug m_β geben, der den Index $(m + i_2)$ hat und zwischen dem und m_α kein J-Zug liegt.

Wir betrachten jetzt, was passiert, wenn die Zugfolge $a_1, m_1, m_2, \ldots, m_k$ auf C_b bis genau nach m_α und m_β angewendet wird. Wir bezeichnen diese Konfiguration als C_{Mitte}. Für jedes $j \in \{1, 2, \ldots, m\}$ sind die Aufkleber in der Konfiguration C_{Mitte} an den (x, z)-Koordinaten $(j, m+i_1)$ und $(j, m+i_2)$ auf der $+y$-Außenseite $(m+i_1, m+i_2, j)$-gekuppelt. Wenn die Zugfolge weiter von C_{Mitte} nach C' ausgeführt wird, kommen keine weiteren Züge mit Index $(m+i_1)$ oder $(m+i_2)$ vor. Diese Aufkleber sind also auch in der Konfiguration C' $(m + i_1, m + i_2, j)$-gekuppelt. Daraus folgt, dass die Aufkleber in jedem Paar jeweils dieselbe Farbe haben.

In der Konfiguration C_{Mitte} müssen die Aufkleber an den Koordinaten $z = i_2$ und $1 \leq x \leq n$ auf der $+y$-Außenseite dasselbe Farbschema, das wir als S bezeichnen, wie die Aufkleber an den Koordinaten $z = i_1$ und $1 \leq x \leq n$ auf der $+y$-Außenseite haben. Die letzten Züge vor Erreichen der Konfiguration C_{mid} sind einige E- und Z-Züge, die m_α und m_β beinhalten. Außerdem bewegt keiner der Züge nach m_α Aufkleber mit der z-Koordinate i_1 und keiner der Züge nach m_β Aufkleber mit der z-Koordinate i_2. Deshalb ist das Farbschema der Aufkleber, die sich direkt nach m_β an den Koordinaten $z = i_2$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden, gleich S. Genauso ist auch das Farbschema der Aufkleber, die sich direkt nach m_α an den Koordinaten $z = i_1$ und $1 \leq x \leq n$ auf der $+y$-Außenseite befinden, gleich S. Aus den Lemmata 6.9.1 und 6.9.2 folgt jetzt, dass die Farbschemata der Aufkleber, die sich in C_b an den Koordinaten $z = i_2$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite befinden, und der Aufkleber, die sich in C_b an den Koordinaten $z = i_1$ und $1 \leq -y \leq n$ auf der $+x$-Außenseite befinden, auch gleich S sind. Dies ist jedoch ein Widerspruch dazu, dass diese beiden Farbschemata in der Konfiguration C_b nach Satz 6.3.4 für $i_1 \neq i_2$ unterschiedlich sind.

Aus diesem Widerspruch folgt, dass ein solches $i_1 \in Z$ nicht existieren kann und Z daher leer ist. □

Dies beendet den Beweis von Satz 6.4.1, der in Abschnitt 6.4 skizziert wurde.

6.10 Fazit

Satz 6.10.1. *STMRC, SQTMRC, GSTMRC und GSQTMRC sind NP-vollständig.*

Beweis. Nach Korollar 6.2.5 und Satz 6.4.1 ist die in Abschnitt 6.1 beschriebene Reduktionsfunktion für STMRC korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch STMRC NP-schwer. Weil STMRC außerdem nach Satz 3.5.1 in NP liegt, ist STMRC NP-vollständig.

Nach Korollar 6.2.4 und Korollar 6.4.5 ist die in Abschnitt 6.1 beschriebene Reduktionsfunktion für SQTMRC korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch SQTMRC NP-schwer. Weil SQTMRC außerdem nach Satz 3.5.1 in NP liegt, ist SQTMRC NP-vollständig.

Nach Korollar 6.2.3 und Korollar 6.4.6 ist die in Abschnitt 6.1 beschriebene Reduktionsfunktion für GSTMRC korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch GSTMRC NP-schwer. Weil GSTMRC außerdem nach Satz 3.5.1 in NP liegt, ist GSTMRC NP-vollständig.

Nach Satz 6.2.2 und Korollar 6.4.7 ist die in Abschnitt 6.1 beschriebene Reduktionsfunktion für GSQTMRC korrekt. Weil CHamPath nach Lemma 4.2.1 NP-schwer ist, ist also auch GSQTMRC NP-schwer. Weil GSQTMRC außerdem nach Satz 3.5.1 in NP liegt, ist GSQTMRC NP-vollständig. □

Kapitel 7

Zusammenfassung und Ausblick

7.1 Zusammenfassung

Wir haben in den Kapiteln 5 und 6 gezeigt, dass die in Kapitel 3 eingeführten Probleme NP-vollständig sind. Das heißt, dass es keinen effizienten Algorithmus gibt, um diese Probleme zu lösen, solange die Komplexitätsklasse P nicht gleich NP ist. Dieses Ergebnis gilt für $n \times n \times 1$ Rubik's Square mit der verwendeten Metrik und $n \times n \times n$ Rubik's Cube mit der STM-Metrik und der SQTM-Metrik unabhängig davon, ob nur die Farben der Aufkleber oder auch die genauen Ursprungspositionen für eine Lösung relevant sind. Es ist also nicht davon auszugehen, dass es in der Zukunft Programme geben wird, die in kurzer Zeit optimale Lösungen für $n \times n \times n$ Rubik's Cube finden können.

7.2 Ausblick

Da wir in dieser Arbeit nur Slice Turns, also Züge einzelner Schichten betrachtet haben, könnte es interessant sein, auch andere Metriken, wie z. B. Wide Turn-basierte Metriken zu betrachten. Wide Turns sind Züge, bei denen beliebig viele benachbarte Schichten in einem Zug bewegt werden, solange eine dieser Schichten eine Außenseite ist. Eventuell lässt sich sogar mit gewissen Einschränkungen zeigen, dass die Probleme für beliebige Metriken NP-vollständig sind.

Der Rubik's Cube ist zwar das bekannteste Drehpuzzle, es gibt aber auch viele ähnliche Drehpuzzles, die z. B. nicht würfelförmig sind. Ein solches Drehpuzzle, für das sich möglicherweise ähnliche Ergebnisse zeigen lassen, ist der dodekaederförmige Megaminx, der sich ähnlich zu einem Rubik's Cube lösen lässt.

Literatur

[Bos20] Siegfried Bosch. *Algebra*. 9th. Springer Spektrum, Berlin, Heidelberg, 2020. ISBN: 978-3-662-61648-2.

[Bot20] Ben Botto. *Implementing an Optimal Rubik's Cube Solver using Korf's Algorithm*. 2020. URL: https://medium.com/@benjamin.botto/implementing-an-optimal-rubiks-cube-solver-using-korf-s-algorithm-bf750b332cf9 (besucht am 2021-12-27).

[Bot21] Ben Botto. *rubiks-cube-cracker*. 2021. URL: https://github.com/benbotto/rubiks-cube-cracker/tree/4.0.0 (besucht am 2021-12-27).

Konferenzversion ESA

[Dem+11] Erik D. Demaine u. a. „Algorithms for Solving Rubik's Cubes". In: *CoRR* abs/1106.5736 (2011). arXiv: 1106.5736. URL: https://arxiv.org/abs/1106.5736.

Konferenzversion STACS

[DER17] Erik D. Demaine, Sarah Eisenstat und Mikhail Rudoy. „Solving the Rubik's Cube Optimally is NP-complete". In: *CoRR* abs/1706.06708 (2017). arXiv: 1706.06708. URL: https://arxiv.org/abs/1706.06708.

[IPS82] Alon Itai, Christos H. Papadimitriou und Jayme Luiz Szwarcfiter. „Hamilton Paths in Grid Graphs". In: *SIAM J. Comput.* 11.4 (1982), S. 676–686. DOI: 10.1137/0211056. URL: https://doi.org/10.1137/0211056.

[MV20] Arne Meier und Heribert Vollmer. *Komplexität von Algorithmen*. 2nd. Lehmanns Media, 2020. ISBN: 978-3-96543-137-9.

Journal? SIAM J. Discr Math?

[Rok+10] Tomas Rokicki u. a. *God's Number is 20*. 2010. URL: https://www.cube20.org/ (besucht am 2021-12-27).

[SW16] Werner Struckmann und Dietmar Wätjen. „Graphentheorie". In: *Mathematik für Informatiker*. 2nd. Springer Vieweg, Berlin, Heidelberg, 2016. Kap. 5, S. 158–192. ISBN: 978-3-662-49870-5.

[WCA21] WCA. *Rankings | World Cube Association*. 2021. URL: https://www.worldcubeassociation.org/results/rankings/333fm/average (besucht am 2021-12-27).