

TECHNISCHE UNIVERSITÄT DORTMUND

Fakultät für Informatik

Lehrstuhl 14 für Software Engineering

BACHELORARBEIT

**Gruppentheorie des  
2×2×2 Zauberwürfels und dessen  
Lösungsalgorithmen**

*Pina Kolling*

Abgabe: Mai 2021

betreut von

Dr. Łukasz CZAJKA

und

M. Sc. Christoph STAHL

10. Mai 2021

# Inhaltsverzeichnis

<b>1 Einleitung</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Struktur . . . . .	2
<b>2 Der <math>2 \times 2 \times 2</math>-Würfel</b>	<b>3</b>
2.1 Terminologie . . . . .	3
2.2 Grundzüge des Würfels . . . . .	5
<b>3 Mathematische Grundlagen</b>	<b>7</b>
3.1 Gruppe . . . . .	7
3.2 Untergruppe . . . . .	9
3.3 Erzeuger und zyklische Gruppe . . . . .	10
3.4 Cayleygraph . . . . .	10
3.5 Gruppenoperation . . . . .	11
3.6 Kommutator . . . . .	12
3.7 Äquivalenzrelation und -klasse . . . . .	12
3.8 Permutationen und Zykelschreibweise . . . . .	14
<b>4 Konfiguration des Würfels</b>	<b>18</b>
4.1 Positionen der Steine im Würfel . . . . .	18
4.2 Ausrichtung der Steine . . . . .	21
4.3 Züge ausführen . . . . .	25
<b>5 Würfel als Gruppe</b>	<b>28</b>
5.1 Gleichheit von Zügen . . . . .	28
5.2 Rotation des Würfels . . . . .	29
5.3 Maximale Anzahl der Rotationen . . . . .	34
5.4 Äquivalenzrelation der Züge . . . . .	35
5.5 Äquivalenzklassen der Züge . . . . .	38
5.6 $2 \times 2 \times 2$ -Zauberwürfel als Gruppe . . . . .	39
5.7 Züge als Gruppenoperation . . . . .	43
5.8 Ordnung der Permutationen . . . . .	44
5.9 Ordnung der Züge . . . . .	50
<b>6 Untergruppen von <math>G_{2 \times 2 \times 2}</math></b>	<b>54</b>
6.1 Beispiel-Untergruppen . . . . .	54

6.2	Erzeuger . . . . .	55
6.3	Durch $FF$ und $RR$ erzeugte Untergruppe . . . . .	56
6.4	Cayleygraph . . . . .	58
<b>7</b>	<b>Valide Konfigurationen des Würfels</b>	<b>60</b>
7.1	Anzahl der validen Würfelkonfigurationen . . . . .	60
7.2	Mächtigkeit von $G_{2 \times 2 \times 2}$ . . . . .	60
7.3	Ausrichtung der Steine (modulo 3) . . . . .	61
<b>8</b>	<b>Lösung des Würfels</b>	<b>64</b>
8.1	Anzahl der 2-Zykel . . . . .	64
8.2	Kommutatoren . . . . .	65
8.3	Lösungsansätze . . . . .	67
8.4	Lösung des Würfels anhand eines Beispiels . . . . .	68
8.5	Muster . . . . .	72
8.6	Schraubendrehermethode . . . . .	73
8.7	Algorithmen für die erste Ebene . . . . .	74
8.8	Algorithmen für die zweite Ebene . . . . .	76
<b>9</b>	<b>Minimale Gruppe</b>	<b>80</b>
9.1	Minimale Grundzüge . . . . .	80
9.2	Minimale Rotation des Würfels . . . . .	81
9.3	Erzeuger und Cayleygraph von $G_{min}$ . . . . .	82
9.4	Äquivalenz der Gruppen . . . . .	82
9.5	Minimaler Lösungsweg . . . . .	84
<b>10</b>	<b>Fazit</b>	<b>87</b>
10.1	Zusammenfassung und Ergebnis . . . . .	87
10.2	Ausblick . . . . .	87
<b>Abbildungsverzeichnis</b>		<b>88</b>
<b>Literatur</b>		<b>91</b>
<b>A</b>	<b>Übergangsfunktionen - Vektor <math>x</math></b>	<b>92</b>
<b>B</b>	<b>Alle Rotationen des Würfels</b>	<b>96</b>
<b>C</b>	<b>Persönliche Korrespondenz mit Jessica Fridrich</b>	<b>98</b>
<b>D</b>	<b>Eidesstattliche Versicherung</b>	<b>99</b>

# 1 Einleitung

Der  $3 \times 3 \times 3$ -Zauberwürfel ist ein mathematisches Drehpuzzle, das 1974 von dem ungarischen Professor Erő Rubik erfunden wurde. Er wollte damit seinen Studenten helfen, dreidimensionale Probleme zu verstehen. Erő Rubik selbst brauchte über einen Monat, um den  $3 \times 3 \times 3$ -Würfel zum ersten Mal zu lösen. Der sogenannte *Rubik's Cube* wurde ab 1980 weltweit verkauft. Die Begeisterung für den Würfel war so groß, dass bereits 1982 die erste Weltmeisterschaft in Budapest stattfand. Der Gewinner war Minh Thai aus den USA, der den Würfel in 22,95 Sekunden löste. [2] Die Zeiten zum Lösen des  $3 \times 3 \times 3$ -Würfels wurden immer wieder unterboten. Im Jahr 2018 löste der Chinesische Yusheng Du den Würfel bei einem Wettbewerb in 3,47 Sekunden und stellte damit einen neuen Weltrekord auf, der bis heute nicht gebrochen wurde [1]. Das Patent für den kleineren  $2 \times 2 \times 2$ -Würfel hat Rubik im Jahr 1981 angemeldet [12]. Dieser Würfel ist Gegenstand dieser Arbeit.

Bis heute sind Kinder und Erwachsene gleichermaßen begeistert von den Zauberwürfeln. Doch die Zauberwürfel sind nicht nur interessante Puzzle zur manuellen Lösung – sie bieten beispielsweise auch die Möglichkeit, sie maschinell mit Bild- und Farberkennung zu lösen. Außerdem können die Würfel als algebraische Strukturen dargestellt werden.

## 1.1 Motivation

Der  $3 \times 3 \times 3$ -Würfel wurde bereits in zahlreichen Arbeiten untersucht [3, 4, 9, 11, 10, 5]. Die *God's Number* – das ist die maximal mögliche Anzahl der nötigen Drehungen zur Lösung – wurde oft berechnet und durch neue Algorithmen verbessert. Die Berechnung der *God's Number* des  $3 \times 3 \times 3$ -Würfels ist wesentlich anspruchsvoller und dadurch auch interessanter als die des  $2 \times 2 \times 2$ -Würfels.

Der  $3 \times 3 \times 3$ -Würfel wurde schon mehrfach als Gruppe dargestellt und untersucht [3, 4, 9], während dies beim  $2 \times 2 \times 2$ -Würfel noch nicht der Fall ist. Ziel dieser Arbeit ist es, das Wissen des  $3 \times 3 \times 3$ -Würfels auf den  $2 \times 2 \times 2$ -Würfel zu übertragen. Der  $2 \times 2 \times 2$ -Würfel hat im Gegensatz zum  $3 \times 3 \times 3$ -Würfel weniger Steine und keine Kantesteine – dadurch ist der kleinere Würfel weniger komplex. Dafür kann der  $2 \times 2 \times 2$ -Würfel aber aufgrund der fehlenden Mittelsteine rotiert werden und so kann die Oberseite beliebig geändert werden. In dieser Arbeit wird das Wissen der Gruppe des  $3 \times 3 \times 3$ -Würfels übertragen und angepasst und somit der  $2 \times 2 \times 2$ -Würfel mithilfe der Gruppentheorie dargestellt.

Wer die Lösungsalgorithmen des  $2 \times 2 \times 2$ -Zauberwürfels selber herleiten möchte, sollte dies vor dem Lesen dieser Arbeit tun, da diese hier teilweise erklärt und genutzt werden.

## 1.2 Struktur

Diese Arbeit setzt sich aus 10 Kapiteln zusammen. Im Folgenden werden die Inhalte und Themen dieser Kapitel aufgelistet.

- 1 In der Einleitung wird eine kurze Übersicht der Geschichte des Würfels gegeben. Außerdem befinden sich hier die Motivation und die Struktur.
- 2 In diesem Kapitel wird der Aufbau des  $2 \times 2 \times 2$ -Würfels und die dazugehörige Terminologie erklärt. Außerdem werden die Grundzüge des Würfels definiert.
- 3 Hier werden die mathematischen Grundlagen erklärt. Dafür werden unter anderem Gruppen und andere algebraische Strukturen definiert und anhand von Beispielen erklärt.
- 4 In dem Kapitel *Konfiguration des Würfels* werden die Positionen der Steine und die Ausrichtung der Steine im Würfel erklärt und auf das mathematische Modell übertragen. Dabei wird die Konfiguration definiert.
- 5 In diesem Kapitel wird die Gruppe des  $2 \times 2 \times 2$ -Würfels beschrieben und die Gleichheit von Zügen definiert. Außerdem werden Äquivalenzrelationen eingeführt, um die Rotationen des Würfels zu realisieren und es wird die Ordnung von Zügen definiert.
- 6 Das Kapitel *Untergruppen* befasst sich mit Beispieluntergruppen, Erzeugern und Cayleygraphen der Gruppe des  $2 \times 2 \times 2$ -Würfels.
- 7 Hier wird die Anzahl der möglichen Würfelkonfigurationen und die Mächtigkeit der Trägermenge der Gruppe des  $2 \times 2 \times 2$ -Würfels berechnet und verglichen.
- 8 In diesem Kapitel werden verschiedene Lösungsansätze und Algorithmen erklärt. Die Lösung des Würfels durch einen Menschen wird anhand eines Beispiels schrittweise erklärt und es findet sich eine allgemeine Anleitung, mit der der  $2 \times 2 \times 2$ -Würfel immer gelöst werden kann.
- 9 Hier wird die Untergruppe mit minimalen Grundzügen beschrieben, die den Würfel vollständig abbildet. Außerdem wird ein Konzept eingeführt, um den optimalen Lösungsweg des Würfels zu berechnen.
- 10 Am Schluss der Arbeit befindet sich die Zusammenfassung, das Ergebnis und der Ausblick.

## 2 Der $2 \times 2 \times 2$ -Würfel

In diesem Kapitel werden die Grundlagen des  $2 \times 2 \times 2$ -Cubes erklärt. Zuerst wird der Aufbau und die Terminologie des Würfels erläutert. Anschließend wird kurz auf die Unterschiede zwischen dem  $2 \times 2 \times 2$ -und dem  $3 \times 3 \times 3$ -Würfel eingegangen. Außerdem werden die sechs Grundzüge des Würfels definiert und erklärt. Darauf basieren alle späteren Algorithmen und die Definition der Gruppe des Würfels.

### 2.1 Terminologie

Die Terminologie und der Aufbau des Würfels sind Grundlagen für die weiteren Kapitel. Im Folgenden wird die Terminologie und der Aufbau des Würfels erklärt.

#### $2 \times 2 \times 2$ -Würfel (auch Zauberwürfel oder *Cube*)

Der Würfel setzt sich aus acht kleineren Würfeln zusammen. In Abbildung 1 ist er links verdreht und rechts im gelösten Zustand zu sehen. Der gelöste Zustand wird als Startkonfiguration bezeichnet. Bei der Startkonfiguration (auch Grundposition, Grundstellung) des  $2 \times 2 \times 2$ -Würfels hat jede Seite 4 Farbflächen derselben Farbe. Bei dem verdrehten Würfel können sich die Steine des Würfels an anderen Positionen befinden und anders ausgerichtet sein.



Abbildung 1: Ungelöster und gelöster  $2 \times 2 \times 2$ -Würfel

#### Eckstein und Farbfläche

Ein  $2 \times 2 \times 2$ -Würfel besteht aus acht Ecksteinen (links in Abbildung 2), die jeweils drei Farbflächen (rechts in Abbildung 2) haben. Ein  $2 \times 2 \times 2$ -Zauberwürfel weist somit 24 Farbflächen auf. Die verschiedenen Farbpaare, die sich im gelösten Zustand jeweils gegenüberliegen, sind weiß und gelb; rot und orange; grün und blau.



Abbildung 2: Eckstein und Farbfläche des Würfels

### Seite

Der  $2 \times 2 \times 2$ -und der  $3 \times 3 \times 3$ -Würfel haben sechs Seiten (bestehend aus jeweils vier Farbflächen) und somit sechs Farben. Die weiße Seite wird üblicherweise als obere Seite bezeichnet. Für den Mechanismus ist die Ausrichtung des Würfels aber nicht relevant.



Abbildung 3: Seite des Würfels

### $3 \times 3 \times 3$ -Würfel

Wesentlich bekannter als der  $2 \times 2 \times 2$ -ist der  $3 \times 3 \times 3$ -Würfel. Er besteht aus 26 Steinen. In Abbildung 4 ist er links ungelöst und rechts in der Startkonfiguration zu sehen.

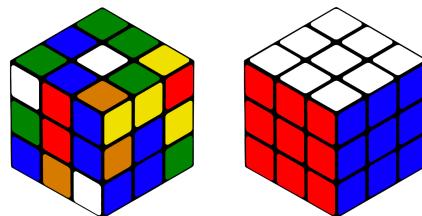


Abbildung 4: Ungelöster und gelöster  $3 \times 3 \times 3$ -Würfel

## Mittel- und Kantsteine

Im Gegensatz zum  $2 \times 2 \times 2$ - hat der  $3 \times 3 \times 3$ -Würfel Kantsteine und Mittelsteine (s. Abbildung 5). Das Besondere an den Mittelsteinen des  $3 \times 3 \times 3$ -Würfels ist, dass sie bei Ebenendrehungen (also bei den Zügen des Würfels) nicht verändert werden. Somit ist beim  $3 \times 3 \times 3$ -Würfel die obere Seite immer identifizierbar: Die obere Seite hat immer das weiße Mittelstück in der Mitte.



Abbildung 5: Kant- und Mittelsteine

Beim  $2 \times 2 \times 2$ -Cube gibt es keine eindeutige Oberseite. Es ist dementsprechend möglich, dass die aktuelle Würfelkonfiguration einer vermeintlich anderen Konfiguration entspricht, bei der jedoch eine andere Seite nach oben gehalten wird. Die Ausrichtung des gesamten Würfels ist bei dem  $3 \times 3 \times 3$ -Würfel also eindeutig vorgegeben, während sie beim  $2 \times 2 \times 2$ -Würfel gedreht werden kann. Dieser Sachverhalt ist entscheidend bei der Übertragung der Gruppentheorie des  $3 \times 3 \times 3$ -Cubes auf den  $2 \times 2 \times 2$ -Würfel. Es wird sich dabei vor allem an *Group Theory an the Rubik's Cube* von Janet Chen [3] und *Group Theory via Rubik's Cube* von Tom Davis [4] orientiert.

## 2.2 Grundzüge des Würfels

Am  $2 \times 2 \times 2$ -Zauberwürfel gibt es sechs verschiedene Drehseiten (auch Ebenen): oben, unten, links, rechts, vorne und hinten. In Abbildung 6 ist die obere Ebene markiert.



Abbildung 6: Ebene des Würfels

---

Abkürzung	Beschreibung des Zuges
-----------	------------------------

---

<i>U</i>	Drehung der <b>oberen</b> Ebene im Uhrzeigersinn
<i>D</i>	Drehung der <b>unteren</b> Ebene im Uhrzeigersinn
<i>R</i>	Drehung der <b>rechten</b> Ebene im Uhrzeigersinn
<i>L</i>	Drehung der <b>linken</b> Ebene im Uhrzeigersinn
<i>F</i>	Drehung der <b>vorderen</b> Ebene im Uhrzeigersinn
<i>B</i>	Drehung der <b>hinteren</b> Ebene im Uhrzeigersinn

---

Die Kürzel stehen für *Up*, *Down*, *Right*, *Left*, *Front*, *Back*. Die entsprechende Ebene wird um  $90^\circ$  im Uhrzeigersinn gedreht, wenn auf diese Ebene geschaut wird. Dementsprechend wirkt es so, als würde die untere Ebene gegen den Uhrzeigersinn gedreht werden, wenn von oben auf den Würfel geschaut wird. So ergibt sich die Menge der Grundzüge:  $\{U, D, R, L, F, B\}$ .

Da der  $2 \times 2 \times 2$ -Würfel im Gegensatz zum  $3 \times 3 \times 3$ -Würfel aber immer lediglich zwei statt drei nebeneinanderliegende Ebenen hat, entspricht eine Drehung der oberen Ebene nach rechts, einer Drehung der unteren Ebene nach links. Auf die Rotationsmöglichkeiten des kompletten Würfels wird in Abschnitt 5.2 genauer eingegangen. Trotzdem werden die Drehungen für jede Ebene definiert. Das ist zwar nicht minimal, dient aber der besseren Anschaulichkeit und Übertragbarkeit der Algorithmen. Eine Drehung der oberen Ebene im Uhrzeigersinn (*U*) beispielsweise entspricht einer Drehung der unteren Ebene im Uhrzeigersinn (*D*) mit anschließender Rotation des kompletten Würfels. Es ist aber übersichtlicher, jede Ebenendrehung als einzelnen Zug darzustellen.

Eine minimale Menge der Grundzüge, die nicht voneinander ableitbar sind, ist  $\{U, R, F\}$ . Die minimale Abbildung des Würfels wird in Kapitel 9 behandelt.

### 3 Mathematische Grundlagen

In diesem Kapitel werden die mathematischen Grundlagen erklärt, die für den weiteren Inhalt dieser Arbeit relevant sind. Es werden Definitionen und Beispiele von Gruppen, Untergruppen, zyklischen Gruppen, Erzeugern, Gruppenoperationen, Kommutatoren, Äquivalenzrelationen, Permutationen und der Zykelschreibweise angegeben. Die genannten Definitionen basieren auf denen von Tobias Glosauer aus dem Buch *Elementar(st)e Gruppentheorie* [8]. Dort finden sich außerdem detailliertere Informationen und weitere Beispiele. Des Weiteren wird der Cayleygraph erklärt.

#### 3.1 Gruppe

##### Definition einer Gruppe

Die Definition einer Gruppe  $(G, \circ)$  ist Grundlage für die folgenden Kapitel.

##### Definition 1 (Gruppe)

Eine Menge  $G$  (auch Trägermenge) mit einer Verknüpfung  $\circ$  wird Gruppe genannt, wenn folgende Bedingungen gelten:

- *Abgeschlossenheit:*  $\forall a, b \in G. (a \circ b) \in G$
- *Assoziativität:*  $\forall a, b, c \in G. (a \circ b) \circ c = a \circ (b \circ c)$
- *Existenz eines neutralen Elements  $n$ :*  $\exists n \in G. \forall a \in G. n \circ a = a \circ n = a$
- *Existenz eines inversen Elements  $a^{-1}$ :*  $\forall a \in G. \exists a^{-1} \in G. a \circ a^{-1} = a^{-1} \circ a = n$

Wenn es sich bei der Gruppe um eine kommutative Gruppe (auch abelsche Gruppe<sup>1</sup>) handelt, muss zusätzlich noch die Eigenschaft der Kommutativität gelten:

##### Definition 2 (Kommutative Gruppe)

Eine Gruppe  $(G, \circ)$  ist eine kommutative Gruppe, wenn gilt:

- *Kommutativität:*  $\forall a, b \in G. (a \circ b) = (b \circ a)$

---

<sup>1</sup> „Zu Ehren von Niels Henrik ABEL (1802-1829); norwegischer Mathematiker und einer der Begründer der Gruppentheorie. Starb leider verarmt und deprimiert im Alter von 26 Jahren an Tuberkulose, kurz bevor er als Anerkennung für seine genialen Arbeiten eine Dozentenstelle in Berlin angeboten bekam.“ [8, S.21, Z.23]

### Beispiel 2.1 (Gruppe)

Zur Veranschaulichung der Gruppdefinition werden hier die natürlichen Zahlen  $\mathbb{N}$  und die ganzen Zahlen  $\mathbb{Z}$  mit dem Operator  $+$  auf die Gruppenaxiome untersucht.

- Die Abgeschlossenheit gilt sowohl für  $(\mathbb{N}, +)$  als auch für  $(\mathbb{Z}, +)$ , da zwei natürliche Zahlen addiert immer eine natürliche Zahl ergeben. Zwei ganze Zahlen addiert ergeben immer eine ganze Zahl.

Beispielsweise sind  $1 + 2 = 3$  und es gilt  $1, 2, 3 \in \mathbb{N}$ .

- Die Verknüpfung ist assoziativ, aufgrund der Definition des Pluszeichens.
- Das neutrale Element von  $(\mathbb{N}, +)$  und  $(\mathbb{Z}, +)$  ist 0. Es gilt also  $\forall n \in \mathbb{N}. n + 0 = 0 + n = n$  (und mit  $\mathbb{Z}$  analog).

Ein Beispiel zur Veranschaulichung:  $3 + 0 = 0 + 3 = 3$

- Die letzte erforderliche Eigenschaft einer Gruppe ist die Existenz eines inversen Elements. Für die Gruppe  $(\mathbb{Z}, +)$  ist  $-z$  das inverse Element für jedes  $z \in \mathbb{Z}$ . Für  $(\mathbb{N}, +)$  gibt es kein inverses Element.

Anhand der oberen Axiome kann nun festgestellt werden, dass  $(\mathbb{Z}, +)$  die Gruppeneigenschaften erfüllt,  $(\mathbb{N}, +)$  aber nicht.  $(\mathbb{Z}, +)$  ist folglich eine Gruppe und  $(\mathbb{N}, +)$  nicht, da kein inverses Element existiert. Es ist aber zu beachten, dass es sich hierbei nicht um formelle Beweise, sondern um anschauliche Beschreibungen handelt. Nun kann  $(\mathbb{Z}, +)$  noch auf die Kommutativität untersucht werden, um zu prüfen, ob es sich um eine abelsche Gruppe handelt.

Da der Plus-Operator als kommutativ definiert ist, ist  $(\mathbb{Z}, +)$  eine abelsche Gruppe.

### Beispiel 2.2 (Gruppe)

Beispiele für endliche Gruppen sind die zyklischen Gruppen der Form  $\mathbb{Z}_{\text{mod } n}$ . Hier wird die Menge für  $n = 6$  mit dem Additionsoperator auf die Gruppeneigenschaften untersucht. Die Elemente der Menge sind dann alle ganzen Zahlen modulo 6, also  $\mathbb{Z}_{\text{mod } 6} = \{0, 1, 2, 3, 4, 5\}$

- Die Abgeschlossenheit gilt für  $(\mathbb{Z}_{\text{mod } 6}, +)$ , da alle Elemente aus  $\mathbb{Z}$  nach der Anwendung von  $\text{mod } 6$  in der Menge  $\{0, 1, 2, 3, 4, 5\}$  liegen.
- Die Verknüpfung ist assoziativ, da das Pluszeichen so definiert ist.
- Das neutrale Element von  $(\mathbb{Z}_{\text{mod } 6}, +)$  ist 0.
- Das Inverse Element für alle  $z \in \mathbb{Z}_{\text{mod } 6}$  ist definiert als  $(6 - z)$ . Für 1 ist es demnach 5, für 2 ist es 4 und für 3 ist das inverse Element die 3.

$(\mathbb{Z}_{\text{mod } 6}, +)$  ist eine endliche Gruppe, da die vier Gruppeneigenschaften erfüllt sind und die Trägermenge  $\mathbb{Z}_{\text{mod } 6}$  endlich ist.

## Mächtigkeit einer Gruppe

Die Mächtigkeit einer Gruppe  $(G, \circ)$  wird auch Gruppenordnung genannt und sagt aus, wie viele Elemente die Menge  $G$  der Gruppe enthält.

### Definition 3 (Mächtigkeit einer Gruppe)

Die Mächtigkeit einer Gruppe  $(G, \circ)$  ist der Betrag der Menge  $G$ , also  $|G|$ .

Wenn  $|G| < \infty$ , wird von einer endlichen Gruppe gesprochen.

### Beispiel 3.1 (Mächtigkeit einer endlichen Gruppe)

Die Mächtigkeit der Gruppe  $(\mathbb{Z}_{\text{mod } 6}, +)$  ist 6. Die Menge  $\mathbb{Z}_{\text{mod } 6}$  enthält die Elemente  $\{0, 1, 2, 3, 4, 5\}$  und somit ist  $|\mathbb{Z}_{\text{mod } 6}| = 6$ .

### Beispiel 3.2 (Mächtigkeit einer unendlichen Gruppe)

Die Mächtigkeit der Gruppe  $(\mathbb{Z}, +)$  ist  $\infty$ , da  $|\mathbb{Z}|$  (abzählbar) unendlich ist.

## 3.2 Untergruppe

Im Folgenden werden Untergruppen definiert.

### Definition 4 (Untergruppe)

Eine Gruppe  $(H, \circ)$  ist eine Untergruppe einer Gruppe  $(G, \circ)$ , wenn  $H \subseteq G$  gilt. Dann wird auch  $(H, \circ) \leqslant (G, \circ)$  geschrieben.

Das Symbol  $\leqslant$  ist zu lesen als *ist Untergruppe von*. Nicht jede Teilmenge  $H \subseteq G$  muss Trägermenge einer Gruppe sein.

Wenn  $(H, \circ)$  eine Untergruppe der Gruppe  $(G, \circ)$  ist, wird  $(G, \circ)$  auch Obergruppe von  $(H, \circ)$  genannt. Jede Gruppe  $(G, \circ)$  mit neutralem Element  $N$  hat die beiden trivialen Untergruppen  $(H_N, \circ)$  mit  $H_N = \{N\}$  und  $(H_G, \circ)$  mit  $H_G = G$ .

### Beispiel 4.1 (keine Untergruppe)

Bei dem oben genannten Beispiel mit  $(\mathbb{N}, +)$  und  $(\mathbb{Z}, +)$  stellt sich heraus, dass  $(\mathbb{Z}, +)$  eine Gruppe ist und  $(\mathbb{N}, +)$  nicht. Obwohl  $\mathbb{N} \subseteq \mathbb{Z}$ , ist  $(\mathbb{N}, +)$  keine Untergruppe von  $(\mathbb{Z}, +)$ , da die Gruppeneigenschaft *Existenz eines inversen Elements* nicht erfüllt sind.

### Beispiel 4.2 (Untergruppe)

Es gilt  $\mathbb{Z}_{\text{mod } 6} \subseteq \mathbb{Z}$ . Da sowohl  $(\mathbb{Z}, +)$ , als auch  $(\mathbb{Z}_{\text{mod } 6}, +)$  Gruppen sind, ist  $(\mathbb{Z}_{\text{mod } 6}, +)$  eine Untergruppe von  $(\mathbb{Z}, +)$ .  $(\mathbb{Z}_{\text{mod } 6}, +)$  und  $(\mathbb{Z}, +)$  wurden im Abschnitt über Gruppen auf die Gruppeneigenschaften untersucht.

## 3.3 Erzeuger und zyklische Gruppe

### Definition 5 (Erzeuger)

Sei die Menge  $M \subseteq G$  eine nicht leere Teilmenge der Trägermenge einer Gruppe  $(G, \circ)$ . Dann wird die Untergruppe  $(M, \circ)$  von  $M$  erzeugt und ist die kleinste Untergruppe von  $(G, \circ)$ , für die  $M \subseteq G$  gilt.  $(M, \circ)$  wird dann Erzeugnis von  $M$  genannt und die Elemente aus  $M$  sind die Erzeuger der Untergruppe  $(M, \circ)$ .

Eine zyklische Gruppe ist eine Gruppe, die von nur einem Element erzeugt wird. Sie besteht ausschließlich aus Potenzen dieses Elementes

### Definition 6 (Zyklische Gruppe)

Sei  $(G, \circ)$  eine Gruppe.  $(G, \circ)$  wird zyklische Gruppe genannt, wenn es ein Element  $a \in G$  gibt, das jedes Element in  $G$  erzeugt. Dann schreibt man auch:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

### Beispiel 6.1 (Erzeuger und zyklische Gruppe)

Ein Beispiel für Erzeuger findet sich anhand der Gruppe der ganzen Zahlen  $(\mathbb{Z}, +)$  und der Addition als Verknüpfung, die bereits als Beispiel der Gruppe beschrieben wurde.

Die Operationen sind hier die Addition und der Übergang von einer Zahl  $z$  zu der negativen Zahl  $-z$ .

Ein Erzeuger dieser Gruppe ist die einelementige Menge  $M = \{1\}$ . Jede positive Zahl  $n$  lässt sich durch die  $n$ -fache Addition von 1 erzeugen und jede negative Zahl durch die Addition von  $((-1) + (-1) \dots)$ .

## 3.4 Cayleygraph

Ein Cayleygraph ist ein Graph, der die Struktur einer Gruppe beschreibt. Er hängt von der Menge der Erzeuger ab und dient dazu, Gruppen bildlich darzustellen. Es handelt sich dabei um einen Graphen mit Knoten, die die verschiedenen Gruppenelemente darstellen.

Pfeile zeigen von einem Element zum nächsten, wenn dies durch einen der Erzeuger erreicht werden kann. [14]

### Beispiel (Cayleygraph)

In Abbildung 7 ist der Cayleygraph der Gruppe  $(\mathbb{Z}_{\text{mod } 6}, +)$  mit dem Erzeuger 1 dargestellt.



Abbildung 7: Cayleygraph von  $(\mathbb{Z}/6\mathbb{Z}, +)$  mit Erzeuger 1

## 3.5 Gruppenoperation

Es gibt Links- und Rechtsoperationen auf Gruppen. Da in dieser Arbeit ausschließlich Rechtsoperationen genutzt werden, beschränkt sich die Definition darauf.

### Definition 7 (Rechtsoperation)

Eine Rechtsoperation einer Gruppe  $(G, \circ)$  auf einer Menge  $M$  ist eine Verknüpfung mit  $m \in M$ ,  $e$  als neutralem Element von  $(G, \circ)$  und  $g, h \in G$ :

$$\cdot : M \times G \rightarrow M \quad (m, g) \mapsto m \cdot g$$

Die folgenden beiden Eigenschaften gelten:

$$m \cdot e = m$$

$$m \cdot (g \circ h) = (m \cdot g) \cdot h$$

Dann operiert  $G$  von rechts auf  $M$ .

### Beispiel 7.1 (Rechtsoperation)

Als Beispiel werden die Gruppe  $(\mathbb{Z}_{\text{mod } 6}, +)$  und die Menge  $\mathbb{Z}$  mit der Verknüpfung  $-$

betrachtet. Die folgenden Eigenschaften gelten, da  $(\mathbb{Z}_{\text{mod } 6}, +)$  eine Rechtsoperation auf  $\mathbb{Z}$  ist, mit  $z \in \mathbb{Z}$  und  $g, h \in \mathbb{Z}_{\text{mod } 6}$ .

- Die Eigenschaft  $z - 0 = z$  ist erfüllt. 0 ist das neutrale Element von  $(\mathbb{Z}_{\text{mod } 6}, +)$ .
- Da sich  $z - (g + h)$  zu  $z - g - h$  umformen lässt, gilt  $z - (g + h) = (z - g) - h$

Demnach operiert  $(\mathbb{Z}_{\text{mod } 6}, +)$  mit  $-$  von rechts auf  $\mathbb{Z}$ .

### 3.6 Kommutator

Die Komplexität eines Kommutators sagt etwas darüber aus, wie stark zwei Elemente einer Gruppe das Kommutativgesetz verletzen. Bei kommutativen Gruppen ist der Kommutator zweier Elemente das neutrale Element der Gruppe [4]. Man sagt dann, dass die beiden Elemente kommutieren.

#### Definition 8 (Kommutator)

Als Kommutator von zwei Elementen  $a, b$  einer Gruppe  $(G, \circ)$  bezeichnet man  $[a, b] = aba^{-1}b^{-1}$ .

#### Beispiel 8.1 (Kommutator)

$[5, 7]$  ist ein Kommutator der Gruppe  $(\mathbb{Z}, +)$ .  $[5, 7]$  entspricht  $5 + 7 - 5 - 7 = 0$  und 0 ist das neutrale Element der Gruppe. Die Gruppe  $(\mathbb{Z}, +)$  ist kommutativ, deshalb ist der Kommutator von allen Elementen der Gruppe 0.

### 3.7 Äquivalenzrelation und -klasse

#### Äquivalenzrelation

Mit Relationen lassen sich Beziehungen von Elementen einer Menge zueinander beschreiben.

#### Definition 9 (Äquivalenzrelation)

Eine Relation  $\sim \subseteq A \times A$  heißt Äquivalenzrelation auf  $A$ , wenn für alle  $x, y, z \in A$  die drei folgenden Eigenschaften gelten: Reflexivität, Symmetrie, Transitivität.

Hier wird  $x \sim y$  als  $x$  ist äquivalent zu  $y$  gelesen. Im Folgenden werden noch die Bedeutungen von Reflexivität, Symmetrie und Transitivität aufgelistet:

$x \sim x$	(Reflexivität)
Aus $(x \sim y)$ folgt $(y \sim x)$ .	(Symmetrie)
Aus $(x \sim y)$ und $(y \sim z)$ folgt $(x \sim z)$ .	(Transitivität)

### Beispiel 9.1 (Relation)

Für die Menge  $A = \{1, 2, 3, 4, 5\}$  wird die Relation  $x < y$  betrachtet:

Bei der Relation  $<$  handelt es sich nicht um eine Äquivalenzrelation, da die Eigenschaft der Reflexivität nicht gilt:  $1 \not< 1$ . Auch die Symmetrie gilt nicht.

### Beispiel 9.2 (Äquivalenzrelation)

Für die Menge  $A = \{1, 2, 3, 4, 5\}$  wird die Relation  $x = y$  betrachtet:

Bei der Relation  $=$  gilt die Reflexivität für alle Elemente, da ein Element immer mit sich selbst identisch ist. Auch die Symmetrie und die Transitivität gelten für die Gleichheit. Somit ist es eine Äquivalenzrelation.

### Beispiel 9.3 (Äquivalenzrelation)

Für die Menge  $A = \{-3, -2, -1, 0, 1, 2, 3\}$  wird die Relation  $x \sim_+ y$  betrachtet, die als  $|x| = |y|$  definiert ist:

Bei der Relation  $\sim_+$  gilt die Reflexivität für alle Elemente, da die Gleichheit reflexiv ist. Auch die Symmetrie und die Transitivität gelten für die Gleichheit mit Betrag. Somit ist es eine Äquivalenzrelation.

## Äquivalenzklasse und Faktormenge

Äquivalenzklassen sind Mengen, die äquivalente Elemente enthalten.

### Definition 10 (Äquivalenzklassen)

Sei  $\sim$  eine Äquivalenzrelation auf der Menge  $M$  und  $x \in M$ . Die Äquivalenzklasse von  $x$  wird dann als  $[x]$  geschrieben und ist definiert als  $\{y \in M \mid y \sim x\} \subseteq M$ .

Jedes Element der Äquivalenzklasse  $[x]$  heißt *Repräsentant von  $[x]$* . Alle Repräsentanten von  $[x]$  sind äquivalent zu  $x$ .

### Beispiel 10.1 (Äquivalenzklassen)

Es wird die Äquivalenzrelation  $x \sim_+ y$ , die als  $|x| = |y|$  definiert ist, auf der Menge  $A = \{-3, -2, -1, 0, 1, 2, 3\}$  betrachtet. Die Äquivalenzklasse von  $[1]$  beispielsweise ist dann  $[1] = \{x \in A \mid x \sim_+ 1\}$ .  $[1]$  enthält dann die Elemente 1 und  $-1$ .

### Definition 11 (Faktormenge)

Die Faktormenge  $M/\sim$  der Menge  $M$  bezüglich der Äquivalenzrelation  $\sim$  besteht aus allen Äquivalenzklassen und ist definiert als  $\{[x] \mid x \in M\}$ .

$M/\sim$  wird als  $M$  modulo  $\sim$  gelesen. Die Elemente von  $M/\sim$  sind Äquivalenzklassen.

### Beispiel 11.1 (Faktormenge)

Es wird wieder die Äquivalenzrelation  $x \sim_+ y$ , die als  $|x| = |y|$  definiert ist, auf der Menge  $A = \{-3, -2, -1, 0, 1, 2, 3\}$  betrachtet.

Die Faktormenge  $A/\sim_+$  enthält dann die Äquivalenzklassen  $[1], [2], [3]$  und  $[0]$ .  $A/\sim_+$  also vier Elemente, während  $A$  sieben Elemente hat.

## 3.8 Permutationen und Zykelschreibweise

Unter einer Permutation versteht man die Vertauschung der Reihenfolge von Objekten.

### Definition 12 (Permutation)

Bei einer  $n$ -elementigen Menge  $M$  ist eine ( $n$ -stellige) Permutation eine bijektive Abbildung  $\pi : M \rightarrow M$ .

Die Zykelschreibweise ist eine kurze Schreibweise für eine Permutation. Die Zykelschreibweise wird nun anhand eines Beispiels erklärt. Die Definition geht über den Rahmen dieser Arbeit hinaus, sie kann aber in dem Buch *Elementar(st)e Gruppentheorie* von Tobias Glosauer [8] nachgelesen werden.

### Beispiel 12.1 (Permutationen und Zykelschreibweise)

Sei  $M$  eine Menge mit fünf Objekten: 1, 2, 3, 4 und 5. Nun können diese Objekte in fünf Plätzen arrangiert werden. Die Plätze werden mit 1 bis 5 nummeriert. Dann kann eine Funktion  $\pi : \{1, 2, 3, 4, 5\} \rightarrow \{1, 2, 3, 4, 5\}$  definiert werden, bei der  $\pi(i)$  die Zahl ist, die in Slot  $i$  liegt. Wenn die Zahlen in der Reihenfolge 5 1 4 3 2 amgeordnet werden, ist 5 auf Platz 1, 1 auf Platz 2, usw. Das ist auch in der folgenden Tabelle zu sehen:

Platz	1	2	3	4	5
Zahl	5	1	4	3	2

Die Funktion  $\pi$  sieht für diese Permutation (s. Tabelle) so aus:

$$\pi(1) = 5 \quad \pi(2) = 1 \quad \pi(3) = 4 \quad \pi(4) = 3 \quad \pi(5) = 2$$

$\pi$  kann auch als eindeutige Zuordnung der Form  $i \mapsto j$  (für  $\pi(i) = j$ ) geschrieben werden, da jede Permutationsfunktion in dieser Form angegeben werden kann [3]:

$$1 \mapsto 5 \quad 2 \mapsto 1 \quad 3 \mapsto 4 \quad 4 \mapsto 3 \quad 5 \mapsto 2$$

Das kann folgendermaßen in der Zyklenschreibweise geschrieben werden:

$$\pi = (1\ 5\ 2)\ (3\ 4)$$

Das wird so gelesen: Die 1 geht auf die 5, die 5 geht auf die 2, die 2 geht wieder auf die 1. Damit ist der erste Zykel geschlossen. Beim zweiten Zykel geht die 3 auf die 4 und die 4 auf die 3.  $\pi$  besteht somit aus zwei Zykeln: ein Zykel hat die Länge drei und der andere die Länge zwei. Die Zykeln sind in Abbildung 8 dargestellt.



Abbildung 8: Zykel  $\pi = (1\ 5\ 2)\ (3\ 4)$

Bei der Zyklenschreibweise ist die Reihenfolge der Elemente ausschlaggebend. Beispielsweise ist  $(1\ 2\ 3)$  nicht das gleiche wie  $(1\ 3\ 2)$ .

Die Identitätspermutation wird als  $\pi = 1$  geschrieben. Dabei werden alle Elemente auf sich selbst abgebildet und die Zykeln bleiben somit unverändert.

### Definition 13 (Anzahl der Permutationen)

Für  $n$  verschiedene Objekte ist die Anzahl der Permutationen  $n!$ .

#### Beispiel 13.1 (Anzahl der Permutationen)

Sei  $M = \{1\ 2\ 3\}$  eine Menge mit drei Elementen. Für das erste Objekt der Permutation gibt es 3 Möglichkeiten der Platzeinname: 1, 2 oder 3. Für das zweite Objekt bleiben dann noch 2 Möglichkeiten (da eine ja bereits im ersten Schritt eliminiert wurde) und danach gibt es nur noch eine Option. Es gibt dann also  $3 \cdot 2 \cdot 1 = 3! = 6$  Permutationsmöglichkeiten.

**Definition 14** (Ordnung von Permutationen)

Die Ordnung einer Permutation ist das kleinste gemeinsame Vielfache der Zyklängen (kurz: *kgV*).

Die Ordnung einer Permutation ist die kleinste Zahl  $n \in \mathbb{N}$ , so dass sich nach  $n$ -facher Ausführung der Permutation die identische Permutation ergibt. Man kann die Ordnung einer Permutation  $\pi$  als  $ord(\pi)$  schreiben.

**Beispiel 14.1** (Ordnung von Permutationen)

Sei die Permutation  $\pi = (1\ 2\ 3)$ . Die Ordnung von  $\pi$  ist 3, da  $\pi$  aus nur einem dreielementigen Zykel besteht.  $\pi \cdot \pi \cdot \pi = (1\ 2\ 3) \cdot (1\ 2\ 3) \cdot (1\ 2\ 3) = (1\ 2\ 3)$

**Beispiel 14.2** (Ordnung von Permutationen)

Sei die Permutation  $\pi = (1\ 5\ 2)\ (3\ 4)$ . Das kleinste gemeinsame Vielfache von 3 und 2 ist 6. Somit hat  $\pi$  die Ordnung 6.

**Definition 15** (Komposition von Permutationen)

Seien  $\pi$  und  $\tau$  zwei  $n$ -stellige Permutationen mit  $n \in \mathbb{N}$ . Die Hintereinanderausführung dieser Permutationen wird als  $\tau \diamond \pi$  geschrieben. Dabei wird zuerst  $\pi$  ausgeführt und das Ergebnis auf  $\tau$  angewendet.

Üblicherweise wird die Komposition von Permutationen mit dem  $\circ$ -Operator geschrieben. Dieser dient in dieser Arbeit bereits als Verknüpfungsoperator der Gruppe des  $2 \times 2 \times 2$ -Würfels. Deshalb wird die Komposition von Permutationen im Verlauf dieser Arbeit mit dem  $\diamond$ -Operator geschrieben.

**Beispiel 15.1** (Komposition von Permutationen)

Seien  $\pi$  und  $\tau$  Permutationen mit  $\pi = (1\ 2)\ (3\ 5)\ (4)$  und  $\tau = (1\ 4\ 3)\ (2\ 5)$ . Die Komposition der Zykel  $\tau \diamond \pi$  ergibt Folgendes:

$$(1\ 4\ 3)\ (2\ 5) \diamond (1\ 2)\ (3\ 5)\ (4) = (1\ 5)\ (2\ 4\ 3)$$

Die Komposition der Permutationen wird im Folgenden schrittweise erklärt. Der Zykel  $(1\ 5)$  ergibt sich folgendermaßen: In der Permutation  $\pi$  geht die 1 auf die 2, in der Permutation  $\tau$  geht die 2 dann auf die 5. Daraus ergibt sich dann der Zykelbeginn  $(1\ 5 \dots)$ . In der Permutation  $\pi$  geht die 5 auf die 3 und die 3 in  $\tau$  auf die 1. Somit ergibt sich dann der Zykel  $(1\ 5)$  für die Komposition der beiden Permutationen. Für den Zykel  $(2\ 4\ 3)$  wird die 2 in  $\pi$  betrachtet. Da sie sich in dem Zykel  $(1\ 2)$  befindet, geht die 2 auf die 1. In  $\tau$

geht die 1 in dem Zykel (1 4 3) auf die 4. Somit ergibt sich (2 4 ...). Die 4 geht in der Permutation  $\pi$  auf sich selbst, da es sich um einen einelementigen Zykel handelt. Die 4 in  $\tau$  geht auf die 3 und es ergibt sich der Zykel (2 4 3 ...). Die 3 bildet in der Permutation  $\pi$  auf die 5 ab und die 5 in  $\tau$  auf die 2. Somit ergibt sich der Zykel (2 4 3). Die Komposition von  $\pi$  und  $\tau$  wird im Folgenden durch Pfeile verdeutlicht:

$$\begin{array}{c} \pi \left\{ \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 5 & 4 & 3 \end{array} \right. \\ \tau \left\{ \begin{array}{ccccc} 2 & 1 & 5 & 4 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 2 & 3 & 1 \end{array} \right. \end{array}$$

## 4 Konfiguration des Würfels

Um mit dem Würfel zu arbeiten, muss festgestellt werden können, in welcher Position er sich befindet. Deshalb wird in diesem Kapitel die Konfiguration des Würfels definiert, bevor der Würfel in Kapitel 5 als Gruppe dargestellt wird. Eine Würfelkonfiguration setzt sich aus zwei Parametern zusammen:

- Position der Ecksteine (angegeben als  $\sigma$ )
- Ausrichtung der Ecksteine (angegeben als  $x$ )

Die Konfiguration des Würfels kann als 2-Tupel geschrieben werden:  $(\sigma, x)$ . In diesem Kapitel wird die Position der Ecksteine als Menge bijektiver Funktionen  $\sigma$  und die Ausrichtung der Ecksteine als Vektor  $x$  definiert. Außerdem wird die Veränderung der Würfelkonfiguration an einem Beispielzug schrittweise erklärt.

### 4.1 Positionen der Steine im Würfel

Die Menge der bijektiven Funktionen  $\sigma$  (für jede Ebenenrotation) enthält Funktionen, die die Übergänge der Würfelsteine darstellen. Die Übergänge beschreiben die Positionsänderung der Steine bei einem Zug. Die Funktion  $\sigma$  bildet jede der Würfelpositionen auf die neue Position ab. Es handelt sich dabei um eine Permutation. Permutationen wurden in Abschnitt 3.8 erklärt.

Die Einteilung der Würfelpositionen ist in den Abbildungen 9 und 10 abgebildet. Die einzelnen Steinpositionen werden mit den Kürzeln benannt, die ihre Position mit *up*, *down*, *right*, *left*, *front* und *back* beschreiben.



Abbildung 9: Namen der Steinpositionen im Würfel



Abbildung 10: Aufgeklappter Würfel mit Namen der Steinpositionen

Jeder Steinposition wird ein einzigartiger Name zugeordnet, um sich darauf zu beziehen. Dabei wird davon ausgegangen, dass die weiße Seite in der Startkonfiguration oben ist und die rote Seite vorne. Die Steinpositionen werden mit 3 Buchstaben beschrieben, die aus den Kürzeln  $u, d, r, l, f, b$  bestehen. Diese Kürzel stehen für *up, down, right, left, front, back*.

Somit heißt die Steinposition oben links beispielsweise *ulf* (für *up, left* und *front*). Jeder Stein bekommt zu dem einen eindeutigen Namen, der seiner Steinposition im gelösten Zustand entspricht. Beispielsweise liegt der Stein *ulf* im gelösten Zustand an der Steinposition *ulf*.

Nun wird zur Veranschaulichung die Permutation  $\sigma_U$  für eine Drehung der oberen Ebene um  $90^\circ$  im Uhrzeigersinn definiert. Grundlagen zu Permutationen und der Zykelschreibweise wurden in Abschnitt 3.8 erklärt. Hier wird  $\sigma_U$  hergeleitet, ausführlich beschrieben und verschiedene Schreibweisen angegeben. Die Herleitung der weiteren Drehungen funktioniert analog. Die Drehung der oberen Ebene ist in Abbildung 11 grafisch dargestellt.

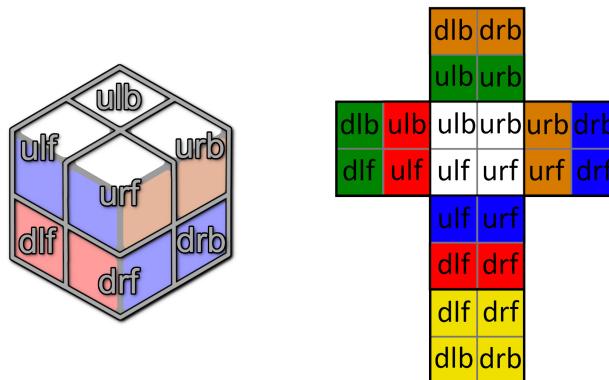


Abbildung 11: Steinpositionen nach Zug  $U$

In Abbildung 11 ist zu sehen, dass die Steine der unteren Ebene nicht bewegt wurden. Die Positionen der oberen Ebene haben sich um einen Stein im Uhrzeigersinn verschoben. Daraus ergeben sich folgende Funktionen  $\sigma_U$ :

$$\begin{array}{llll} \sigma_U(ulf) = ulb & \sigma_U(ulb) = urb & \sigma_U(urb) = urf & \sigma_U(urf) = ulf \\ \sigma_U(dlf) = dlf & \sigma_U(dlb) = dbl & \sigma_U(drb) = drb & \sigma_U(drf) = drf \end{array}$$

Üblich ist auch die Notation der Form  $i \mapsto j$ :

$$\begin{array}{llll} ulf \mapsto ulb & ulb \mapsto urb & urb \mapsto urf & urf \mapsto ulf \\ dlf \mapsto dlf & dbl \mapsto dbl & drb \mapsto drb & drf \mapsto drf \end{array}$$

Daraus entstehen folgende Zykel:  $\sigma_U = (ulf\ ulb\ urb\ urf)(dlf)(dbl)(drb)(drf)$

Einelementige Zykel müssen nicht aufgeschrieben werden. Dann ergibt sich  $\sigma_U = (ulf\ ulb\ urb\ urf)$ , was den Zykel beschreibt, in dem die Steine rotiert werden, wenn die obere Ebene gedreht wird.

Die Drehungen aller Ebenen können durch folgende Zykel beschrieben werden:

$$\begin{aligned} \sigma_U &= (ulf\ ulb\ urb\ urf) \\ \sigma_D &= (dlf\ drf\ drb\ dbl) \\ \sigma_F &= (ulf\ urf\ drf\ dlf) \\ \sigma_B &= (ulb\ dbl\ drb\ urb) \\ \sigma_L &= (ulb\ ulf\ dlf\ dbl) \\ \sigma_R &= (urb\ drb\ drf\ urf) \end{aligned}$$

Die Indizes an den Funktionen  $\sigma$  stehen für die verschiedenen Grundzüge des Würfels. Diese wurden in Abschnitt 2.2 erklärt.

Die Identitätspermutation wird als  $\sigma = 1$  geschrieben. Somit wird der leere Zug folgendermaßen definiert:

$$\sigma_N = 1$$

## 4.2 Ausrichtung der Steine

Der  $2 \times 2 \times 2$ -Würfel besteht aus 8 Ecksteinen, die jeweils 3 Farbflächen haben. Somit hat jeder Stein 3 mögliche Ausrichtungen. Um die Ausrichtung der Steine zu erkennen, bekommen die Würfelpositionen an einer Farbfläche eine Nummer zugeordnet. Dafür werden die weißen und die gelben Seiten markiert und nummeriert. Auf diese Nummern wird sich als  $x_i$  mit  $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$  bezogen - mit  $x_1$  als Position 1,  $x_2$  als Position 2, usw.

Außerdem bekommt jeder Stein an jeder Farbfläche eine Zahluordnung. Da jeder Stein 3 Ausrichtungen haben kann, werden die Farbflächen mit 0, 1 und 2 nummeriert. Die Nummerierung beginnt mit der weißen bzw. gelben Fläche bei 0 und zählt dann im Uhrzeigersinn die Flächen. In der Startkonfiguration sind alle  $x_i = 0$ , der Vektor  $x$  ist dann  $(0, 0, 0, 0, 0, 0, 0, 0)$ . Das wird kurz als  $x = 0$  geschrieben.



Abbildung 12: Ausgeklappter Würfel mit Markierungen für  $x_i$  (links) und Farbflächennummerierungen (rechts)

Im Folgenden wird der Zug  $R$  ausgeführt (s. Abbildung 13) und die Veränderung der Farbflächennummerierung zur Veranschaulichung dargestellt.  $R$  ist eine Drehung der rechten Ebene um  $90^\circ$  im Uhrzeigersinn. Die Kennzeichnungen  $x_{1-8}$  bleiben an der gleichen Position. Die Nummerierungen der Farbflächen ändern sich mit Drehung der Ebene und ermöglichen so eine Zuordnung der Ecksteinausrichtung. Die linke Seite des Würfels wird dabei nicht beeinflusst. Deshalb sind die Flächen an den Positionen  $x_1, x_3, x_5, x_7$  alle 0, da sie der linken Hälfte des Würfels zugeordnet sind. Die anderen Positionen von  $x$  zeigen nun aber andere Farbflächen:

$$x_2 = 2 \quad x_4 = 1 \quad x_6 = 1 \quad x_8 = 2$$

Daher gilt  $x = (0, 2, 0, 1, 0, 1, 0, 2)$  nach dem Zug  $R$ . Das ist auch anhand von Abbildung 13 zu erkennen. Links sind dort die Positionen der Vektoreinträge von  $x$  abgebildet und rechts sieht man den Würfel mit den Farbflächennummerierungen, nachdem der Zug  $R$  ausgeführt wurde.



Abbildung 13: Links: Positionen  $x_1$  bis  $x_8$ , rechts: Veränderung der nummerierten Ecksteine nach dem Zug  $R$

Anhand des Beispielzuges  $R$  kann für jeden Vektoreintrag eine Funktion  $\Gamma_R$  aufgestellt werden, die die Veränderung des Vektors  $x$  nach Ausführen des Zuges  $R$  bei jeder beliebigen Ausgangskonfiguration beschreibt. Da  $x_1, x_3, x_5$  und  $x_7$  nicht beeinflusst werden, bleiben diese unverändert. Der Vektoreintrag, der durch  $\Gamma_R$  in den Folgewert verändert wird, ist im Folgenden schwarz hervorgehoben. Alle anderen Einträge sind ausgegraut.

$$\Gamma_{R_1}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$$

$$\Gamma_{R_3}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = (x_1, x_2, \textcolor{black}{x}_3, x_4, x_5, x_6, x_7, x_8)$$

$$\Gamma_{R_5}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = (x_1, x_2, x_3, x_4, \textcolor{black}{x}_5, x_6, x_7, x_8)$$

$$\Gamma_{R_7}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = (x_1, x_2, x_3, x_4, x_5, x_6, \textcolor{black}{x}_7, x_8)$$

Die Flächen an den Positionen  $x_2, x_4, x_6$  und  $x_8$  werden in Abhängigkeit der vorherigen Steinausrichtungen verändert. Es ergeben sich folgende Funktionen für die Positionen  $x_2, x_4, x_6$  und  $x_8$  nach dem Zug  $R$ :

$$\Gamma_{R_2}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = \begin{cases} (x_1, 2, x_3, x_4, x_5, x_6, x_7, x_8) & \text{falls } x_4 = 0 \\ (x_1, 0, x_3, x_4, x_5, x_6, x_7, x_8) & \text{falls } x_4 = 1 \\ (x_1, 1, x_3, x_4, x_5, x_6, x_7, x_8) & \text{falls } x_4 = 2 \end{cases}$$

Die Funktion  $\Gamma_{R_2}$  verändert den Vektoreintrag  $x_2$  nach Ausführen des Zuges  $R$  in Abhängigkeit des Vektoreintrages  $x_4$ . Die Farbfläche, die durch das Ausführen des Zuges auf die Position  $x_2$  gelangt, steht in direkter Abhängigkeit der Farbfläche an Position  $x_4$ , da es sich dabei um denselben Stein handelt. Wenn sich an der Position  $x_4$  zu Beginn eine Farbfläche mit dem Wert 0 befindet, so wird die Farbfläche mit dem Wert 2 desselben Steines durch Ausführen von  $R$  an die Position  $x_2$  gebracht. Das ist auch in Abbildung 14 zu sehen. Analog funktioniert das mit  $x_4 = 1$  (dann wird  $x_2 = 0$ ) und  $x_4 = 2$  (dann wird  $x_2 = 1$ ).



Abbildung 14: Veränderung von Vektoreintrag  $x_2$  bei Zug  $R$

Die anderen Funktionen für die Veränderung des Vektors  $x$  werden ebenfalls durch die Abhängigkeit der Steinflächen zueinander definiert.

$$\Gamma_{R_4}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = \begin{cases} (x_1, x_2, x_3, 1, x_5, x_6, x_7, x_8) & \text{falls } x_8 = 0 \\ (x_1, x_2, x_3, 2, x_5, x_6, x_7, x_8) & \text{falls } x_8 = 1 \\ (x_1, x_2, x_3, 0, x_5, x_6, x_7, x_8) & \text{falls } x_8 = 2 \end{cases}$$

$$\Gamma_{R_6}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = \begin{cases} (x_1, x_2, x_3, x_4, x_5, 1, x_7, x_8) & \text{falls } x_2 = 0 \\ (x_1, x_2, x_3, x_4, x_5, 2, x_7, x_8) & \text{falls } x_2 = 1 \\ (x_1, x_2, x_3, x_4, x_5, 0, x_7, x_8) & \text{falls } x_2 = 2 \end{cases}$$

$$\Gamma_{R_8}((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) = \begin{cases} (x_1, x_2, x_3, x_4, x_5, x_6, x_7, 2) & \text{falls } x_6 = 0 \\ (x_1, x_2, x_3, x_4, x_5, x_6, x_7, 0) & \text{falls } x_6 = 1 \\ (x_1, x_2, x_3, x_4, x_5, x_6, x_7, 1) & \text{falls } x_6 = 2 \end{cases}$$

Es gibt für den Zug  $R$  acht Funktionen  $\Gamma_R$  – eine für jeden Vektoreintrag. Die Funktionen  $\Gamma_{R_2}$  und  $\Gamma_{R_8}$  verändern verschiedene Vektoreinträge auf die gleiche Weise, die Funktionen  $\Gamma_{R_4}$  und  $\Gamma_{R_6}$  ebenfalls. Auch die Funktionen  $\Gamma_{R_1}, \Gamma_{R_3}, \Gamma_{R_5}$  und  $\Gamma_{R_7}$  arbeiten analog. Da diese Funktionen in Hinblick auf Ein- und Aufgabe gleich aufgebaut sind, reichen drei verschiedene Funktionen für die Veränderung jedes Vektoreintrags aus  $x$  nach dem Zug  $R$  aus.

$$g(x) = \begin{cases} 2 & \text{falls } x = 0 \\ 0 & \text{falls } x = 1 \\ 1 & \text{falls } x = 2 \end{cases} \quad h(x) = \begin{cases} 1 & \text{falls } x = 0 \\ 2 & \text{falls } x = 1 \\ 0 & \text{falls } x = 2 \end{cases} \quad i(x) = x$$

Die Funktionen  $g$  und  $h$  können auch ohne Fallunterscheidung mit modulo 3 geschrieben werden:

$$g(x) = (x + 2) \bmod 3 \quad h(x) = (x + 1) \bmod 3$$

Da  $i$  die Identitätsfunktion ist, kann diese weggelassen werden. Mit den Funktionen  $g$  und  $h$  lassen sich die Ausrichtungen der Steine nach dem Zug  $R$  bestimmen. So wird der Vektor  $x$  nach dem Zug  $R$  durch die Funktion  $\gamma_R$  verändert, die sich aus den Funktionen  $\Gamma_{R_{1-8}}$  zusammensetzt:

$$\begin{aligned} \gamma_R((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, g(x_4), x_3, h(x_8), x_5, h(x_2), x_7, g(x_6)) \end{aligned}$$

Analog dazu gibt es für jeden der sechs Grundzüge eine Funktion  $\gamma$ , die die Veränderung der Steinausrichtung realisiert. Diese Funktionen lassen sich ebenfalls mit den Funktionen  $g$ ,  $h$  und  $i$  bilden.

$$\begin{aligned} \gamma_U((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_3, x_1, x_4, x_2, x_5, x_6, x_7, x_8) \end{aligned}$$

$$\begin{aligned} \gamma_D((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, x_2, x_3, x_4, x_6, x_8, x_5, x_7) \end{aligned}$$

$$\begin{aligned}\gamma_R((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, g(x_4), x_3, h(x_8), x_5, h(x_2), x_7, g(x_6))\end{aligned}$$

$$\begin{aligned}\gamma_L((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (h(x_5), x_2, g(x_1), x_4, g(x_7), x_6, h(x_3), x_8)\end{aligned}$$

$$\begin{aligned}\gamma_F((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, x_2, h(x_7), g(x_3), x_5, x_6, g(x_8), h(x_4))\end{aligned}$$

$$\begin{aligned}\gamma_B((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (g(x_2), h(x_6), x_3, x_4, h(x_1), g(x_5), x_7, x_8)\end{aligned}$$

Bei dem leeren Zug bleibt der Vektor unverändert. Die folgende Funktion ergibt sich:

$$\begin{aligned}\gamma_N((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)\end{aligned}$$

Das oben genannte Beispiel des Zuges  $R$  (s. Abbildung 13) wird nun schrittweise mithilfe von  $\gamma_R$  berechnet. Dafür befindet sich der Würfel zu Beginn in der Startkonfiguration ( $x = (0, 0, 0, 0, 0, 0, 0, 0)$ ). Die Steinposition wird hier nicht berücksichtigt. Wenn der Zug  $R$  ausgeführt wird, wird  $\gamma_R((0, 0, 0, 0, 0, 0, 0, 0))$  berechnet:

$$\begin{aligned}\gamma_R((0, 0, 0, 0, 0, 0, 0, 0)) \\ = (0, g(0), 0, h(0), 0, h(0), 0, g(0)) \\ = (0, 2, 0, 1, 0, 1, 0, 2)\end{aligned}$$

Der Vektor  $x$  lautet nach dem Zug  $R$  von der Startkonfiguration ausgehend:  $(0, 2, 0, 1, 0, 1, 0, 2)$ .

### 4.3 Züge ausführen

Eine Würfelkonfiguration  $C = (\sigma, x)$  wird durch das Ausführen eines Zuges verändert. Die Permutation  $\sigma$  repräsentiert dann die neue Position der Steine im Würfel und der Vektor  $x$  die Ausrichtung der Steine. Ein Zug  $Z$  kann dabei einer der Grundzüge ( $U, D, R, L, F, B$ ) oder eine Aneinanderreihung von Grundzügen sein. Wird ein Zug  $Z$  auf

einer Würfelkonfiguration  $C$  ausgeführt, wird das als  $C \cdot Z$  geschrieben. Das Ergebnis von  $C \cdot Z$  ist dann eine neue Folgekonfiguration  $C'$ .

Die Startkonfiguration  $C = (1, 0)$  wird im folgenden Beispiel durch das dreifache Ausführen des Zuges  $LLFF$  ( $LLFF^3 = LLFFLLFFLLFF$ ) schrittweise verändert. Die Position der Steine – dargestellt durch  $\sigma$  – verändert sich nach dem ersten Ausführen von  $LLFF$  wie folgt:

Zug	ulb	urb	ulf	urf	dlb	drb	dlf	drf
L	ulf	urb	dlf	urf	ulb	drb	dlb	drf
L	dlf	urb	dlb	urf	ulf	drb	ulb	drf
F	ulf	urb	dlb	drf	urf	drb	ulb	dlf
F	urf	urb	dlb	dlf	drf	drb	ulb	ulf

Der neue Vektor  $x$  wird nach dem Teilzug  $LLFF$  durch  $\gamma_F(\gamma_F(\gamma_L(\gamma_L(x))))$  berechnet.

$$\begin{aligned}
\gamma_F(\gamma_F(\gamma_L(\gamma_L(x)))) &\Rightarrow \gamma_F(\gamma_F(\gamma_L(\gamma_L((0, 0, 0, 0, 0, 0, 0, 0, 0, 0))))) \\
&= \gamma_F(\gamma_F(\gamma_L((h(0), 0, g(0), 0, g(0), 0, h(0), 0, 0, 0)))) \\
&= \gamma_F(\gamma_F(\gamma_L((1, 0, 2, 0, 2, 0, 1, 0)))) \\
&= \gamma_F(\gamma_F((h(1), 0, g(2), 0, g(2), 0, h(1), 0))) \\
&= \gamma_F(\gamma_F((0, 0, 0, 0, 0, 0, 0))) \\
&= \gamma_F((0, 0, h(0), g(0), 0, 0, g(0), h(0))) \\
&= \gamma_F((0, 0, 1, 2, 0, 0, 2, 1)) \\
&= (0, 0, h(1), g(2), 0, 0, g(2), h(1)) \\
&= (0, 0, 0, 0, 0, 0, 0)
\end{aligned}$$

Aus dieser Rechnung geht hervor, dass der Vektor nach Ausführen der Drehung  $L$  zu  $(1, 0, 2, 0, 2, 0, 1, 0)$  wird. Wird  $L$  dann nochmal ausgeführt, so ist der Vektor wieder  $(0, 0, 0, 0, 0, 0, 0, 0)$ . Der Würfel ist dann aber nicht gelöst, da die Position der Steine ( $\sigma$ ) verändert ist. Wird nun die Drehung  $F$  zweimal ausgeführt, geht der Vektor über  $(0, 0, 1, 2, 0, 0, 2, 1)$  wieder in  $(0, 0, 0, 0, 0, 0, 0, 0)$  über.

Die Konfiguration  $C'$  nach dem ersten Ausführen des Teilzuges  $LLFF$  ist somit

$$C' = ((ulb\ urf\ dlf)(dlb\ drf\ ulf), (0, 0, 0, 0, 0, 0, 0, 0))$$

oder kurz  $C' = ((ulb\ urf\ dlf)(dlb\ drf\ ulf), 0)$ .

Wenn der Zug  $LLFF$  nun erneut ausgeführt wird, verändert der Vektor  $x$  sich wieder auf die gleiche Weise und wird wieder  $(0, 0, 0, 0, 0, 0, 0, 0)$ . Die Permutation  $\sigma$  der Position ergibt nach dem zweiten Ausführen von  $LLFF$   $(\text{urf dlf ulb})(\text{drf ulf dbl})$ . Die Folgekonfiguration nach dem zweiten Ausführen von  $LLFF$  ist somit

$$C'' = ((\text{dlf urf ulb})(\text{ulf drf dbl}), (0, 0, 0, 0, 0, 0, 0, 0)).$$

Das dritte Ausführen von  $LLFF$  bringt den Würfel wieder in die Ausgangskonfiguration. Die Permutationsfunktion ist dann 1 (die Identität) und der Vektor  $x$  ist wieder  $(0, 0, 0, 0, 0, 0, 0, 0)$ . Die Konfiguration ist dann

$$C''' = (1, 0).$$

Daraus folgt, dass der Zug  $LLFF$  den Würfel nach dreifacher Ausführung wieder in den Ausgangszustand bringt. Darauf wird genauer in Abschnitt 5.8 eingegangen.

## 5 Würfel als Gruppe

In diesem Kapitel wird die Gruppe des  $2 \times 2 \times 2$ -Würfels definiert. Zuerst wird dazu die Rotation des Würfels und die Gleichheit zweier Züge durch Äquivalenzrelationen und Äquivalenzklassen realisiert. Das ist notwendig, damit gleiche Züge in der Trägermenge der Gruppe nicht doppelt vorkommen. Gleiche Züge werden dann durch eine Äquivalenzklasse repräsentiert.

Dann wird die Gruppe des  $3 \times 3 \times 3$ -Cubes [3] auf den  $2 \times 2 \times 2$ -Cube übertragen. Dafür wird die Gruppe des  $2 \times 2 \times 2$ -Würfels auf die vier Gruppenaxiome (Abgeschlossenheit, Assoziativität, Existenz eines neutralen Elements und Existenz eines inversen Elements) untersucht. Außerdem wird geprüft, ob es sich um eine Abelsche Gruppe handelt und dafür die Kommutativität untersucht. Auf der Gruppe des  $2 \times 2 \times 2$ -Würfels wird dann eine Gruppenoperation für das Ausführen von Zügen definiert. Es werden auch die Ordnung von Permutationen und Zügen und die Äquivalenz von Zügen berechnet.

### 5.1 Gleichheit von Zügen

Für den weiteren Verlauf der Arbeit wird  $A_Z$  als die unendliche Menge aller Züge des Würfels definiert. Zwei Züge  $Z_1$  und  $Z_2 \in A_Z$  gelten als gleich, wenn sie mit gleicher Ausgangskonfiguration des Würfels die gleiche Zielkonfiguration hervorrufen. Ein Zug besteht aus einem oder mehreren Grundzügen ( $U, D, F, B, L, R$ ). Das mehrfache Ausführen von Zügen kann mit der Exponentenschreibweise dargestellt werden. So wird beispielsweise  $RR$  (zwei Drehungen der rechten Ebene im Uhrzeigersinn) auch als  $R^2$  geschrieben. Die Exponentenschreibweise kann für alle Züge angewendet werden, auch wenn sie mehr als eine Ebene rotieren. Der Zug  $(LLFF)^2$  beispielsweise entspricht dann  $LLFFLLFF$ .

Ein Beispiel für die Gleichheit von Zügen wird nun genauer betrachtet: Wird eine Ebene viermal hintereinander gedreht, ist der Würfel wieder in der vorherigen Position. Wenn der Würfel in einer Konfiguration  $C = (\sigma, x)$  ist und ein Zug  $Z \in \{U^4, D^4, R^4, L^4, F^4, B^4\}$  ausgeführt wird, ist die Folgekonfiguration wieder  $C$ .

$$\forall Z \in \{U, D, R, L, F, B\} . C \cdot Z^4 = C$$

Das bedeutet, dass jeder Zug  $Z = Z_1 Z_2 Z_3$  mit  $Z_2 \in \{U^4, D^4, R^4, L^4, F^4, B^4\}$  die gleiche Konfiguration wie der Zug  $Z_1 Z_3$  hervorruft. Der Exponent kann in diesem Fall modulo 4

gerechnet werden, da vier Drehungen einer Ebene nacheinander wieder zum Startzustand führen. Es gilt folglich:

$$\forall Z \in \{U, D, F, B, L, R\}, n \in \mathbb{N} . C \cdot Z^n = C \cdot Z^{n \bmod 4}$$

Das gilt, da jede Ebenendrehung ( $U, D, R, L, F$  oder  $B$ ) durch eine Permutationsfunktion  $\sigma$  definiert ist.  $\sigma$  besteht für jeden dieser Grundzüge aus nur einem vierelementigen Zykel. Diese Zyklen wurden in Abschnitt 4.1 definiert. Nach vier Ausführungen eines vierelementigen Zykels befindet sich dieser wieder im Ausgangszustand. Das wird genauer in Abschnitt 5.8 beschrieben. Außerdem muss der Vektor  $x$  für die Ausrichtung der Steine berücksichtigt werden. Dieser Vektor wird durch eine Funktion  $\gamma$  verändert.  $\gamma$  wurde in Abschnitt 4.2 für jeden Grundzug definiert. Der Vektor  $x$  befindet sich immer wieder in seinem Ausgangszustand, wenn die gleiche Funktion  $\gamma$  viermal hintereinander ausgeführt wird. Das wird in Anhang A für alle Grundzüge des Würfels gezeigt.

Für alle  $n$ , die Vielfache von vier sind gilt dann:

$$\forall Z \in \{U, D, F, B, L, R\}, n \in \mathbb{N}, n \bmod 4 = 0 . C \cdot Z^n = C$$

In diesem Fall kann man folgende Umformung durchführen:

$$C \cdot Z^n = C \cdot Z^{n \bmod 4} = C \cdot Z^0 = C$$

$Z^0$  repräsentiert einen leeren Zug. Das entspricht keiner Veränderung der Folgekonfiguration des Würfels.

Da die Anzahl der möglichen Züge ( $|A_Z|$ ) im Gegensatz zur Anzahl der validen Würfelkonfigurationen (s. Kapitel 7) unendlich ist, gibt es unendlich viele Fälle, in denen zwei Züge die gleiche Folgekonfiguration hervorrufen und somit als gleich gelten. Dies wird im weiteren Verlauf dieser Arbeit durch Äquivalenzklassen realisiert. Die Berechnung aller gleichen Züge überschreitet den Rahmen dieser Arbeit – eine Realisierungsmöglichkeit dafür wären Termersetzungssysteme (*Rewriting*).

## 5.2 Rotation des Würfels

Der  $2 \times 2 \times 2$ -Würfel hat im Gegensatz zum  $3 \times 3 \times 3$ -Würfel keine Mittelsteine, die fest darüber entscheiden, wie der Würfel ausgerichtet ist. Der  $2 \times 2 \times 2$ -Würfel kann daher im gelösten Zustand sein, ohne dass die obere Seite weiß ist. Deshalb muss es möglich sein, den Würfel ganz zu rotieren. Das soll im nächsten Abschnitt als Äquivalenzrelation umgesetzt

werden. Dazu werden in diesem Abschnitt die Rotationsmöglichkeiten des Würfels definiert. Um die Drehungen zu benennen, werden die Achsen des Würfels als  $x$ ,  $y$  und  $z$  definiert. Das ist in Abbildung 15 zu sehen. Die vertikale Achse wird  $z$  genannt. Die  $x$ -Achse verläuft von vorne nach hinten durch den Würfel und die  $y$ -Achse von rechts nach links.



Abbildung 15: Würfel mit  $x$ ,  $y$  und  $z$ -Achsen

Mit den Bezeichnungen der Achsen können für die möglichen Rotationen des Würfels Nachfolgekonfigurationen festgelegt werden. Dazu werden zuerst die einzelnen Rotationen des Würfels benannt. Dabei handelt es sich um  $90^\circ$ -Drehungen.

Abkürzung	Beschreibung der Rotation
$Z_l$	Rotation des Würfels um die $z$ -Achse nach links (gegen den Uhrzeigersinn)
$Z_r$	Rotation des Würfels um die $z$ -Achse nach rechts (im Uhrzeigersinn)
$Y_l$	Rotation des Würfels um die $y$ -Achse nach links (gegen den Uhrzeigersinn)
$Y_r$	Rotation des Würfels um die $y$ -Achse nach rechts (im Uhrzeigersinn)
$X_l$	Rotation des Würfels um die $x$ -Achse nach links (gegen den Uhrzeigersinn)
$X_r$	Rotation des Würfels um die $x$ -Achse nach rechts (im Uhrzeigersinn)
$N_R$	keine Rotation des Würfels

Die Rotationen sind zur besseren Anschaulichkeit nicht minimal definiert. Es gibt für jede Würfelseite nur vier Rotationsmöglichkeiten ( $0^\circ$ ,  $90^\circ$ ,  $180^\circ$ ,  $270^\circ$ ), da immer um  $90^\circ$  gedreht wird. Beispielsweise ist  $Z_l$  das gleiche wie  $Z_r^3$ . Das bedeutet, dass eine Drehung des Würfels um  $90^\circ$  nach links äquivalent zu drei  $90^\circ$  Drehungen des Würfels nach rechts ist. Die Drehung nach links entspricht  $0^\circ - 90^\circ = 270^\circ$  während drei Drehungen nach rechts  $0^\circ + 90^\circ + 90^\circ + 90^\circ = 270^\circ$  entsprechen.

Die Steine werden durch eine Rotation alle an einen neuen Platz gebracht. Anders als bei der Drehung der Ebenen, wo eine Auswahl der Steine die Position ändert, ändern hier alle Steine die Position. Die Folgekonfiguration des Würfels nach einer Rotation ist dann eine andere, äquivalente Konfiguration.

Anhand der Rotation  $Z_r$ , also einer Rotation des kompletten Würfels um die  $z$ -Achse um  $90^\circ$  im Uhrzeigersinn, wird nun die Veränderung der Würfelpositionen erläutert. Der Würfel ist in Abbildung 16 nach der Rotation  $Z_r$  abgebildet.



Abbildung 16: Würfel nach Rotation um  $z$ -Achse

Die Permutationsfunktion der Rotationen wird im Folgenden  $\delta$  genannt. Da bei den Rotationen alle Steine die Position wechseln, muss es für jede Rotation 8 Funktionen  $\delta$  geben, für jeden Eckstein eine Funktion:

$$\begin{aligned}\delta_{Z_r}(urf) &= ulf & \delta_{Z_r}(ulf) &= ulb & \delta_{Z_r}(ulb) &= urb & \delta_{Z_r}(urb) &= urf \\ \delta_{Z_r}(drf) &= dlf & \delta_{Z_r}(dlf) &= dbl & \delta_{Z_r}(dbl) &= drb & \delta_{Z_r}(drb) &= drf\end{aligned}$$

Die äquivalente Schreibweise in der Form  $i \mapsto j$  lautet:

$$\begin{array}{llll} urf \mapsto ulf & ulf \mapsto ulb & ulb \mapsto urb & urb \mapsto urf \\ drf \mapsto dlf & dlf \mapsto dbl & dbl \mapsto drb & drb \mapsto drf \end{array}$$

In der Zykel-Schreibweise entspricht die Funktion  $\delta_{Z_r}$  für die Rotation  $Z_r$  dem folgenden Ausdruck:

$$\delta_{Z_r} = ( urf \; ulf \; ulb \; urb ) ( drf \; dlf \; dbl \; drb )$$

Die übrigen Rotationen können ebenfalls durch Funktionen  $\delta$  in der Zykelschreibweise abgebildet werden. Die leere Rotation ist dabei die Identitätspermutation 1. Im Folgenden sind die Funktionen  $\delta$  für alle Rotationen aufgelistet:

$$\begin{aligned}\delta_{Z_r} &= (\textit{ulf ulb urb urf})(\textit{dlf dbl drb drf}) \\ \delta_{Z_l} &= (\textit{ulf urf urb ulb})(\textit{dlf drf drb dbl}) \\ \delta_{Y_r} &= (\textit{ulf ulb dbl dlf})(\textit{urf urb drb drf}) \\ \delta_{Y_l} &= (\textit{ulf dlf dbl ulb})(\textit{urf drf drb urb}) \\ \delta_{X_r} &= (\textit{ulf urf drf dlf})(\textit{urb ulb dbl drb}) \\ \delta_{X_l} &= (\textit{ulf dlf drf urf})(\textit{urb ulb dbl drb}) \\ \delta_{N_R} &= 1\end{aligned}$$

Da die Rotationen die Würfelkonfiguration in eine andere, äquivalente Würfelkonfiguration überführen, muss es neben der Permutationsfunktionen für die Veränderung der Steinposition auch Übergangsfunktionen für den Vektor  $x$  geben, der die Ausrichtung der Steine darstellt. Die Funktionen  $\gamma$  wurden für jeden Zug des Würfels ( $U, D, R, L, F, B$ ) bereits in Abschnitt 4.2 definiert und beschrieben. Die Vektoreinträge der Steinausrichtungen werden dort mit den Funktionen  $g, h$  und  $i$  verändert.

$$g(x) = (x + 2) \bmod 3 \quad h(x) = (x + 1) \bmod 3 \quad i(x) = x$$

Die Überführungsfunktionen des Vektors  $x$  werden im Folgenden  $\beta$  genannt. Für jede der Rotationen gibt es eine Funktion  $\beta$ , die den Vektor in seinen Folgezustand überführt. Die Identitätsfunktion  $i$  muss nicht mit aufgeführt werden. Die Funktionen  $\beta$  für die Rotationen sind im Folgenden definiert:

$$\begin{aligned}\beta_{Z_r} ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ &= (x_3, x_1, x_4, x_2, x_7, x_5, x_8, x_6) \\ \\ \beta_{Z_l} ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ &= (x_2, x_4, x_1, x_3, x_6, x_8, x_5, x_7) \\ \\ \beta_{Y_r} ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ &= (h(x_3), g(x_4), g(x_7), h(x_8), g(x_1), h(x_2), h(x_5), g(x_6))\end{aligned}$$

$$\begin{aligned}\beta_{Y_l} & ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ & = (h(x_5), g(x_6), g(x_1), h(x_2), g(x_7), h(x_8), h(x_3), g(x_4))\end{aligned}$$

$$\begin{aligned}\beta_{X_r} & ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ & = (g(x_5), h(x_1), h(x_7), g(x_3), h(x_6), g(x_2), g(x_8), h(x_4))\end{aligned}$$

$$\begin{aligned}\beta_{X_l} & ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ & = (g(x_2), h(x_6), h(x_4), g(x_8), h(x_1), g(x_5), g(x_3), h(x_7))\end{aligned}$$

Wenn der Würfel nicht rotiert wird, bleibt der Vektor  $x$  unverändert. Die Funktion  $\beta$  für die leere Rotation  $N_R$  ist im Folgenden definiert:

$$\begin{aligned}\beta_{N_R} & ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ & = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)\end{aligned}$$

Es können auch mehrere Rotationen nacheinander ausgeführt werden. Die Funktionen  $\delta$  und  $\beta$  werden dann jeweils verschachtelt. Das erfolgt analog zu dem mehrfachen Ausführen von Zügen (s. Abschnitt 4.3).

Beim Betrachten der Rotationen und der dazugehörigen Funktionen fällt auf, dass die Rotationen auch durch eine Kombination von Zügen definiert werden können. Die Rotationen entsprechen den folgenden Zügen:

$$\begin{aligned}Z_l & \Leftrightarrow DU^{-1} \\ Z_r & \Leftrightarrow D^{-1}U \\ Y_l & \Leftrightarrow LR^{-1} \\ Y_r & \Leftrightarrow L^{-1}R \\ X_l & \Leftrightarrow BF^{-1} \\ X_r & \Leftrightarrow B^{-1}F \\ N_R & \Leftrightarrow N\end{aligned}$$

Jede Rotation kann also durch die Ebenendrehungen von zwei gegenüberliegenden Würfelseiten dargestellt werden.

### 5.3 Maximale Anzahl der Rotationen

Die mehrfache Ausführung einer Rotation wird auch mit der Exponentenschreibweise geschrieben. Somit gilt für jede einelementige Rotation  $T$  und Konfiguration  $C$ :

$$\forall T \in \{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\} . C \cdot TTTT = C \cdot T^4 = C \cdot N_R = C$$

Dabei ist  $N_R$  die leere Rotation und  $T$  ist eine beliebige Rotation des Würfels. Es gilt somit für jede beliebige Rotation  $T$ :

$$T^0 = N_R$$

Jede einelementige Rotation ist durch die Funktionen  $\delta$  und  $\beta$  definiert. Jede dieser Funktionen  $\delta$  besteht in der Zyklenschreibweise aus zwei 4-Zykeln. Diese Zykel befinden sich nach vier Ausführungen wieder in ihrem Ausgangszustand. Darauf wird in Abschnitt 5.8 weiter eingegangen. Außerdem wird bei jeder Rotation der Vektor  $x$  durch eine Funktion  $\beta$  verändert. Der Vektor bleibt nach vierfachem Ausführen von  $\beta$  unverändert. Da alle vierfachen der einelementigen Rotationen ( $Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R$ ) keine Veränderung hervorrufen, kann der Exponent der Rotationen modulo 4 gerechnet werden:

$$\forall T \in \{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\}, n \in \mathbb{N} . C \cdot T^n = C \cdot T^{n \bmod 4}$$

Anhand dieser Aussage ist ersichtlich, dass der Würfel sich nach mehreren Rotationen wieder seiner Ausgangsausrichtung nähern kann. Es gibt für die Rotationen also eine maximale Tiefe, jede weitere Rotation bringt den Würfel wieder näher zu seiner Ausgangsrotation. In diesem Abschnitt wird berechnet, wie oft der Würfel maximal um  $90^\circ$  rotiert werden muss, um zurück in die Ausgangsposition zu gelangen.

Da der Würfel 6 Seiten hat, die jeweils 4 verschiedene Ausrichtungen haben können, gibt es  $4 \cdot 6 = 24$  verschiedene Rotationsmöglichkeiten für den Würfel. In Abbildung 17 sind die vier verschiedenen Ausrichtungen des Würfels zu sehen, wenn die weiße Seite als obere Seite angenommen wird. In den Abbildungen wird von einem gelösten Würfel ausgegangen. Für die anderen fünf Seiten gibt es ebenfalls vier Möglichkeiten der Ausrichtung. Alle Rotationsmöglichkeiten sind in Anhang B in Abbildung 45 dargestellt.



Abbildung 17: Rotationsmöglichkeiten des Würfels mit der weißen Seite oben

Neben den Abbildungen aller Rotationsmöglichkeiten des Würfels, befindet sich in Anhang B eine Verknüpfungstafel, die alle Rotationen und die Verknüpfung dieser abbildet. Anhand dieser vollständigen Darstellung der Rotationsmöglichkeiten kann festgestellt werden, dass der Würfel maximal drei Rotationen von der Ausgangsausrichtung entfernt sein kann. Mit jeder weiteren Rotation nähert er sich seiner vorherigen Ausrichtung wieder an.

## 5.4 Äquivalenzrelation der Züge

Da der  $2 \times 2 \times 2$ -Würfel im Gegensatz zum  $3 \times 3 \times 3$ -Würfel keine eindeutige Ausrichtung hat, werden in diesem Abschnitt Äquivalenzrelationen eingeführt, um die Rotationen des Würfels umzusetzen. Damit eine Relation eine Äquivalenzrelationen ist, müssen die drei folgenden Eigenschaften gelten: Reflexivität, Symmetrie, Transitivität. In Abschnitt 3.7 finden sich Definition und Erklärung.

In dem Fall des  $2 \times 2 \times 2$ -Würfels handelt es sich um eine Relation  $\sim$  von zwei Zügen  $Z_1, Z_2$  aus der Menge aller Züge  $A_Z$  (ohne Rotationen). Dann ist die Relation  $\sim$  eine Teilmenge von  $A_Z \times A_Z$ . Die Relation ist im Folgenden definiert:

$$Z_1 \sim Z_2 := \text{ } Z_1 \text{ und } Z_2 \text{ ergeben (mit optionaler Rotation) die gleiche Würfelkonfiguration}$$

Die Relation  $\sim$  prüft zwei Züge  $Z_1$  und  $Z_2$  auf Gleichheit und berücksichtigt dabei gleichzeitig die Rotation des Würfels.

Daraus ergibt sich folgende Definition mit  $C$  als Würfelkonfiguration und  $W$  als Element (oder Kombination von Elementen) aus  $\{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\}$ . Dabei stellt  $N_R$  die leere Rotation dar – das entspricht keiner Rotation des Würfels.

$$Z_1 \sim Z_2 : \Leftrightarrow C \cdot Z_1 = C \cdot W Z_2$$

Somit ergibt sich beispielsweise  $F \sim L \Leftrightarrow C \cdot F = C \cdot Z_r L$ , da eine Drehung der vorderen Ebene und eine Drehung des Würfels nach links mit einer Drehung der linken Ebene

eine äquivalente Würfelkonfiguration ergeben. Der Würfel ist dann lediglich verschieden ausgerichtet. In Abbildung 18 ist dieses Beispiel grafisch dargestellt: Links befindet sich der gelöste Würfel, in der Mitte der Würfel nach dem Zug  $F$  und rechts der Würfel nach dem Zug  $Z_rL$ . Die beiden rechten Würfel sind in der äquivalenten Konfigurationen, aber anders gedreht.

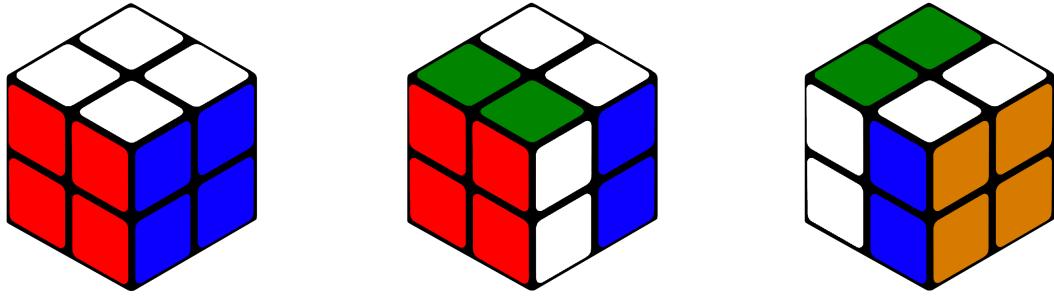


Abbildung 18: Würfel gelöst (links), nach Zug  $F$  (Mitte) und nach  $Z_rL$  (rechts)

Damit  $\sim$  eine Äquivalenzrelation ist, müssen Reflexivität, Symmetrie und Transitivität gelten. Diese Eigenschaften werden im Folgenden für die Relation  $\sim$  gezeigt.

### Reflexivität

Für die Reflexivität muss  $Z \sim Z$  für alle Züge gelten. Jeder Zug muss dafür zu sich selbst in Relation stehen.

$$Z_1 \sim_R Z_2 : \Leftrightarrow C \cdot Z_1 = C \cdot W Z_2$$

Um zu zeigen, dass  $Z_1$  und  $Z_2$  äquivalent sind, wird die Rotation  $W$  als  $N_R$  gewählt, so dass keine Rotation ausgeführt wird.

$$\begin{aligned} Z_1 \sim Z_2 &: \Leftrightarrow C \cdot Z_1 = C \cdot W Z_2 \\ &\Leftrightarrow C \cdot Z_1 = C \cdot N_R Z_2 \\ &\Leftrightarrow C \cdot Z_1 = C \cdot Z_2 \end{aligned}$$

Bei  $Z_1 \sim Z_2$  mit  $W = N_R$  sind die Züge  $Z_1$  und  $Z_2$  immer äquivalent, da sie bei gleicher Startkonfiguration die gleiche Folgekonfiguration des Würfels erzeugen. Es gilt somit die Reflexivität für die Relation  $\sim$ .

## Symmetrie

Für die Symmetrie muss folgendes gelten: Aus  $Z_1 \sim Z_2$  folgt  $Z_2 \sim Z_1$ .

$$\begin{aligned} Z_1 \sim Z_2 &\Rightarrow Z_2 \sim Z_1 \\ \text{mit } Z_1 \sim Z_2 : \Leftrightarrow C \cdot Z_1 &= C \cdot WZ_2 \\ \Leftrightarrow C \cdot Z_1 &= C \cdot W_1 Z_2 \Rightarrow C \cdot Z_2 = C \cdot W_2 Z_1 \end{aligned}$$

$Z_2 \sim Z_1$  muss gelten, wenn  $Z_1 \sim Z_2$  gilt. Da  $Z_1 \sim Z_2$  gilt, sind die Züge  $Z_1$  und  $Z_2$  mit optionaler Rotation gleich.

**Fall 1:** Die optionale Rotation  $W$  entspricht der leeren Rotation  $N_R$ . Dann führen die Züge  $Z_1$  und  $Z_2$  zu derselben Folgekonfiguration des Würfels und werden als gleich angesehen:

$$\begin{aligned} Z_1 \sim Z_2 &\Rightarrow Z_2 \sim Z_1 \text{ mit } W = N_R \\ \Leftrightarrow C \cdot Z_1 &= C \cdot N_R Z_2 \Rightarrow C \cdot Z_2 = C \cdot N_R Z_1 \\ \Leftrightarrow C \cdot Z_1 &= C \cdot Z_2 \Rightarrow C \cdot Z_2 = C \cdot Z_1 \end{aligned}$$

Folglich gilt die Symmetrie für  $W = N_R$ .

**Fall 2:** Die optionale Rotation besteht aus einem oder mehreren Elementen aus  $\{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\}$ . Die Symmetrie gilt, wenn  $W_2$  das Inverse von  $W_1$  ist. Das Inverse einer Rotation ist die Rotation um die gleiche Achse, aber in die andere Richtung. Das Inverse von  $W$  wird als  $W^{-1}$  geschrieben. Da es sich bei den Rotationen (so wie bei den Ebenendrehungen) um  $90^\circ$ -Drehungen handelt, entspricht das inverse Element einer Rotation der dreifachen Ausführung dieser. Es gilt dann:

$$\forall W \in \{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\} . W^{-1} = WWW = W^3$$

Da die Rotationen zur besseren Übersichtlichkeit nicht minimal definiert wurden, sind in der folgenden Tabelle alle Rotationen und die dazugehörigen Inversen abgebildet:

Rotation $W$	$Z_r$	$Z_l$	$Y_r$	$Y_l$	$X_r$	$X_l$
Inverses $W^{-1}$	$Z_l$	$Z_r$	$Y_l$	$Y_r$	$X_l$	$X_r$

Wenn sich eine Rotation aus mehreren Elementen aus  $\{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\}$  zusammensetzt, muss das hintere Element zuerst invertiert werden. Die Defini-

tion ist analog zu der Definition des inversen Elements der Züge aus  $G_{2 \times 2 \times 2}$ . Diese Definition findet sich in Abschnitt 5.6.

Es gilt:

$$C \cdot Z_1 = C \cdot WZ_2 \Rightarrow C \cdot Z_2 = C \cdot W^{-1}Z_1$$

Das gilt, da durch  $W^{-1}$  der Würfel in die entgegengesetzte Richtung rotiert wird und die Züge somit wieder die gleiche Würfelkonfiguration ergeben.

Folglich gilt die Symmetrie für  $\sim$ .

### Transitivität

Es muss gelten: Aus  $Z_1 \sim Z_2$  und  $Z_2 \sim Z_3$  folgt  $Z_1 \sim Z_3$ .

$$\begin{aligned} Z_1 \sim Z_2 & \quad \wedge Z_2 \sim Z_3 & \Rightarrow Z_1 \sim Z_3 \\ \Leftrightarrow C \cdot Z_1 = C \cdot W_1 Z_2 & \wedge C \cdot Z_2 = C \cdot W_2 Z_3 \Rightarrow C \cdot Z_1 = C \cdot W_3 Z_3 \end{aligned}$$

Da die Züge  $Z_1$  und  $Z_2$  mit der Rotation  $W_1$  die gleiche Würfelkonfiguration ergeben, und die Züge  $Z_2$  und  $Z_3$  nach der Rotation  $W_2$  auch die gleiche Würfelkonfiguration ergeben, gilt das auch für die beiden Züge  $Z_1$  und  $Z_3$  nach der Rotation  $W_3 = W_1 W_2$ , da dann alle nötigen Rotationen durchgeführt wurden:

$$C \cdot Z_1 = C \cdot W_1 Z_2 \wedge C \cdot Z_2 = C \cdot W_2 Z_3 \Rightarrow C \cdot Z_1 = C \cdot W_1 W_2 Z_3$$

Die Transitivität gilt somit für die Relation  $\sim$ .

Da die Eigenschaften der Reflexivität, Symmetrie und Transitivität für die Relation  $\sim$  gelten, handelt es sich um eine Äquivalenzrelation.

## 5.5 Äquivalenzklassen der Züge

Äquivalenzklassen und Faktormengen wurden in Abschnitt 3.7 eingeführt. In diesem Abschnitt werden die Äquivalenzklassen der Äquivalenzrelation  $\sim$  auf der Menge aller Züge  $A_Z$  definiert und damit eine Faktormenge gebildet, die diese Äquivalenzklassen enthält. Jede Äquivalenzklasse ist definiert als:

$$[Z] := \{Y \in A_Z \mid Y \sim Z\} \subseteq A_Z$$

Demnach enthält jede Äquivalenzklasse  $[Z]$  alle Züge der Menge  $A_Z$ , die mit der Äquivalenzrelation  $\sim$  äquivalent zu  $Z$  sind. Dabei ist  $[Z]$  eine Teilmenge von  $A_Z$ . Alle äquivalenten Elemente einer Äquivalenzklasse  $[Z]$  werden als Repräsentanten dieser Äquivalenzklasse bezeichnet. So sind die Züge  $R$  und  $RRRRR$  beispielsweise Repräsentanten der Äquivalenzklasse  $[R]$ , da die Züge  $R$  und  $RRRRR$  mit der Äquivalenzrelation  $\sim$  äquivalent zu  $R$  sind.

Die Gleichheit zweier Züge wurde durch die Äquivalenzrelation  $\sim$  definiert. Dabei gelten zwei Züge als äquivalent, wenn sie bei derselben Startkonfiguration mit optionaler Rotation des Würfels zur gleichen Folgekonfiguration führen. Daher sind zwei gleiche Züge  $Z_1, Z_2 \in A_Z$  immer Repräsentanten der gleichen Äquivalenzklasse. Umgekehrt sind zwei Züge  $Z_1, Z_2 \in A_Z$ , die nicht zur gleichen Folgekonfiguration führen, Repräsentanten unterschiedlicher Äquivalenzklassen. Daraus resultiert, dass zwei verschiedene Äquivalenzklassen keine äquivalenten Züge enthalten, da alle äquivalenten Züge in genau einer Äquivalenzklasse sind.

Die Faktormenge  $A_Z / \sim$  wird im weiteren Verlauf der Arbeit  $G_{2 \times 2 \times 2}$  genannt. Sie enthält die Äquivalenzklassen aller Würfelzüge, ohne dabei gleiche Züge oder Würfelrotationen doppelt zu enthalten. Die Elemente von  $G_{2 \times 2 \times 2}$  sind alle Äquivalenzklassen bezüglich der Äquivalenzrelation  $\sim$ . Es gilt demnach:

$$G_{2 \times 2 \times 2} := \{[Z] \mid Z \in A_Z\}$$

$G_{2 \times 2 \times 2}$  enthält somit die Äquivalenzklassen aller möglichen Züge des Würfels. Im weiteren Verlauf dieser Arbeit werden die eckigen Klammern der Äquivalenzklassen in  $G_{2 \times 2 \times 2}$  weggelassen, um die Notation zu vereinfachen.

Zwei Äquivalenzklassen bzw. deren Repräsentanten können durch den Operator  $\circ$  verknüpft werden. Die Züge werden dann nacheinander (von links) ausgeführt. Das Ausführen der Züge erfolgt bei den Äquivalenzklassen der Züge äquivalent zu dem in Abschnitt 4.3 definierten Ausführen von Zügen.

## 5.6 $2 \times 2 \times 2$ -Zauberwürfel als Gruppe

Im Folgenden wird die Definition der Gruppe des  $3 \times 3 \times 3$ -Würfels aus *Group Theory and the Rubik's Cube* von Janet Chen [3] als Gruppe des  $2 \times 2 \times 2$ -Würfels umgesetzt. Die Gruppe des  $2 \times 2 \times 2$ -Würfels heißt im Folgenden  $(G_{2 \times 2 \times 2}, \circ)$ . Grundlagen und Definition der Gruppe wurden in Abschnitt 3.1 erklärt.

Die Trägermenge  $G_{2 \times 2 \times 2}$  der Gruppe wurde in Abschnitt 5.5 definiert. Sie besteht aus den Äquivalenzklassen aller möglichen Zügen des Würfels. Äquivalente Züge sind dabei Repräsentanten der gleichen Äquivalenzklasse.

Der Operator  $\circ$  ist als Konkatenation zweier Züge definiert. Seien  $Z_1$  und  $Z_2$  zwei Züge in  $G_{2 \times 2 \times 2}$ . Dann bedeutet  $Z_1 \circ Z_2$ , dass zuerst  $Z_1$  und dann  $Z_2$  ausgeführt wird.  $Z_1 \circ Z_2$  kann auch als  $Z_1 Z_2$  geschrieben werden.

Im Folgenden wird gezeigt, dass  $(G_{2 \times 2 \times 2}, \circ)$  eine Gruppe ist, indem  $(G_{2 \times 2 \times 2}, \circ)$  bezüglich der Gruppenkriterien untersucht wird:

### Abgeschlossenheit

$$\forall Z_1, Z_2 \in G_{2 \times 2 \times 2} . (Z_1 \circ Z_2) \in G_{2 \times 2 \times 2}$$

Seien  $Z_1$  und  $Z_2$  Züge und somit Elemente aus  $G_{2 \times 2 \times 2}$ . Dann ist auch  $Z_1 \circ Z_2$  ein Element aus  $G_{2 \times 2 \times 2}$ . Die Menge  $G_{2 \times 2 \times 2}$  enthält Äquivalenzklassen. Diese wurden in Abschnitt 5.5 mit den Elementen aus der unendlichen Menge aller Züge  $A_Z$  definiert. Es sind somit alle Elemente der Menge  $A_Z$  Repräsentanten der Äquivalenzklassen in  $G_{2 \times 2 \times 2}$ . Eine Verknüpfung zweier Züge ist auch ein Zug aus  $A_Z$ . Somit ist  $Z_1 \circ Z_2$  ebenfalls Repräsentant einer Äquivalenzklasse in  $G_{2 \times 2 \times 2}$ . Die Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  ist folglich unter dem Operator  $\circ$  abgeschlossen.

Mit den Ergebnissen aus Abschnitt 7.2 kann die Abgeschlossenheit von  $(G_{2 \times 2 \times 2}, \circ)$  auch anders begründet werden: In  $G_{2 \times 2 \times 2}$  findet sich zu jeder validen Würfelkonfiguration ein Zug, mit dem diese erreicht werden kann und jede Verknüpfung von zwei validen Zügen führt zu einer validen Würfelkonfiguration. Daher gilt die Abgeschlossenheit bei der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$ .

### Assoziativität

$$\forall Z_1, Z_2, Z_3 \in G_{2 \times 2 \times 2} . (Z_1 \circ Z_2) \circ Z_3 = Z_1 \circ (Z_2 \circ Z_3)$$

Um die Assoziativität zu zeigen, wird eine Schreibweise für das Ausführen der Züge eingeführt. Ein beliebiger, fester Stein im Würfel wird hier  $s$  genannt. Beim Ausführen eines Zuges  $Z$  wird nun  $Z(s)$  geschrieben, um die neue Position des Steines zu erhalten. Die Positionen sind (wie oben beschrieben) 3-Buchstaben-Kürzel, bestehend aus  $u, d, r, l, f, b$ .

Bei der Betrachtung von  $Z_1 \circ Z_2$ , wird zuerst  $Z_1$  und dann  $Z_2$  ausgeführt.  $Z_1(s)$  bewegt den Stein  $s$  zu der Position  $Z_1(s)$ . Der Zug  $Z_2$  bewegt den Stein dann zu der Position  $Z_2(Z_1(s))$ . Folglich gilt  $Z_1 \circ Z_2 = Z_2(Z_1(s))$ .

Nun muss noch  $(Z_1 \circ Z_2) \circ Z_3 = Z_1 \circ (Z_2 \circ Z_3)$  gezeigt werden. Dafür wird gezeigt, dass sich  $(Z_1 \circ Z_2) \circ Z_3$  und  $Z_1 \circ (Z_2 \circ Z_3)$  beide zu  $Z_3(Z_2(Z_1(s)))$  umformen lassen:

$$\begin{aligned} & (Z_1 \circ Z_2) \circ Z_3 \\ \Leftrightarrow & ((Z_1 \circ Z_2) \circ Z_3)(s) \\ = & Z_3(Z_1 \circ Z_2)(s)) \\ = & Z_3(Z_2(Z_1(s))) \end{aligned}$$

$$\begin{aligned} & Z_1 \circ (Z_2 \circ Z_3) \\ \Leftrightarrow & (Z_1 \circ (Z_2 \circ Z_3))(s) \\ = & (Z_2 \circ Z_3)(Z_1(s)) \\ = & Z_3(Z_2(Z_1(s))) \end{aligned}$$

Somit ist  $(G_{2 \times 2 \times 2}, \circ)$  assoziativ.

### Existenz eines neutralen Elements $N$

$$\exists N \in G_{2 \times 2 \times 2} \forall Z \in G_{2 \times 2 \times 2} . N \circ Z = Z \circ N = Z$$

Das neutrale Element  $N$  muss eine Äquivalenzklasse aus der Menge der Züge  $G_{2 \times 2 \times 2}$  sein. Für alle Züge  $Z \in G_{2 \times 2 \times 2}$  muss gelten:  $N \circ Z = Z \circ N = Z$ . Wird der Zug  $Z$  mit dem neutralen Element  $N$  verknüpft, so bleibt er unverändert. Betrachtet man den physischen Würfel, so ist das neutrale Element der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  der leere Zug. Es werden dabei keine der Ebenen des Würfels gedreht. Wenn ein Zug  $Z$  ausgeführt wird und dann der Zug  $N$ , bedeutet das *erst Z ausführen und dann nichts*, was das gleiche ist wie *Z auszuführen*.

Wenn das auf das mathematischen Modell des Würfels übertragen wird, ändert sich die Würfelkonfiguration durch das Ausführen von  $N$  nicht. Die Permutationsfunktion für das neutrale Element ist dann  $\sigma_N = 1$  und die Übergangsfunktion  $\gamma_N$  des Vektors  $x$  ist  $\gamma_N(x) = x$ . Der Vektor wird dabei unverändert zurückgegeben.

Wird beispielsweise eine einzelne Ebene viermal am Stück gedreht, befindet sich der Würfel wieder in der Ausgangskonfiguration. Somit gilt beispielsweise  $RRRR = R^4 = N$ . Das gilt analog für alle einelementigen Züge des Würfels. Die vierfachen Ausführungen der Grundzüge sind alle als Repräsentanten des leeren Zuges in der Äquivalenzklasse von  $N$  enthalten. Für jeden beliebigen Zug  $Z$  aus  $G_{2 \times 2 \times 2}$  gilt somit auch  $Z^0 = N$ , da die Würfelkonfiguration bei nullfacher Ausführung eines Zuges unverändert bleibt.

Das neutrale Element  $N$  von  $(G_{2 \times 2 \times 2}, \circ)$  ist somit die Äquivalenzklasse des leeren Zuges.

### Existenz eines inversen Elements $Z^{-1}$

$$\forall Z \in G_{2 \times 2 \times 2} \exists Z^{-1} \in G_{2 \times 2 \times 2} . Z \circ Z^{-1} = Z^{-1} \circ Z = N$$

Jeder Zug  $Z$  überführt eine Würfelkonfiguration in eine Folgekonfiguration. Das passiert durch eine Permutationsfunktion  $\sigma$  und eine Übergangsfunktion  $\gamma$  für den Vektor  $x$ . Betrachtet man den physischen Würfel, so wird auffallen, dass man die einzelnen Ebenen auch gegen den Uhrzeigersinn drehen kann und somit eine Ebenendrehung invertiert. Eine Ebenendrehung um  $90^\circ$  gegen den Uhrzeigersinn entspricht einer Ebenendrehung um  $270^\circ$  im Uhrzeigersinn. Die Funktionen  $\sigma$  und  $\gamma$  sind dabei gleich. Die Inversen der einzelnen Ebenendrehungen werden somit folgendermaßen definiert:

$$\forall Z \in \{U, D, F, B, L, R\} . Z^{-1} = ZZZ = Z^3$$

Soll ein Zug invertiert werden, der aus mehreren Grundzügen besteht, so muss das hintere Element zuerst invertiert werden. Bei einem Zug  $Y$  der Länge  $n$  wird zuerst der  $n$ -te Grundzug  $Z_n$  invertiert, indem er in  $Z_n Z_n Z_n$  überführt wird. Daraufhin werden die weiteren Elemente des kompletten Zuges von hinten invertiert. Im Folgenden ist das inverse Element jedes Zuges definiert. Dabei ist  $n \in \mathbb{N}$  und  $Z_i$  repräsentiert alle Teilzüge  $Z_1 - Z_n$ , aus denen sich der Zug  $Y$  zusammensetzt.

$$\begin{aligned} \forall Y \in G_{2 \times 2 \times 2}, Y &= (Z_1 \circ Z_2 \circ \dots \circ Z_n), Z_i \in \{U, D, F, B, L, R\} . \\ Y^{-1} &= {Z_n}^{-1} \circ {Z_{n-1}}^{-1} \circ \dots \circ {Z_1}^{-1} \end{aligned}$$

Das kann mit der oben beschriebenen Definition von  $Z^{-1}$  (mit  $Z \in \{U, D, F, B, L, R\}$ ) folgendermaßen umgeformt werden:

$$\begin{aligned} Y^{-1} &= {Z_n}^{-1} \circ {Z_{n-1}}^{-1} \circ \dots \circ {Z_1}^{-1} \\ &= Z_n Z_n Z_n \circ Z_{n-1} Z_{n-1} Z_{n-1} \circ \dots \circ Z_1 Z_1 Z_1 \\ &= {Z_n}^3 \circ {Z_{n-1}}^3 \circ \dots \circ {Z_1}^3 \\ &= {Z_n}^3 {Z_{n-1}}^3 \dots {Z_1}^3 \end{aligned}$$

Mit diesen Ausdrücken sind die inversen Elemente für jeden Zug aus  $G_{2 \times 2 \times 2}$  definiert.

Somit ist  $(G_{2 \times 2 \times 2}, \circ)$  eine Gruppe, da die vier Gruppenaxiome erfüllt sind.

$(G_{2 \times 2 \times 2}, \circ)$  ist keine kommutative Gruppe, da beispielsweise eine Rotation der rechten Ebene im Uhrzeigersinn ( $R$ ) und eine Rotation der vorderen Ebene im Uhrzeigersinn ( $F$ ) in umgekehrter Reihenfolge ein anderes Ergebnis haben. Dieses Beispiel ist in Abbildung 19 grafisch dargestellt oder kann händisch an einem Würfel ausprobiert werden.

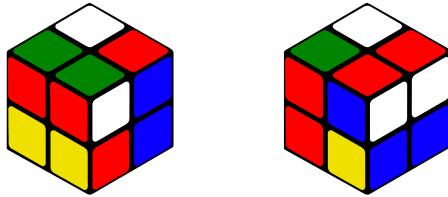


Abbildung 19: Würfel nach Zügen  $FR$ (links) und  $RF$ (rechts)

## 5.7 Züge als Gruppenoperation

Im Folgenden wird eine Gruppenoperation beschrieben, die eine Würfelkonfiguration durch das Ausführen eines Zuges auf eine neue Würfelkonfiguration abbildet. Bei Gruppenoperationen beeinflussen die Elemente einer Gruppe eine Menge. In diesem Fall beeinflussen die Züge des Würfels die Konfiguration des Würfels. Es handelt sich um eine Rechtsoperation, da die Elemente der Gruppe von rechts auf den Elementen der Menge operieren. Die Rechtsoperation wurde in Abschnitt 3.5 definiert.

Bei  $G_{2 \times 2 \times 2}$  handelt es sich um die Trägermenge und  $M_C$  ist die Menge aller Konfigurationen. Der Punktoperator ist im Folgenden definiert:

$$\cdot : M_C \times G_{2 \times 2 \times 2} \rightarrow M_C$$

Wird eine Konfiguration  $C = (\sigma, x)$  aus der Menge der Konfigurationen  $M_C$  durch das Ausführen eines Zuges  $Z \in G_{2 \times 2 \times 2}$  in eine neue Konfiguration überführt, so wird diese Folgekonfiguration als  $(C \cdot Z) \in M_C$  geschrieben. Die folgenden beiden Eigenschaften müssen bei der Rechtsoperation gelten:

$$C \cdot N = C \text{ für alle } C \in M_C \text{ und das neutrale Element } N \in G_{2 \times 2 \times 2}$$

Wenn der leere Zug  $N$  ausgeführt wird, wird die Konfiguration des Würfels nicht verändert. Der leere Zug überführt die Konfiguration mit  $\sigma_N = 1$  und  $\gamma_N(x) = x$ .

Sowohl die Permutationsfunktion  $\sigma$  als auch der Vektor  $x$  bleiben bei Ausführung des leeren Zuges  $N$  unverändert. Daher gilt:

$$\begin{aligned} C \cdot N &\Leftrightarrow (\sigma, x) \cdot N \\ &= (\sigma_N \diamond \sigma, \gamma_N(x)) \\ &= (\sigma, x) \\ &= C \end{aligned}$$

$$C \cdot (Z_1 \circ Z_2) = (C \cdot Z_1) \cdot Z_2 \text{ für alle } Z_1, Z_2 \in G_{2 \times 2 \times 2} \text{ und } C \in M_C$$

Sei  $C$  eine Konfiguration des Würfels. Wird von der Konfiguration  $C$  ausgehend der Zug  $Z_1 \in G_{2 \times 2 \times 2}$  ausgeführt, ist die neue Konfiguration des Würfels  $C \cdot Z_1$ . Wenn nun noch ein weiterer Zug  $Z_2 \in G_{2 \times 2 \times 2}$  ausgeführt wird, ist die neue Konfiguration des Würfels  $(C \cdot Z_1) \cdot Z_2$ . Es wurde demnach mit Konfiguration  $C$  gestartet und die Züge  $Z_1$  und  $Z_2$  wurden ausgeführt. Das kann folgendermaßen umgeformt werden:

$$\begin{aligned} (C \cdot Z_1) \cdot Z_2 & \\ \Leftrightarrow C \cdot Z_1 Z_2 & \\ \Leftrightarrow C \cdot (Z_1 \circ Z_2) & \end{aligned}$$

Die neue Konfiguration kann demnach auch als  $C \cdot (Z_1 \circ Z_2)$  geschrieben werden und somit gilt  $(C \cdot Z_1) \cdot Z_2 = C \cdot (Z_1 \circ Z_2)$ .

Da beide Eigenschaften gelten, handelt es sich um eine Rechtsoperation. Die Züge der Gruppenträgermenge operieren von rechts auf der Menge aller Würfelkonfigurationen.

## 5.8 Ordnung der Permutationen

In den Abschnitten 5.1 und 5.3 wurde folgendes gezeigt:

$$\forall Z \in \{U, D, F, B, L, R\}, n \in \mathbb{N} . C \cdot Z^n = C \cdot Z^{n \bmod 4}$$

$$\forall T \in \{Z_r, Z_l, Y_r, Y_l, X_r, X_l, N_R\}, n \in \mathbb{N} . C \cdot T^n = C \cdot T^{n \bmod 4}$$

Das bedeutet, dass alle Steine des Würfels wieder in ihre vorherige Position gelangen, wenn eine eelementige Ebenen oder Würfelrotation viermal hintereinander ausgeführt wird. Deshalb werden die Grundzüge  $U, D, F, B, L, R$  und die Rotationen  $X_r, X_l, Y_r, Y_l, Z_L, Z_r$  als Permutationen der Ordnung 4 bezeichnet.

Nicht nur die Züge  $U, D, F, B, L, R$  kommen nach dem Wiederholen in den Ausgangszustand. Auch alle anderen Züge bringen den Würfel bei wiederholtem Ausführen wieder in die Ausgangsposition, die der Würfel vor Ausführung des Zuges hatte [4]. Dazu sind je nach Zug verschiedene viele Wiederholungen nötig.

Es ist aber zu beachten, dass dieser Abschnitt lediglich die Ordnung der Permutationen behandelt. Überträgt man dies auf die Würfelkonfiguration, so wird nur die Steinposition  $\sigma$  beachtet. Die Ordnung der Permutationen ist daher die Anzahl der Durchführungen, die benötigt werden, damit alle Steine wieder an der Ausgangsposition sind. Die Ausrichtung der Steine wird hier aber nicht berücksichtigt. Die Ordnung im Bezug auf die komplette Würfelkonfiguration wird in dem Abschnitt 5.9 als *Ordnung der Züge* beschrieben. In diesem Abschnitt wird die Ordnung der Permutation definiert und anhand eines Beispiels beschrieben. Außerdem wird die Zykelstruktur grafisch dargestellt und anschließend ein Algorithmus zur Berechnung der Permutationsordnung eingeführt.

### Beispiel: Ordnung der Permutation

Der Zug  $LF$  beispielsweise hat die Ordnung 15, die Permutation der Steine hat aber die Ordnung 5. Nach 5 Wiederholungen von  $LF$  befinden sich alle Steine wieder an ihrer Ausgangsposition (links in Abbildung 20, von der Startkonfiguration ausgehend). Nach 15 Wiederholungen befindet sich der Würfel wieder in der gleichen Konfiguration, wie vor dem Zug (rechts in Abbildung 20).

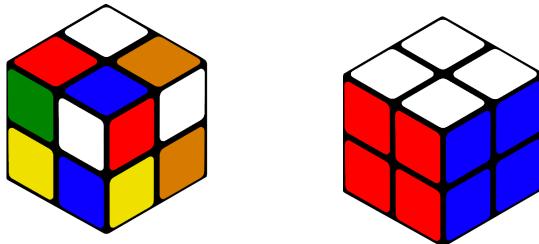


Abbildung 20: Ordnung des Zuges und der Permutation  $LF$

Links in Abbildung 20 ist zu sehen, dass alle Würfelsteine an der jeweiligen Ausgangsposition sind, aber nicht richtig ausgerichtet. Wird auf die Startkonfiguration  $(1, 0)$  der Zug  $(LF)^5$  angewandt, gelangt man zu dieser Folgekonfiguration:

$$(1, 0) \cdot (LF)^5 = (1, (1, 0, 1, 1, 1, 0, 1, 1))$$

Der Würfel ist nach fünf Wiederholungen von  $LF$  nicht gelöst, da die Ausrichtung der Steine verändert ist – der Vektor  $x$  ist nicht 0. Die Ordnung der Permutation von  $LF$  ist 5, da die Funktion  $\sigma$  nach fünffachem Ausführen 1 ist. Die Ordnung des Zuges von  $LF$  ist allerdings 15, da sich der Würfel erst dann wieder in seiner Ausgangskonfiguration befindet. Somit ist die Würfelkonfiguration nach dem Ausführen von  $(LF)^{15}$  auf dem Startzustand wieder  $(1, 0)$ :

$$(1, 0) \cdot (LF)^{15} = (1, 0)$$

Das gilt dann auch für jede andere Startkonfiguration nach Ausführen des Zuges  $(LF)^{15}$ :

$$(\sigma, x) \cdot (LF)^{15} = (\sigma, x)$$

### **Definition: Ordnung einer Permutation**

Die Ordnung einer Permutation ist im Folgenden mathematisch definiert. Dabei ist  $(\sigma, x)$  eine beliebige Würfelkonfiguration.

$$\forall Z \in G_{2 \times 2 \times 2} \exists n \in \mathbb{N} . (\sigma, x) \cdot Z^n = (\sigma, x')$$

Demnach gibt es für jeden beliebigen Zug  $Z$  eine natürliche Zahl  $n$ , die die Ordnung der Permutation des Zuges ist. Wird dieser Zug  $Z$   $n$ -mal ausgeführt, befindet sich die Permutationsfunktion  $\sigma$  wieder im Ausgangszustand. Der Vektor  $x$  wird dabei nicht berücksichtigt.

### **Zykelstruktur**

Die Ordnung einer Permutation lässt sich anhand ihrer Zykelstruktur bestimmen. Zu Beginn dieses Abschnitts wurde die Ordnung einer Permutation bereits definiert und beschrieben. Dabei handelt es sich um die Anzahl der Wiederholungen, die für einen Zug notwendig sind, damit die Steine die gleiche Anordnung wie zu Beginn des Zuges haben. Dabei geht es um die Steinpositionen und nicht um die Steinausrichtungen.

Beispielsweise besteht die Permutationsfunktion  $\sigma_U = (ulf\ ulb\ urb\ urf)$  des Zuges  $U$  (eine Drehung der oberen Ebene um  $90^\circ$  im Uhrzeigersinn) aus genau einem vierelementigen Zykel. Wird der Zug  $U$  viermal ausgeführt, befinden sich die Würfelsteine wieder in ihrer vorherigen Position. In der folgenden Tabelle ist das vierfache Ausführen der Permutation  $\sigma_U$  abgebildet.

Ausführung	ulf	ulb	urb	urf
1	ulb	urb	urf	ulf
2	urb	urf	ulf	ulb
3	urf	ulf	ulb	urb
4	ulf	ulb	urb	urf

Die vierte Zeile der Tabelle hat dieselbe Anordnung der Steine wie die oberste Zeile (vor Ausführung von  $U$ ). Somit hat die Permutation der beschriebenen Ebenenrotation  $U$  die Ordnung 4, da  $\sigma_U$  nach vier Wiederholungen wieder zur Ausgangspermutation führt. Das gilt auch für die anderen einelementigen Züge ( $D, F, B, L, R$ ). Bei jeder Permutation eines Zuges  $Z$ , die aus lediglich einem  $n$ -elementigen Zykel besteht, ist die Ordnung der Permutation  $n$ . Dabei ist  $n$  eine natürliche Zahl  $\mathbb{N}$  und  $(\sigma, x)$  eine beliebige Würfelkonfiguration:

$$\forall Z \in G_{2 \times 2 \times 2} \text{ mit } \sigma_Z = (i_1 \ i_2 \ \dots \ i_n) . (\sigma, x) \cdot Z^n = (\sigma, x')$$

Wenn der Zug  $Z$  mehrfach ausgeführt wird, wird nach jeder  $n$ -ten Wiederholung der Ausgangszustand der Permutationen erreicht. [4] Es gilt folglich auch:

$$\forall Z \in G_{2 \times 2 \times 2} \text{ mit } Z = (i_1 \ i_2 \ \dots \ i_n), n, k \in \mathbb{N} . (\sigma, x) \cdot Z^{k*n} = (\sigma, x')$$

Auch bei komplexeren Permutationen von Zügen, die aus mehr als einem Zykel bestehen, kann anhand der Zykelstruktur die Ordnung bestimmt werden. Dazu muss das *kleinste gemeinsame Vielfache* aller Zykelgrößen bestimmt werden. [4]

Der besseren Übersichtlichkeit halber sind die Züge in Abbildung 21 grafisch dargestellt. Dieser Graph vereinfacht das Ablesen der Zykel, wenn bei einem Zug mehrere Ebenenrotationen kombiniert werden.

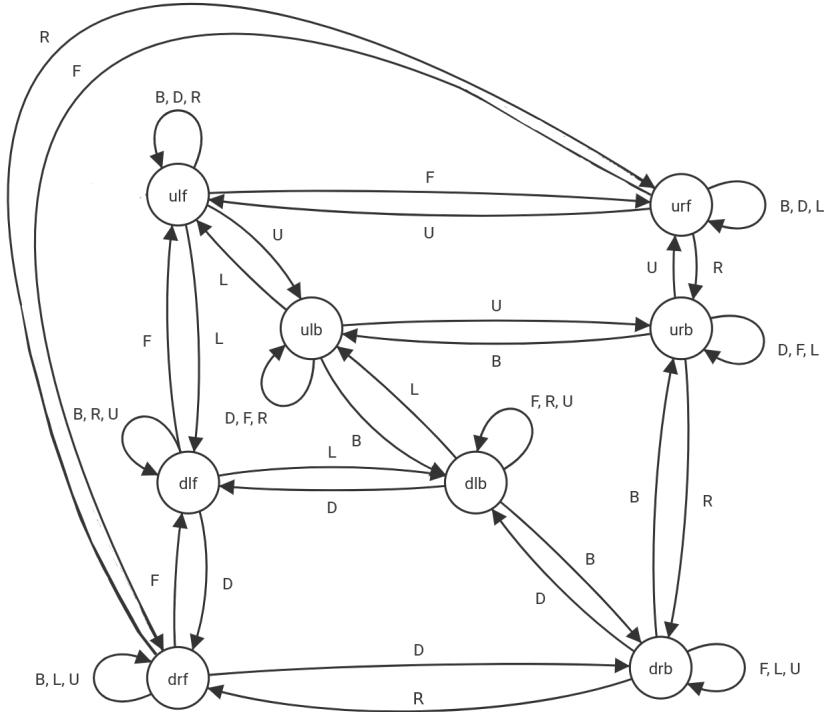


Abbildung 21: Graph aller Zugpermutationen

Mithilfe des Graphen oder der Permutationsfunktionen  $\sigma$  kann nun die Zykelstruktur der Permutationen für den Beispielzug  $LLFF$  dargestellt werden. Dazu wird eine Tabelle erstellt, die zeilenweise jede Position auf ihre neue Position abbildet. Der Zug  $LLFF$  setzt sich aus den Zügen  $L$  und  $F$  zusammen.

Zug	ulb	urb	ulf	urf	dlb	drb	dlf	drf
L	ulf	urb	dlf	urf	ulb	drb	dlb	drf
L	dlf	urb	dlb	urf	ulf	drb	ulb	drf
F	ulf	urb	dlb	drf	urf	drb	ulb	dlf
F	urf	urb	dlb	dlf	drf	drb	ulb	ulf

Die grauen Einträge bleiben bei der jeweiligen Ebenenrotation unverändert. Die Zykel des Zuges  $LLFF$  sind in Abbildung 22 grafisch dargestellt. Dort ist zu sehen, dass  $LLFF$  aus zwei einelementigen und zwei dreielementigen Zyklern besteht.

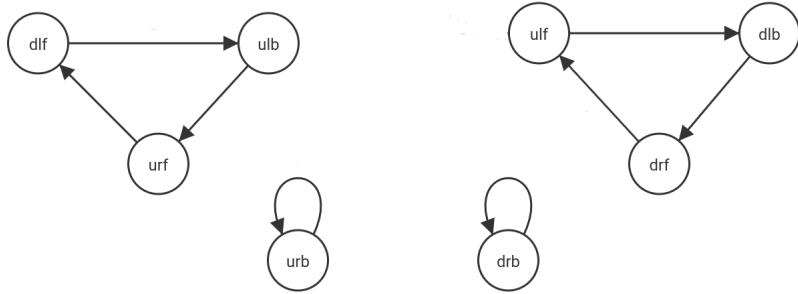


Abbildung 22: Zykel des Zuges  $LLFF$

In der Zykelschreibweise wird der Zug  $LLFF$  somit als  $\sigma_{LLFF} = ( \text{dlf } \text{ulb } \text{urf})( \text{ulf } \text{dlb } \text{drf})$  geschrieben. Da es zwei Zykel der Länge drei gibt, befinden sich alle Würfelsteine nach drei Zügen wieder in ihrer Ausgangsposition:

$$kgV(3, 3, 1, 1) = 3$$

Die Permutation des Zuges  $LLFF$  hat also die Ordnung 3.

Außerdem kann abgelesen werden, dass sechs der acht Steine bei dem Zug  $LLFF$  bewegt werden. Die anderen beiden ( $urb$  und  $drb$ ) bleiben unverändert. Das kann beispielsweise an der grafischen Abbildung der Zykel (22) gesehen werden.

Bei dem Beispielzug  $LLFF$  ist nach dreifacher Ausführung des Zuges nicht ausschließlich die Position der Steine korrekt sondern auch die Ausrichtung. Somit ist die *Ordnung des Zuges* auch 3. Darauf wird genauer in Abschnitt 5.9 eingegangen.

### Algorithmus

Aus diesen Erkenntnissen ergibt sich folgender Algorithmus zur Bestimmung der Ordnung einer Permutation. Als Eingabeparameter wird ein Zug  $Z$  übergeben. Die Rückgabe ist die Permutationsordnung des Zuges  $Z$ .

---

**Algorithmus 1:** Ordnung einer Permutation bestimmen

---

**Data:** Zug  $Z$

**Result:**  $kgVList$  ist die Ordnung der Permutation

```
1  $perm \leftarrow$  Permutationsfunktion von Zug  $Z$ 
2  $list \leftarrow$  leere Liste initialisieren
3  $z \leftarrow$  Anzahl der Zykel von  $perm$ 
4 while  $z > 0$  do
5    $zykel\_length \leftarrow$  Zykellänge von Zykel  $z$ 
6    $list \leftarrow zykel\_length$  hinzufügen
7    $z \leftarrow z-1$ 
8  $kgVList \leftarrow kgV$  von Elementen aus  $list$  berechnen
9 return  $kgVList$ 
```

---

In Zeile 1 wird die Permutationsfunktion des Zuges der Variablen  $perm$  zugewiesen und in Zeile 2 wird eine leere Liste initialisiert, um darin die Längen der einzelnen Zykel zu speichern. Danach wird in Zeile 3 die Anzahl der Zykel ausgelesen und in der Variablen  $z$  gespeichert. Daraufhin wird eine *while*-Schleife  $z$ -mal ausgeführt. In jedem Durchlauf wird die Länge von einem der  $z$  Zykel ausgelesen und in die Liste hinzugefügt. Außerdem wird  $z$  dekrementiert. Nachdem alle Zykellängen in  $list$  gespeichert sind, wird in Zeile 8 das *kleinste gemeinsame Vielfache* der Listenelemente berechnet und der Variablen  $kgVList$  zugewiesen. Dabei handelt es sich um die Ordnung der Permutation und deshalb wird  $kgVList$  in Zeile 9 zurückgegeben.

Die Ordnung der Permutation wird zur Berechnung der Ordnung von Zügen benötigt. Diese wird im folgenden Abschnitt beschrieben und es wird ein Algorithmus zur Berechnung eingeführt.

## 5.9 Ordnung der Züge

In diesem Abschnitt wird gezeigt, dass der Würfel wieder in die Ausgangsposition gelangt, wenn ein beliebiger Zug  $Z \in G_{2 \times 2 \times 2}$  wiederholt auf den Würfel angewendet wird. Das wird in der folgenden Formel dargestellt, dabei ist  $C$  eine beliebige Würfelkonfiguration.

$$\forall Z \in G_{2 \times 2 \times 2} \exists n \in \mathbb{N} . C \cdot Z^n = C$$

Außerdem wird ein Algorithmus zu Berechnung der Ordnung von Zügen beschrieben.

## Beweis

Der folgende Beweis orientiert sich an dem Beweis aus *Group Theory via Rubik's Cube* von Tom Davis [4].

Jedes Mal wenn ein Zug wiederholt wird, werden die Steine im Würfel neu angeordnet und ausgerichtet. Da es eine endliche Anzahl an Würfelkonfigurationen gibt, muss eine Würfelkonfiguration wiederholt werden, wenn ein Zug oft genug durchgeführt wird. Die Zahl der validen Würfelkonfigurationen ist zwar sehr groß, aber endlich (3 674 160). Demnach muss eine Konfiguration wiederholt werden, wenn der Zug häufiger ausgeführt, als es mögliche Würfelkonfigurationen gibt. Die Anzahl der validen Würfelkonfigurationen wird in Kapitel 7 berechnet.

Übertragen auf das mathematische Modell des Würfels bedeutet das folgendes: Bei einem beliebigen Zug  $Z \in G_{2 \times 2 \times 2}$ , der auf eine Konfiguration  $C$  angewandt wird, wird nach wiederholtem Ausführen eine Würfelkonfiguration wiederholt. Wenn die wiederholte Konfiguration  $C'$  zuerst nach  $n \in \mathbb{N}$  Wiederholungen des Zuges  $Z$  auftritt und das zweite Mal nach  $m \in \mathbb{N}$  Wiederholungen, gilt:

$$C' = C \cdot Z^n = C \cdot Z^m \text{ mit } 0 < n < m$$

Da  $n$  und  $m$  das erste Vorkommen einer wiederholenden Konfiguration repräsentieren, gilt dann auch:

$$C \cdot Z^{n-1} \neq C \cdot Z^{m-1}$$

Wenn auf die gleiche Ausgangskonfiguration  $C$   $n$ -mal oder  $m$ -mal der Zug  $Z$  angewandt wird, erreicht man die gleiche Folgekonfiguration  $C'$ . Wird auf diese Folgekonfiguration  $C'$  dann der Zug  $Z^{-1}$  angewandt, ist die Folgekonfiguration  $C'''$  wieder gleich. Dabei ist es irrelevant, ob vorher  $n$ -mal oder  $m$ -mal  $Z$  ausgeführt wurde. Von der gleichen Ausgangskonfiguration ausgehend wird die gleiche Folgekonfiguration erreicht, wenn der gleiche Zug ausgeführt wird. Demnach gilt:

$$\begin{aligned} (C \cdot Z^n) \cdot Z^{-1} &= (C \cdot Z^m) \cdot Z^{-1} \\ \Leftrightarrow C' \cdot Z^{-1} &= C' \cdot Z^{-1} \\ \Leftrightarrow C'' &= C'' \end{aligned}$$

Beim Anwenden von  $Z^{-1}$  auf die Konfiguration  $C'$  wird die letzte Ausführung von  $Z$  wieder rückgängig gemacht, da  $Z^{-1}$  das Inverse des Zuges  $Z$  ist. Wenn der Zug  $Z$   $n$ -mal ausgeführt wird und danach  $Z^{-1}$  ausgeführt wird, ist es das gleiche wie  $n - 1$ -mal  $Z$  auszuführen. Folglich gilt:

$$(C \cdot Z^n) \cdot Z^{-1} = C \cdot (Z^n \circ Z^{-1}) = C \cdot Z^{n-1}$$

Demnach gilt dann :

$$\begin{aligned} (C \cdot Z^n) \cdot Z^{-1} &= (C \cdot Z^m) \cdot Z^{-1} \\ \Leftrightarrow C \cdot Z^{n-1} &= C \cdot Z^{m-1} \end{aligned}$$

Das widerspricht dann aber der Annahme, dass  $m$  der kleinste Wert für eine Wiederholung der Konfiguration ist. In diesem Fall ist  $n-1$  bzw.  $m-1$  die kleinste Anzahl an Ausführungen für eine wiederholende Konfiguration:

$$\begin{aligned} (C \cdot Z^n) \cdot Z^{-1} &= (C \cdot Z^m) \cdot Z^{-1} \\ \Leftrightarrow C \cdot Z^{n-1} &= C \cdot Z^{m-1} \\ \Leftrightarrow C'' &= C'' \end{aligned}$$

Deshalb muss  $n = 0$  sein, damit  $m$  die erste Wiederholung einer Position repräsentiert.

Daraus folgt: Wenn ein Zug wiederholt auf einen Würfel angewendet wird, kommen die Steine wieder in die Ausgangsposition.

## Algorithmus

Es wurde bereits gezeigt, dass sich eine Würfelkonfiguration wiederholt, wenn ein beliebiger Zug wiederholt angewandt wird. Die Anzahl der Wiederholungen eines Zuges, bis der Würfel wieder in der Ausgangskonfiguration ist, nennt man Ordnung eines Zuges. Für die Berechnung dieser wird nun ein Algorithmus entworfen, der als Pseudocode dargestellt wird. Dazu wird der Algorithmus 1 zur Berechnung der Ordnung einer Permutation benötigt.

Der Algorithmus braucht für die Berechnung der Ordnung eines Zuges  $Z$  zwei Eingabeparameter: Den Zug  $Z$  und die Ausgangskonfiguration  $C$  des Würfels. Die Ausgabe ist die Ordnung eines Zuges.

---

**Algorithmus 2:** Ordnung eines Zuges bestimmen

---

**Data:** Konfiguration  $C(\sigma, x)$ , Zug  $Z$   
**Result:**  $kgV(count, ord)$  ist Ordnung eines Zuges

- 1  $ord \leftarrow$  Ordnung der Permutation von  $Z$
- 2  $x' \leftarrow x$
- 3  $count \leftarrow 1$
- 4  $C \leftarrow C \cdot Z^{ord}$
- 5 **while**  $x \neq x'$  **do**
- 6      $C \leftarrow C \cdot Z^{ord}$
- 7      $count \leftarrow count + 1$
- 8 **return**  $kgV(count, ord)$

---

In Zeile 1 wird die Variable  $ord$  mit der Ordnung der Permutationen von  $Z$  initialisiert. Die Berechnung der Permutationsordnung wurde in Abschnitt 5.8 in Algorithmus 1 beschrieben. Dann wird der Startwert des Vektors  $x$  in der Variablen  $x'$  gespeichert, um in der weiteren Berechnung Vergleiche damit durchzuführen (Zeile 2). Außerdem wird in Zeile 3 die Variable  $Count$  mit 1 initialisiert – sie zählt die nötigen Ausführungen des Zuges  $Z$ , bis der Vektor wieder in der Ausgangskonfiguration ist.  $count$  wird mit 1 initialisiert, da vor der *while*-Schleife in Zeile 4 bereits eine Anwendung von  $Z$  durchgeführt wird. Die Anzahl der Ausführung von  $Z$  ist dabei immer  $ord$ , da die Ordnung des Zuges die Ausrichtung der Steine und die Steinposition berücksichtigt. Die Steine sind ausschließlich nach Vielfachen von  $ord$  Zügen an der richtigen Position.

Die *while*-Schleife in Zeile 5 wird ausgeführt, bis  $x$  wieder in der gleichen Konfiguration wie zum Start ist. Bei jeder Ausführung wird  $Z^{ord}$  ausgeführt (Zeile 6) und  $count$  inkrementiert (Zeile 7). Die Ordnung des Zuges  $Z$  setzt sich zusammen aus der Ordnung der Permutation von  $Z$  und der Anzahl der Durchführungen von  $Z^{ord}$ , bis die Ausrichtung der Steine wieder in der Anfangskonfiguration ist. Daher ist die Ordnung eines Zuges das *kleinste gemeinsame Vielfache* von diesen beiden Werten (Zeile 8).

## 6 Untergruppen von $G_{2 \times 2 \times 2}$

Dieses Kapitel behandelt einige der Untergruppen der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$ . Im ersten Teil wird auf die trivialen Untergruppen eingegangen, außerdem werden noch weitere Untergruppen beschrieben. Die Definition und Erklärung der Untergruppe und des Erzeugers findet sich in Abschnitt 3.2. Außerdem werden die Cayleygraphen zu zwei Untergruppen dargestellt und erklärt. Die Cayleygraphen dienen der Veranschaulichung von Gruppenstrukturen. Die Untergruppe, die den  $2 \times 2 \times 2$ -Würfel minimal aber komplett abbildet, findet sich in Kapitel 9.

### 6.1 Beispiel-Untergruppen

Wie bereits in Abschnitt 3.2 erklärt, hat jede Gruppe zwei triviale Untergruppen. Die beiden trivialen Untergruppen von  $(G_{2 \times 2 \times 2}, \circ)$  werden hier  $(H_N, \circ)$  und  $(H_G, \circ)$  genannt:

$$(H_N, \circ) \leqslant (G_{2 \times 2 \times 2}, \circ) \text{ und } (H_G, \circ) \leqslant (G_{2 \times 2 \times 2}, \circ)$$

Die Untergruppe  $(H_N, \circ)$  enthält in der Trägermenge  $H_N$  ausschließlich die Äquivalenzklasse des neutralen Elements  $N$ . Bei der Untergruppe  $(H_G, \circ)$  hingegen ist die Trägermenge  $H_G$  die gleiche Menge wie  $G_{2 \times 2 \times 2}$ .

$$(H_N, \circ) = (\{N\}, \circ) \text{ und } (H_G, \circ) = (G_{2 \times 2 \times 2}, \circ)$$

Im Rahmen dieser Arbeit kann nur auf einen Teil der Untergruppen von  $(G_{2 \times 2 \times 2}, \circ)$  eingegangen werden. Der folgende Abschnitt beschreibt zwei anschauliche Untergruppen des Würfels. Diese Untergruppen hat Tom Davis (in *Group Theory via Rubik's Cube*) [4] für den 3x3x3-Würfel genannt. Hier werden zwei seiner Untergruppen auf den 2x2x2 übertragen:

- Die Untergruppe  $(H_{E1}, \circ)$  lässt nur die Rotation einer Ebene zu. Die Züge der Trägermenge erreichen lediglich vier Würfelkonfigurationen (sowohl beim 2x2x2- als auch beim 3x3x3-Würfel). Das kann auch gut an einem *Cube* nachvollzogen werden, da durch das Drehen von nur einer Ebene auch nur vier verschiedene Ergebnisse erzielt werden können.

Da die Trägermenge  $H_{E1}$  die Äquivalenzklassen aller möglichen Züge der Untergruppe beinhaltet, sind hier genau vier Elemente enthalten. Jeder Zug, der durch die Drehung einer Ebene ausgeführt wird, ist ein Repräsentant dieser vier Züge.

Auch anhand des mathematischen Modells des  $2 \times 2 \times 2$ -Würfels kann festgestellt werden, dass die Züge der Untergruppe  $(H_{E1}, \circ)$  genau vier Würfelkonfigurationen erreichen.

Jede Ebenendrehung ( $U, D, R, L, F$  oder  $B$ ) ist durch eine Permutationsfunktion  $\sigma$  definiert. Dabei besteht  $\sigma$  für jeden dieser Grundzüge aus nur einem vierelementigen Zykel. Diese Zyklen wurden in Abschnitt 4.1 definiert. Die Ordnung der Permutation ist im Fall einer einzelnen Ebenendrehung immer vier. Die Ordnung einer Permutation wurde in Abschnitt 5.8 beschrieben.

Die Ordnung eines Zuges wurde in Abschnitt 5.9 definiert. Bei der Ordnung eines Zuges wird zusätzlich zu den Permutationen die Funktion  $\gamma$  berücksichtigt, die die Ausrichtung der Steine darstellt.  $\gamma$  wurde in Abschnitt 4.2 definiert. Jede dieser Funktionen  $\gamma$  gibt die Eingabe unverändert zurück, wenn sie viermal direkt nacheinander ausgeführt wird. Der Beweis dazu findet sich in Anhang A.

Somit ist die Ordnung einer einzelnen Ebenendrehung immer vier und die Trägermenge  $H_{E1}$  enthält genau vier Züge. Durch diese vier Züge können genau vier verschiedene Würfelkonfigurationen erreicht werden.

- Eine weitere Untergruppe von  $(G_{2 \times 2 \times 2}, \circ)$  ist  $(H_{E2}, \circ)$ . Hier dürfen zwei gegenüberliegende Ebenen gedreht werden. Bei der Gruppe des  $3 \times 3 \times 3$ -Würfels ergeben sich daraus 16 mögliche Würfelkonfigurationen [4]. Bei dem  $2 \times 2 \times 2$ -Cube sind es allerdings lediglich vier, da es nur zwei Ebenen gibt und die Rotation der Würfels nicht anhand der Mittelsteine unterschieden werden kann. Durch die Äquivalenzklassen der Rotationen ergibt sich somit eine zu  $(H_{E1}, \circ)$  äquivalente Untergruppe.

## 6.2 Erzeuger

Die folgenden Beispiele stammen aus Tom Davis' *Group Theory via Rubik's Cube* [4] und werden hier von der Gruppe des  $3 \times 3 \times 3$ -Cubes auf den  $2 \times 2 \times 2$ -Cube übertragen. Erzeuger wurden in Abschnitt 3.3 definiert und erklärt.

Ein Beispiel für einen Erzeuger einer Untergruppe  $(G_F, \circ)$  von  $(G_{2 \times 2 \times 2}, \circ)$  ist der einzelne Zug  $\{F\}$ , der diese Untergruppe erzeugt. Durch den Zug  $F$  können genau vier Würfelkonfigurationen erreicht werden und die Trägermenge  $G_F$  der Untergruppe  $(G_F, \circ)$  enthält somit vier Elemente:

$$G_F = \{N, F, FF, FFF\}$$

Alle weiteren Züge, die durch  $F$  erzeugt werden, sind äquivalent zu einem dieser Züge sind. Beispielsweise ist  $FFFF$  ein Repräsentant der Äquivalenzklasse von  $N$  – der Würfel befindet sich nach Ausführen dieses Zuges wieder in der Ausgangsposition.

Ein weiteres Beispiel ist die Untergruppe, die von  $\{FF\}$  erzeugt wird. Dabei kann die obere Ebene ausschließlich halbe Drehungen (statt Vierteldrehungen) machen und somit nur zwei Positionen erreichen. Die Trägermenge enthält daher die Äquivalenzklassen der beiden Züge  $FF$  und  $FFFF$ .

Die komplette Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  wird erzeugt durch  $\{U, D, R, L, F, B\}$ . Eine minimale Gruppe des  $2 \times 2 \times 2$ -Würfels wird in Kapitel 9 beschrieben und durch  $\{U, R, F\}$  erzeugt.

Die Untergruppen, die von genau einem Element aus  $G_{2 \times 2 \times 2}$  erzeugt werden, nennt man zyklische Gruppen. Die oben beschriebene Untergruppe  $(G_F, \circ)$ , die durch  $F$  erzeugt wird, ist eine solche zyklische Untergruppe.  $(G_F, \circ)$  wird erzeugt durch:

$$\langle F \rangle = \{F^n \mid n \in \mathbb{Z}\}$$

Das bedeutet, dass die Trägermenge  $G_F$  die Äquivalenzklassen der folgenden Elemente enthält:

$$\{N, F^1, F^2, F^3, F^4, \dots\}$$

Zyklische Gruppen können unendlich sein. Die Gruppe  $(G_F, \circ)$  ist aufgrund der Äquivalenzklassen aber endlich. Die Gleichheit der einelementigen Züge wurde bereits in Abschnitt 5.1 beschrieben.

Da die Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  endlich ist, erzeugt jedes Element der Gruppe eine endliche zyklische Untergruppe [4]. Die Größe dieser Untergruppe hängt von der Ordnung des Zuges ab. Die Ordnung wurde in Abschnitt 5.8 beschrieben. Die Ordnung des Zuges  $FR$  beispielsweise ist 15 – wenn  $FR$  15-mal auf dem  $2 \times 2 \times 2$ -Würfel ausgeführt wird, ist er wieder in der Ausgangsposition. Die Gruppe, die durch  $\{FR\}$  erzeugt wird, hat somit 15 Elemente, da mit dem Zug 15 Würfelkonfigurationen erreichbar sind. Bei dem  $3 \times 3 \times 3$ -Würfel ist die Ordnung des Zuges  $FR$  105 [4].

### 6.3 Durch $FF$ und $RR$ erzeugte Untergruppe

Das Beispiel der durch  $\{FF, RR\}$  erzeugten Untergruppe hat Tom Davis in *Group Theory via Rubik's Cube* [4] ebenfalls beschrieben und hier wird es von dem  $3 \times 3 \times 3$ - auf den  $2 \times 2 \times 2$ -Würfel übertragen. Da die beiden Züge  $FF$  und  $RR$  als Einheiten gesehen werden,

muss jede der Ebenendrehungen eine halbe Drehung sein. Es wurde in Abschnitt 5.1 bereits gezeigt, dass  $(FF)^2 = N$  und  $(RR)^2$  Repräsentanten der Äquivalenzklasse von  $N$  sind, da der Würfel dann wieder in der Ausgangskonfiguration ist.

$$C \cdot (FF)^2 = C \text{ und } C \cdot (RR)^2 = C$$

Wenn bei einem gelösten  $2 \times 2 \times 2$ -Würfel  $FFRR$  ausgeführt wird, befindet sich der Würfel nach 3 Wiederholungen wieder in der Startkonfiguration. Das gilt auch für den Zug  $RRFF$ . Die Ordnung von  $FFRR$  und  $RRFF$  ist daher 3. Bei dem  $3 \times 3 \times 3$ -Cube ist die Ordnung dieser Züge 6 [4]. Die durch  $\{FF, RR\}$  erzeugte Untergruppe des  $3 \times 3 \times 3$ -Würfels hat somit mehr Elemente als die des  $2 \times 2 \times 2$ -Würfels.

Im Folgenden werden alle Mitglieder der Untergruppe des  $2 \times 2 \times 2$ -Cubes aufgelistet. Alle anderen möglichen Kombinationen von  $FF$  und  $RR$  erreichen dieselbe Würfelkonfiguration wie diese sieben Züge:

$$\begin{array}{cccc} N & RR & FFRR & RRFFRR \\ & FF & RRFF & FFRRFF \end{array}$$

Zum Vergleich: Tom Davis erhält bei dem  $3 \times 3 \times 3$ -Würfel zwölf Elemente in der durch  $\{FF, RR\}$  erzeugten Untergruppe.

Die äquivalenten Züge können auch mathematisch erkannt werden, ohne die Züge an einem Würfel auszuprobieren. Das wird im Folgenden beispielhaft mit dem Zug  $(RRFF)^2 RR$  gemacht.

$$(RRFF)^2 RR = RRFFRRFFRR$$

Da  $RRFF$  die Ordnung 3 hat, befindet sich der Würfel nach  $(RRFF)^3$  wieder in der Ausgangskonfiguration.

$$C \cdot (RRFF)^3 = C \cdot RRFFRRFFRR = C$$

Daraus kann geschlossen werden, dass nach dem Ausführen von  $RRFFRRFFRR$  einzig  $FF$  ausgeführt werden muss, um wieder in die Ausgangsposition zu gelangen. Somit kann die Position, die durch  $RRFFRRFFRR$  erreicht wird, auch durch  $(FF)^{-1}$  erreicht werden.

$$C \cdot RRFFRRFFRR = C \cdot (FF)^{-1}$$

Da das Inverse eines Zuges  $Z$  als  $ZZZ$  definiert ist, gilt für die Züge  $FF$  und  $RR$ :

$$(FF)^{-1} = F^{-1}F^{-1} = FFFFFF = FF$$

$$(RR)^{-1} = R^{-1}R^{-1} = RRRRRR = RR$$

Die Inversen von  $FF$  und  $RR$  sind demnach  $FF$  und  $RR$ . Deshalb ist der Zug  $RRFFRRFFRR$  äquivalent zu dem Zug  $FF$ , da dieser äquivalent zu  $(FF)^{-1}$  ist.

$$C \cdot RRFFRRFFRR = C \cdot FF$$

Die Tatsache, dass  $\{FF, RR\}$  eine Untergruppen mit lediglich 7 bzw. 12 Elementen bei dem  $2 \times 2 \times 2$ - bzw. dem  $3 \times 3 \times 3$ -Würfel erzeugt, ist besonders überraschend, da  $\{F, R\}$  bei dem  $3 \times 3 \times 3$ -Würfel eine Untergruppe der Größe 73 483 200 erzeugt [4]. Bei dem  $2 \times 2 \times 2$ -Cube kommt die Untergruppe mit  $5! \cdot 3^5$  auf lediglich 29 160 Mitglieder, aber auch das ist deutlich größer als 7.

## 6.4 Cayleygraph

Cayleygraphen wurden in Abschnitt 3.4 eingeführt. Sie dienen der Visualisierung von Untergruppen und deren Erzeugern. Ein simples Beispiel ist in Abbildung 23 zu sehen: Der Cayleygraph der Untergruppe  $(G_F, \circ)$  von  $(G_{2 \times 2 \times 2}, \circ)$ , die durch  $\{F\}$  erzeugt wird. Die Untergruppe  $(G_F, \circ)$  wurde in Kapitel 6.2 beschrieben.



Abbildung 23: Cayleygraph zu Erzeuger  $\{F\}$

Dieser Cayleygraph ist anschaulich, da er nicht sonderlich komplex ist. Die Untergruppe wird durch die Ebenendrehung  $F$  erzeugt. Dadurch ergeben sich vier Elemente in der Trägermenge:

$$G_F = \{F, FF, FFF, N\}$$

Jedes Element aus  $G_F$  wird durch einen Knoten dargestellt. Die Pfeile zwischen den Knoten zeigen, welches Element sich durch das weitere Hinzufügen eines Erzeugers ergibt. In diesem Fall ist der Zyklus einer einzelnen Ebenendrehung zu sehen.

Im Vergleich dazu ist der Cayleygraph der durch  $\{FF, RR\}$  erzeugten Untergruppe komplexer (s. Abbildung 24). Diese Untergruppe wurde in Abschnitt 6.3 beschrieben. Die roten Pfeile repräsentieren den Erzeuger  $\{FF\}$ , da es sich dabei in der Startkonfiguration um die rote Seite des Würfels handelt. Die blauen Pfeile repräsentieren den Erzeuger  $\{RR\}$ , da es sich dabei um die blaue Würfelseite handelt. Elemente, die durch ein anderes Element in Kombination mit einem Erzeuger entstehen, sind durch einen Pfeil (Erzeuger) miteinander verbunden.

Anhand dieses Cayleygraphen kann beispielsweise abgelesen werden, dass die Züge  $FFFF$  und  $RRRR$  dem neutralen Element  $N$  entsprechen. Von dem Knoten  $FF$  führt ein roter Pfeil zu  $N$ . Die roten Pfeile repräsentieren den Erzeuger  $FF$ . Somit erzeugen  $FFFF$  und  $N$  die gleiche Würfelkonfiguration.

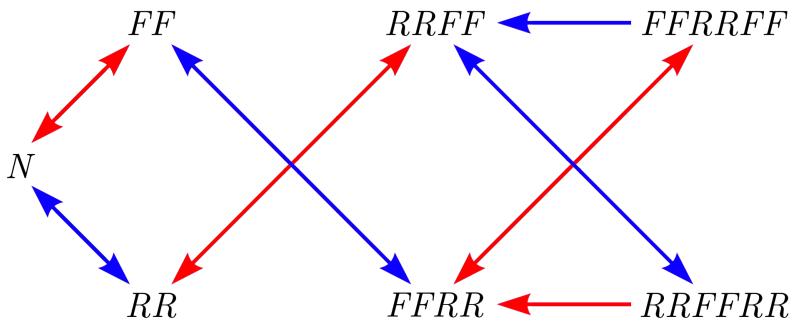


Abbildung 24: Cayleygraph zu Erzeuger  $\{FF, RR\}$

Dieser Cayleygraph ist wesentlich komplexer, als der Graph der Untergruppe  $(G_F, \circ)$  (Abbildung 23). Trotzdem stellt er eine sehr kleine erzeugte Untergruppe dar, wenn man das mit der Größe der anderen erzeugbaren Untergruppen von  $(G_{2 \times 2 \times 2}, \circ)$  vergleicht. Die Untergruppen und Cayleygraphen können bei der Gruppe des  $2 \times 2 \times 2$ -Würfels (und des  $3 \times 3 \times 3$ -Würfels) sehr groß werden. In Kapitel 9 wird die Untergruppe der minimalen, vollständigen Abbildung des Würfels definiert. Der Cayleygraph dieser Untergruppe wird in Abschnitt 9.3 beschrieben und enthält 3 647 160 Knoten.

## 7 Valide Konfigurationen des Würfels

In diesem Kapitel wird die Anzahl der validen Würfelkonfigurationen berechnet – sowohl anhand des physischen Würfels als auch mithilfe der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$ . Dazu wird die Mächtigkeit der Gruppe berechnet. Die Definition der Mächtigkeit und Beispiele sind in Abschnitt 3.1 zu finden.

Außerdem wird gezeigt, dass für die Ausrichtung  $x$  der Steine  $(\sum_{i=1}^8 x_i) \bmod 3 = 0$  gilt.

### 7.1 Anzahl der validen Würfelkonfigurationen

Im Folgenden wird die Anzahl der möglichen Würfelkonfigurationen anhand des Würfels berechnet. Nicht jede der theoretisch möglichen Würfelkonfigurationen kann auch wirklich durch Ebenendrehungen erreicht werden. Wie viele Möglichkeiten es im  $2 \times 2 \times 2$ -Würfel gibt und welche davon wirklich erreichbar sind, wird nun schrittweise anhand des Würfelaufbaus berechnet.

Dazu wird zuerst die Anzahl der möglichen Steinpositionen berechnet: Die Ecksteine können sich in jeder der acht Ecken befinden. Deshalb gibt es pro Eckstein 8 mögliche Positionen im Würfel. Da es 8 Ecksteine gibt, gibt es somit  $8! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 40\,320$  mögliche Positionen für die Ecksteine.

Außerdem können die Ecksteine gedreht sein, es können also verschiedene Farbflächen oben sein. Da die Steine aus 3 Farbflächen bestehen, können sieben davon durch Ebenendrehungen 3 verschiedene Ausrichtungen annehmen. Der achte Stein kann durch die Möglichkeit der Rotation des kompletten Würfels als richtig gedreht angenommen werden. Es gibt folglich  $3^7 = 2187$  Möglichkeiten für die Ausrichtung der Ecksteine.

Da es keine Mittelsteine im Würfel gibt, reduziert die Rotation des Würfels die Möglichkeiten um den Faktor 24, denn es gibt 6 Seiten, die jeweils 4 Ausrichtungen haben können. Das sind dann  $6 \cdot 4 = 24$ . Alle 24 Ausrichtungsmöglichkeiten sind in Anhang B abgebildet.

Somit ergibt es  $(3^7 \cdot 8!) \cdot \frac{1}{24}$  mögliche Konfigurationen für den Würfel. Das sind 3 674 160 Konfigurationen.

### 7.2 Mächtigkeit von $G_{2 \times 2 \times 2}$

Die Mächtigkeit der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  ist die Anzahl der Elemente von  $G_{2 \times 2 \times 2}$ . Das wird auch als  $|G_{2 \times 2 \times 2}|$  bezeichnet. Die Mächtigkeit der Gruppe entspricht der Anzahl der validen Würfelkonfigurationen, da  $G_{2 \times 2 \times 2}$  die Äquivalenzklassen aller möglichen Züge

enthält. Wenn zwei Züge mit gleicher Ausgangskonfiguration die gleiche Folgekonfiguration des Würfels hervorrufen, sind sie Repräsentanten der gleichen Äquivalenzklasse in  $G_{2 \times 2 \times 2}$ . Somit bringt jedes Element von  $G_{2 \times 2 \times 2}$  den Würfel in eine andere Würfelkonfiguration und es sind keine äquivalenten Züge doppelt enthalten. Außerdem wurden die Äquivalenzklassen mit der Menge alle Züge des Würfels gebildet. Somit ist jeder mögliche Zug enthalten und  $|G_{2 \times 2 \times 2}|$  entspricht der Anzahl der validen Würfelkonfigurationen.

Da die Mächtigkeit der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  der Anzahl der validen Würfelkonfigurationen entspricht, setzt sie sich aus dem Produkt der Konfigurationsparameter  $\sigma$  und  $x$  zusammen. Außerdem müssen die Äquivalenzen bezüglich der Rotationen berücksichtigt werden.

$\sigma$  ist die Menge der bijektiven Funktionen für jede Ebenenrotation. Es sind die Übergänge der acht Würfelsteine als Permutationen enthalten. Da es 8 Permutationsobjekte gibt, ist die Anzahl der Permutationsmöglichkeiten  $8! = 40320$ .

Der andere Parameter der Würfelkonfiguration ist der 8-dimensionale Vektor  $x$ . Jeder der Werte in  $x$  ist aus der Menge  $\{0, 1, 2\}$ . Somit gibt es drei Möglichkeiten für jeden Wert im Vektor. Das ergibt dann  $3^8 = 6561$  mögliche Konfigurationen des Vektors.

Ohne Berücksichtigung der Rotationen wird ein Wert von  $40320 \cdot 6561 = 264\,539\,520$  möglichen Konfigurationen erreicht. Da durch die Rotationen eine der Steinausrichtungen in  $x$  als richtig angenommen werden kann, wird  $264\,539\,520$  durch drei geteilt und ergibt dann  $88\,179\,840$ . Außerdem gibt es  $6 \cdot 4 = 24$  Rotationsmöglichkeiten, die in den Äquivalenzklassen berücksichtigt werden. Alle 24 Rotationsmöglichkeiten sind in Anhang B abgebildet. Somit muss  $88\,179\,840$  durch 24 geteilt werden, um die Mächtigkeit der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  zu berechnen.  $|G_{2 \times 2 \times 2}|$  ist dann  $88\,179\,840 \div 24 = 3\,674\,160$ .

Die Mächtigkeit der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  entspricht der Anzahl der validen Würfelkonfigurationen:  $3\,674\,160$ .

### 7.3 Ausrichtung der Steine (modulo 3)

Die Konfiguration des Würfels ist als  $C = (\sigma, x)$  definiert. In diesem Abschnitt wird gezeigt, dass bei jeder validen Würfelkonfiguration für die Werte des Vektors  $x$  folgendes gilt:

$$\left( \sum_{i=1}^8 x_i \right) \bmod 3 = 0$$

Sei  $C' = (\sigma', x')$  eine Nachfolgekonfiguration der Konfiguration  $C = (\sigma, x)$ . Dabei ist  $Z$  einer der Züge aus  $G_{2 \times 2 \times 2}$ .

$$(\sigma, x) \cdot Z = (\sigma', x')$$

Für diese Vektoren  $x$  und  $x'$  gilt dann:

$$\left( \sum_{i=1}^8 x'_i \right) \bmod 3 = \left( \sum_{i=1}^8 x_i \right) \bmod 3 = 0$$

Der Würfel kann durch einen der Grundzüge des Würfels oder einer Kombination der Grundzüge verändert werden. Die Veränderungen des Vektors  $x$  durch das Ausführen der Grundzüge sind in der folgenden Tabelle detailliert zu sehen. Die Variable  $s$  beschreibt dabei die Veränderung der Summe der Vektoreinträge. In Abschnitt 4.2 sind die Funktionen definiert, die die Veränderungen des Vektor  $x$  für jeden der Züge realisieren.

Zug $Z$	Vektor $x$	$s$	$\bmod 3$
$U$	$(x_3, x_1, x_4, x_2, x_5, x_6, x_7, x_8)$	+0	0
$D$	$(x_1, x_2, x_3, x_4, x_6, x_8, x_5, x_7)$	+0	0
$R$	$(x_1, (x_4 + 2) \bmod 3, x_3, (x_8 + 1) \bmod 3, x_5, (x_2 + 1) \bmod 3, x_7, (x_6 + 2) \bmod 3)$	+6	0
$L$	$((x_5 + 1) \bmod 3, x_2, (x_1 + 2) \bmod 3, x_4, (x_7 + 2) \bmod 3, x_6, (x_3 + 1) \bmod 3, x_8)$	+6	0
$F$	$(x_1, x_2, (x_7 + 1) \bmod 3, (x_3 + 2) \bmod 3, x_5, x_6, (x_8 + 2) \bmod 3, (x_4 + 1) \bmod 3)$	+6	0
$B$	$(x_2 + 2) \bmod 3, (x_6 + 1) \bmod 3, x_3, x_4, (x_1 + 1), (x_5 + 2) \bmod 3, x_7, x_8)$	+6	0

Jede valide Würfelkonfiguration  $C$  kann ausschließlich durch Züge erreicht werden. Züge bestehen aus Elementen der Menge  $\{U, D, R, L, F, B\}$ . In der Startkonfiguration ist der Summe der Vektoreinträge 0. Der Vektor  $x$  ist dabei  $(0, 0, 0, 0, 0, 0, 0, 0, 0)$  und die Summe der Einträge ist somit 0. Es gilt

$$\left( \sum_{i=1}^8 (0, 0, 0, 0, 0, 0, 0, 0) \right) \bmod 3 = 0$$

Bei jedem der Grundzüge aus  $\{U, D, R, L, F, B\}$  wird die Summe der Vektoreinträge um den Wert von  $s$  verändert. Die Variable  $s$  ist bei den Grundzügen entweder 0 oder 6. Es gilt demnach auch:

$$s \bmod 3 = 0$$

Somit muss die Summe  $s$  der Vektoreinträge immer 0 sein, wenn modulo 3 gerechnet wird, da jeder Zug  $Z$  aus einem der Grundzüge aus  $\{U, D, R, L, F, B\}$  oder einer Kombination dieser besteht. Jedes Vielfache von 6 und 0 ergibt 0, wenn modulo 3 gerechnet wird. Es gilt demnach:

$$(k \cdot s) \bmod 3 = 0 \text{ für } k \in \mathbb{N}$$

Und somit gilt auch:

$$\left( \sum_{i=1}^8 x'_i \right) \bmod 3 = \left( \sum_{i=1}^8 x_i \right) \bmod 3 = 0.$$

Da in Abschnitt 5.2 gezeigt wurde, dass die Rotationen auch als Kombination von Zügen definiert werden können, gilt die Aussage auch für jede Rotation des Würfels.

## 8 Lösung des Würfels

Die übliche, händische Methode zum Lösen eines Zauberwürfels erfolgt durch das Kombinieren verschiedener Ebenendrehungen. Diese werden als eine Einheit angewendet und verändern die Konfiguration des Würfels dann spezifisch. Es gibt beispielsweise eine Kombination, die 3 der 4 Ecken der oberen Ebene untereinander im Uhrzeigersinn tauscht und deren Ausrichtung dabei nicht verändert.

In diesem Kapitel wird die Anzahl der 2-Zykel der Züge untersucht und Kommutatoren erklärt. Dann wird beispielhaft ein Lösungsvorgang eines Menschen schrittweise beschrieben und erklärt. Außerdem werden Muster des Würfels algorithmisch beschrieben und grafisch dargestellt. Danach werden verschiedene Lösungsalgorithmen des  $3 \times 3 \times 3$ -Cubes auf den  $2 \times 2 \times 2$ -Würfel übertragen.

### 8.1 Anzahl der 2-Zykel

Die Position der Würfelsteine wird durch die Permutationsfunktionen  $\sigma$  beschrieben.  $\sigma$  besteht aus verschiedenen Zykeln in Abhängigkeit von der Position der Steine. Das wurde in Abschnitt 4.1 definiert und beschrieben. Jeder  $n$ -Zykel kann als Produkt von 2-Zykeln geschrieben werden. Wenn  $n$  dabei gerade ist, hat das dazugehörige 2-Zykel-Produkt eine ungerade Anzahl an 2-Zykeln und anders herum. [4]

Jede Würfelkonfiguration kann durch eine Kombination der Ebenendrehungen  $U, D, F, B, L, R$  (und der Rotationen des Würfels) erreicht werden. Die Zykel der einzelnen Ebenendrehungen des Würfels sind im Folgenden als Produkt von 2-Zykeln geschrieben:

$$\begin{aligned}\sigma_U &= (ulf\ ulb\ urb\ urf) = (ulf\ ulb)(ulf\ urb)(ulf\ urf) \\ \sigma_D &= (dlf\ drf\ drb\ dbl) = (dlf\ drf)(dlf\ drb)(dlf\ dbl) \\ \sigma_F &= (ulf\ urf\ drf\ dlf) = (ulf\ urf)(ulf\ drf)(ulf\ dlf) \\ \sigma_B &= (ulb\ dbl\ drb\ urb) = (ulb\ dbl)(ulb\ drb)(ulb\ urb) \\ \sigma_L &= (ulb\ ulf\ dlf\ dbl) = (ulb\ ulf)(ulb\ dlf)(ulb\ dbl) \\ \sigma_R &= (urb\ drb\ drf\ urf) = (urb\ drb)(urb\ drf)(urb\ urf)\end{aligned}$$

Anhand der Funktionen der Grundzüge ist ersichtlich, dass jeder Grundzug durch einen 4-Zykel definiert ist. Jeder 4-Zykel kann als Produkt aus drei 2-Zykeln geschrieben werden. Die Anzahl der 2-Zykel einer einzelnen Ebenendrehung ist demnach ungerade. Die Anzahl

der 2-Zykel eines Zuges, der aus zwei Ebenendrehungen besteht ist demnach gerade. Beispielsweise hat der Zug  $LF$  eine gerade Anzahl an 2-Zykeln:

$$\begin{aligned}\sigma_{LF} &= (ulb\ urf\ drf\ dlf\ dbl) \\ &= (ulb\ urf)(ulb\ drf)(ulb\ dlf)(ulb\ dbl)\end{aligned}$$

Die Zykel treffen ausschließlich eine Aussage über die Position der Steine im Würfel. Die Rotation wird durch den Vektor  $x$  dargestellt und hier nicht berücksichtigt.

Bei dem  $3 \times 3 \times 3$ -Würfel ist die Anzahl der 2-Zykel jeder Permutation gerade, deshalb gibt es keinen Zug, der genau zwei Steine im Würfel tauscht [4]. Ein Zug, der genau zwei Steine tauscht, wird durch *einen* 2-Zykel dargestellt – das wäre eine ungerade Anzahl an 2-Zykeln. Im Gegensatz zum  $3 \times 3 \times 3$ -Würfel kann die Anzahl der 2-Zykel des  $2 \times 2 \times 2$ -Würfels ungerade sein und somit es gibt für diesen Würfel Algorithmen, die die Position von genau zwei Steinen tauschen. Diese Algorithmen sind in Abschnitt 8.8 beschrieben.

## 8.2 Kommutatoren

Kommutatoren wurden in Abschnitt Abschnitt 3.6 erklärt. Der Kommutator von zwei Zügen  $Y, Z$  der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  ist demnach definiert als:

$$[Y, Z] = YZY^{-1}Z^{-1}$$

Kommutternde Elemente sind Elemente, die als Kommutator das neutrale Element einer Gruppe ergeben. Das neutrale Element ist hier der leere Zug  $N$ .

$$[Y, Z] = N \Rightarrow Y \text{ und } Z \text{ sind kommutierende Elemente}$$

Zwei gleiche Züge  $Y, Z$  der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  kommutieren:

$$\forall Y, Z \in G_{2 \times 2 \times 2}, Y = Z \cdot [Y, Z] = N$$

Zu dieser Aussage folgt ein Beweis. Zur besseren Übersichtlichkeit wird dabei  $[Y, Z]$  mit  $Y = Z$  nun als  $[Z, Z]$  geschrieben.

$$\forall Z \in G_{2 \times 2 \times 2} \cdot [Z, Z] = N$$

Auf eine Konfiguration  $C$  angewandt, ist der Kommutator zweier gleicher Elemente im Folgenden definiert:

$$\forall Z \in G_{2 \times 2 \times 2} . C \cdot [Z, Z] = C$$

Das kann dann folgendermaßen umgeformt werden:

$$\begin{aligned} C \cdot [Z, Z] &= C \cdot ZZZ^{-1}Z^{-1} \\ &= C \cdot Z(ZZ^{-1})Z^{-1} \\ &= C \cdot Z(N)Z^{-1} \\ &= C \cdot ZZ^{-1} \\ &= C \cdot N \\ &= C \end{aligned}$$

Somit kommutieren alle Zugpaare aus  $G_{2 \times 2 \times 2}$ , die aus zwei gleichen Zügen bestehen.

Es kommutieren nicht ausschließlich gleiche Zugpaare, sondern auch Züge, die gegenüberliegende Ebenen beeinflussen. Somit bewegen sie nicht dieselben Steine. Diese sogenannten *elementfremden Zykel* kommutieren [13]. Auch bei dem Vektor  $x$  werden dann keine gemeinsamen Einträge beeinflusst. Das sind dann die folgenden Kommutatoren, mit  $n, m \in \mathbb{N}$ :

$$\begin{array}{lll} [U^n, D^m] & [F^n, B^m] & [L^n, R^m] \\ [D^n, U^m] & [B^n, F^m] & [R^n, L^m] \end{array}$$

Da die Zugpaare nicht dieselben Steine beeinflussen, ist es nicht relevant, dass die Gruppe nicht kommutativ ist. Durch den Aufbau des Kommutators werden beide Züge ausgeführt und wieder invertiert.

Wenn zwei Züge  $Y, Z \in G_{2 \times 2 \times 2}$  nicht kommutieren, kann anhand der Komplexität des Kommutators bis zu einem gewissen Grad eine Aussage darüber getroffen werden, wie groß die Veränderung der Würfelkonfiguration nach dem Ausführen von  $[Y, Z]$  ist. Zur Veranschaulichung folgt nun ein Beispiel mit den Zügen  $L$  und  $F$  und der Startkonfiguration  $C = (1, 0)$ :

$$C \cdot [L, F] = C \cdot LFL^{-1}F^{-1}$$

Dabei verändern vier der acht Steine im Würfel ihre Position und Ausrichtung. Die anderen vier bleiben unverändert.

Die Folgekonfiguration ist im Folgenden zu sehen, mit  $C = (1, 0)$ :

$$C \cdot [L, F] = ((\text{ulb ulf})(\text{dlf drf}), (0, 0, 2, 0, 0, 0, 0, 1))$$

Es haben demnach zwei Steinpaare ihre Position getauscht und ihre Ausrichtung verändert. Im Vergleich dazu werden beispielsweise bei dem Kommutator von  $[L, R]$  keine Steinpositionen verändert, da  $L$  und  $R$  keine gemeinsamen Steine beeinflussen.

Um aussagekräftigere Ergebnisse zu der Kommutativität der Zugpaare zu bekommen, müsste eine größere Menge der Kommutatoren berechnet und verglichen werden. Das ist allerdings zu Umfangreich für den Rahmen dieser Arbeit. Die Berechnung und Auswertung der Kommutatoren sollte maschinell erfolgen.

### 8.3 Lösungsansätze

Für die Lösung des Würfels sind Züge nützlich, die lediglich wenige Steine beeinflussen. So können dann gezielt bestimmte Steine gedreht oder getauscht werden.

Es gibt verschiedene Vorgehensweisen, um den Würfel zu lösen. Üblicherweise werden die Ebenen des Würfels nacheinander gelöst. Für die Lösungsalgorithmen ist die Farbe der ersten Seite nicht relevant. Es wird aber häufig mit weiß begonnen, da die Anordnung der Farben so leichter zu merken ist. Dann kann schneller gesehen werden, in welche Ebene ein Stein gehört. [7] Deshalb wird im weiteren Verlauf dieser Arbeit bei der Lösung mit der weißen Seite begonnen.

Die beiden unten beschriebenen Lösungsansätze führen nicht zu einer optimalen Lösung des Würfels. Mehr zu der optimalen Lösung findet sich am Ende von Abschnitt 8.4 und in Abschnitt 9.5. Außerdem ist zu beachten, dass es eine Vielzahl weiterer Lösungsansätze gibt.

#### Ebenen nacheinander vollständig lösen

Einer der Lösungsansätze geht so vor, dass die beiden Ebenen nacheinander vollständig gelöst werden. Dazu wird zuerst die erste Ebene und danach die zweite vollständig gelöst. Die erste Ebene kann durch simplere Züge gelöst werden als die zweite Ebene. Grund dafür ist, dass die Anordnung der Steine der zweiten Ebene beim Lösen der ersten Ebene noch nicht relevant ist. Beim Lösen der zweiten Ebene müssen komplexere Züge genutzt werden, um den gelösten Zustand der ersten Ebene beizubehalten.

Eine gängige Lösungsmethode für die zweite Ebene sieht vor, dass zuerst alle Steine der Ebene richtig ausgerichtet werden. Dann sind alle  $x_i = 0$ . Danach werden die Positionen noch getauscht. Die Würfelkonfiguration ist dann  $(1, 0)$  und der Würfel gelöst.

Dieses ebenenweise Vorgehen wird üblicherweise bei dem  $3 \times 3 \times 3$ -Würfel angewandt und wurde hier auf den  $2 \times 2 \times 2$ -Würfel übertragen: Beim  $3 \times 3 \times 3$ -Würfel wird zuerst die obere Ebene gelöst, dann die Mittlere, gefolgt von der Unteren. Wird dieses Vorgehen auf den  $2 \times 2 \times 2$ -Würfel übertragen, können sämtliche Lösungsschritte, die die Kanten beeinflussen, ignorieren, da der  $2 \times 2 \times 2$ -Würfel keine Kantsteine hat. Außerdem gibt es keine mittlere Ebene und die entsprechenden Lösungsschritte des  $3 \times 3 \times 3$ -Würfels werden ebenfalls nicht auf den  $2 \times 2 \times 2$ -Würfel übertragen.

Dieser Lösungsansatz wird auch *CFOP-Methode*<sup>2</sup> oder *Fridrich-Methode*<sup>3</sup> genannt [5].

wird in Abschnitt 8.4 anhand eines Beispiels schrittweise ausgeführt und erklärt. Außerdem werden die Algorithmen für die beiden Ebenen in den Abschnitten 8.7 und 8.8 beschrieben. Dies kann als eine Anleitung zum Lösen des Würfels dienen.

### Steine ausrichten und dann positionieren

Bei einem anderen Lösungsansatz werden zuerst alle Steine der ersten Ebene richtig ausgerichtet. Es gibt dann eine weiße Seite, die aus vier weißen Farbflächen besteht. Die Position der Steine ist dabei jedoch nicht relevant. Danach werden alle Steine der zweiten Ebene ausgerichtet. Auch hier ist die Position nicht relevant. Es gibt dann eine weiße und eine gelbe Seite, die anderen vier Seiten sind allerdings nicht gelöst, da die Steinposition noch nicht berücksichtigt wurde. Wenn alle Steine korrekt ausgerichtet sind und der Vektor  $x = 0$  ist, werden sie untereinander getauscht und der Würfel wird so gelöst. Dieses Vorgehen wird Ortega-Methode genannt [6].

## 8.4 Lösung des Würfels anhand eines Beispiels

In diesem Abschnitt wird der Würfel schrittweise anhand eines Beispiels gelöst. Dazu wird die gängige Lösungsmethode des  $3 \times 3 \times 3$ -Würfels auf den  $2 \times 2 \times 2$ -Würfel übertragen. Das Vorgehen dieser Lösungsmethode wurde in Abschnitt 8.3 beschrieben. Die Beschreibungen der Algorithmen dieser Lösungsmethode finden sich in den Abschnitten 8.7 und 8.8.

---

<sup>2</sup>Die Abkürzung *CFOP* bezieht sich auf das Lösen des  $3 \times 3 \times 3$ -Würfels und steht für: *Cross, First two layers, Orient last layer* und *Permute last layer*. Das beschreibt das Vorgehen dieser Methode. [5]

<sup>3</sup>Nach Jessica Fridrich benannt, die diese Methode erfunden hat. [Jessica Fridrich, persönliche Korrespondenz per E-Mail, s. Anhang C]

In diesem Beispiel wird der Würfel mit dem Zug  $FUBRF^{-1}$  verdreht (s. Abbildung 25). Nun wird schrittweise beschrieben, wie ein Mensch den Würfel lösen würde. Der Würfel befindet sich zu Beginn in der Konfiguration  $C = ((ulf\ dlf\ dbl\ urf), (2, 2, 0, 0, 2, 2, 1, 0))$ . In den Abbildungen wurde der Würfel noch um  $90^\circ$  um die  $z$ -Achse rotiert. Es gibt somit eine andere, zu  $C$  äquivalente Würfelkonfiguration  $C' = ((ulb\ urb\ urf)(ulf\ dbl)(drb\ drf\ dl), (0, 2, 0, 2, 1, 2, 0, 2))$ .

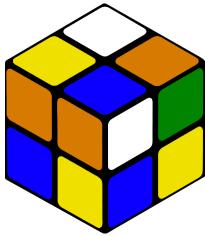


Abbildung 25: Würfel nach Zug  $FUBRF^{-1}$

Im ersten Schritt des menschlichen Ansatzes zum Lösen des Würfels sollen die Steine der oberen Ebene so angeordnet werden, dass die Farbflächen dort alle weiß sind und die vier oberen Steine in der richtigen Position zueinander sind. Für die Lösung der oberen Ebene muss  $x_{1-4} = (0, 0, 0, 0)$  gelten und die Steine der Ebene müssen an der richtigen Position zueinander sein.

Dafür sucht der Lösende Steine mit weißen Farbflächen und findet den weiß-orange-blauen Stein an der Position  $urf$ . Mit dem Zug  $F^{-1}$  findet der Stein seinen Platz in der oberen Ebene, mit der weißen Farbfläche oben. Nun ist  $x''_{1-4} = (0, 2, 0, 1)$ . Der Würfel ist in Abbildung 26 dargestellt: Es befinden sich nun zwei Steine der oberen Ebene richtig ausgerichtet an der richtigen Position – der weiß-orange-blaue Stein und der weiß-rot-blaue Stein. Die neue Würfelkonfiguration ist dann  $C'' = C' \cdot F^{-1} = ((ulb\ urb\ ulf\ dbl\ dl)\ drb\ urb), (0, 2, 0, 1, 1, 2, 2, 1))$ .



Abbildung 26: Lösung von Mensch: Schritt 1

Der nächste Stein, der angeordnet wird, ist hier der weiß-grün-orange Stein. Er wird durch den Zug  $R^{-1}$  in Position gebracht und findet seinen Platz neben dem weiß-orange-blauen Stein in der oberen Ebene (s. Abbildung 27). Die Würfelkonfiguration  $C'''$  ist dann  $C'' \cdot R^{-1} = ((ulb\ urf)(drb\ drf)(urb\ ulf\ dbl\ dlf), (0, 1, 0, 0, 2, 0, 1, 2))$ .



Abbildung 27: Lösung von Mensch: Schritt 2

Der letzte Stein mit weißer Farbfläche wird dann durch den Zug  $RD^{-1}R^{-1}$  positioniert. Die obere Ebene ist nun gelöst und alle Steine mit weißen Farbflächen sind wie in der Startkonfiguration zueinander ausgerichtet. (s. Abbildung 28). Die Würfelkonfiguration ist  $C^{IV} = ((ulb\ urf)(urb\ ulf)(drb\ drf\ dlf), (0, 0, 0, 0, 2, 0, 1, 0))$ .



Abbildung 28: Lösung von Mensch: Schritt 3

Für den nächsten Schritt rotiert der Mensch den Würfel, hier zweimal um die  $y$ -Achse (s. Abbildung 29). Die weiße Seite ist nun unten und zwei der vier gelben Farbflächen sind nach oben ausgerichtet. Dann ist die Würfelkonfiguration  $C^V = ((ulb\ drb\ urb\ dbl\ ulf\ drf)(urf\ dlf), (1, 0, 2, 0, 0, 0, 0, 0))$ .  $C^V$  ist zu  $C^{VI}$  äquivalent, da der Würfel nur rotiert wurde.



Abbildung 29: Lösung von Mensch: Schritt 4

Dann führt der Lösende den Zug  $RUR^{-1}U^{-1} R^{-1}FRF^{-1}$  aus [6] und erhält einen gelösten Würfel, der falsch herum gehalten wird (s. Abbildung 30).

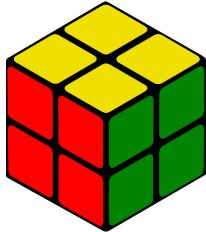


Abbildung 30: Gelöster *Cube* mit weißer Seite unten

Die Würfelkonfiguration ist  $C^{VI} = ((ulb\ drb)(urb\ dlb)(ulf\ drf)(urf\ dlf), (0, 0, 0, 0, 0, 0, 0, 0))$ . Diese Konfiguration ist äquivalent zu der Konfiguration  $(1, 0)$ . Daher wird dieser Würfel nun noch zweimal um die  $x$ -Achse gedreht und befindet sich dann in der Konfiguration  $C^{VII} = (1, 0)$ .

Der Mensch folgt beim Lösen des *Cubes* bestimmten Kombinationen, die in verschiedenen Situationen angewandt werden können. In diesem Fall hat der Mensch 13 Ebenendrehungen durchgeführt, während das Verdrehen lediglich 5 Ebenenrotationen benötigte. Der Mensch hat folglich nicht den kürzesten Weg gewählt, aber dafür einen Weg, den er bei verschiedenen Würfelkonfigurationen anpassen und verwenden kann. Wenn die Verdrehung des Würfels invertiert wird  $((FUBRF^{-1})^{-1})$ , ergibt das die Kombination  $FR^{-1}B^{-1}U^{-1}F^{-1}$ , um den Würfel zu lösen. Es stellt sich die Frage, wie viele Ebenendrehungen der  $2 \times 2 \times 2$ -Würfel maximal von der Lösung entfernt sein kann. Diese Zahl wird auch *God's Number* genannt.

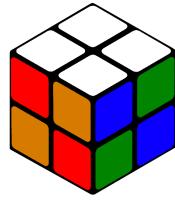
## God's Number

Im Folgenden werden die *God's Number*, *Quarter-Turn* Metrik und *Half-Turn* Metrik kurz beschrieben. Bei einer Ebenendrehung werden die Ebenen um  $90^\circ$  gedreht. Eine Ebenendrehung um  $180^\circ$  wird als zwei Vierteldrehungen gewertet. Das wird *Quarter-Turn* Metrik genannt. Es gibt noch andere Metriken, wie z. B. die *Half-Turn* Metrik, bei der eine Drehung der Ebene sowohl um  $90^\circ$  als auch um  $180^\circ$  als eine Drehung gezählt wird [11]. Wenn in der *Quarter-Turn* Metrik gerechnet wird, ist die *God's Number* des  $2 \times 2 \times 2$ -Würfels 14 [9]. In der *Half-Turn* Metrik ist sie 11 [10]. Ein Konzept zum Finden der optimalen Lösung mithilfe der *Quarter-Turn* Metrik wird in Abschnitt 9.5 beschrieben.

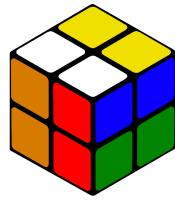
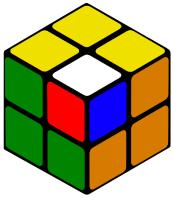
## 8.5 Muster

Dieser Abschnitt wurde von dem Abschnitt *Pretty Patterns* in Tom Davis' *Group Theory via Rubik's Cube* inspiriert [4]. Dort werden acht hübsche Muster des  $3 \times 3 \times 3$ -Würfels gezeigt. In diesem Abschnitt werden vier Muster des  $2 \times 2 \times 2$ -Würfels gezeigt und die dazugehörigen Algorithmen von der Startkonfiguration ausgehend beschrieben. Diese vier Muster sind in Abbildung 31 dargestellt. Außerdem wird die Konfiguration der Würfels angegeben.

Muster 1 lässt die weiße und gelbe Seite unverändert und bildet ein Karomuster auf den anderen vier Seiten. Dabei werden die Farbpaare rot-orange und grün-blau zusammen im Karomuster angeordnet. Die Konfiguration des Würfels ist dann  $C = ((ulb\ urf)(drb\ dlf), (0, 0, 0, 0, 0, 0, 0, 0))$ .



$$\begin{array}{c} \text{Muster 1} \\ RR\;FF\;RR\;UU \end{array} \quad \begin{array}{c} \text{Muster 2} \\ R\;FU^{-1}\;RR\;UF^{-1}\;R\;U\;FF\;RR \end{array}$$



Muster 3	Muster 4
<i>UU FF RR UU</i>	<i>U FF UU RR U</i>

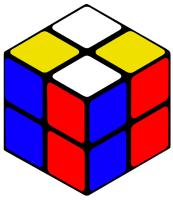


Abbildung 31: Muster des  $2 \times 2 \times 2$ -Würfels

Muster 2 hat einen *Würfel im Würfel*. Dabei werden zwei Steine getauscht, die keine gemeinsame Farbfläche haben. Der Würfel befindet sich dann in der Konfiguration  $C = ((\text{ulb } \text{drf})(\text{ulf } \text{dlf})(\text{drb } \text{urb}), (0, 0, 0, 0, 0, 0, 0, 0))$

Muster 3 zeigt abwechselnd Quer- und Längsstreifen auf den verschiedenen Seiten. Die Konfiguration des Würfels ist dann  $C = ((\text{ulb } \text{dlf } \text{drb}) (\text{urb } \text{ulf } \text{drf})), (0, 0, 0, 0, 0, 0, 0, 0))$ .

Muster 4 ordnet die Farben wie vier Säulen an. Die weiße und die gelbe Seite sind dabei kariert, die anderen Seiten gestreift. Die Konfiguration des Würfels ist dann  $C = ((\text{urb } dlf)(\text{ulf } drb)), (0, 0, 0, 0, 0, 0, 0, 0))$ .

Diese Muster sind in den meisten Fällen zwar keine üblichen Lösungsalgorithmen, sollten aber in dieser Arbeit auch nicht unerwähnt bleiben

## 8.6 Schraubendrehermethode

Die Methode, die oft als simpelste Methode zum Lösen von Zauberwürfeln beschrieben wird, ist die Schraubendrehermethode. Bei den üblichen  $2 \times 2 \times 2$ -Würfel ist auf einer oder mehreren Seiten in der Mitte zwischen den Steinen eine Schraube zu sehen (s. links in Abbildung 32). Um den Würfel auseinander zu bauen, muss diese Schraube gelockert

werden. Daraufhin können die Steine ohne Probleme abgenommen werden. Dann werden die Steine neu arrangiert und der Würfel kann in der gelösten Konfiguration wieder zusammen gebaut werden.



Abbildung 32: Lösung durch Schraubendrehermethode

Ob das wirklich die simpelste Methode ist, liegt wohl im Auge des Betrachters und unter Berücksichtigung der Tatsache, dass der Weltrekord des  $2 \times 2 \times 2$ -Würfels mit der Methode des algorithmischen, händischen Lösens bei 0,49 Sekunden liegt [1], ist die Schraubendrehermethode wohl kaum die schnellste Methode.

## 8.7 Algorithmen für die erste Ebene

In diesem Abschnitt werden Algorithmen zum Lösen der ersten Ebene mit der Fridrich-Methode beschrieben. Bei dieser Methode werden im ersten Schritt die vier Steine der oberen Ebene richtig ausgerichtet und richtig zueinander angeordnet. Die Vorgehensweise dieser Methode wurde bereits in Abschnitt 8.3 beschrieben.

Die Fridrich-Methode ist ein Lösungsansatz für den  $3 \times 3 \times 3$ -Würfel, der auf den  $2 \times 2 \times 2$ -übertragen werden kann. Da der  $2 \times 2 \times 2$ -im Gegensatz zum  $3 \times 3 \times 3$ -Würfel keine Mittelsteine hat, kann ein Eckstein als richtig angenommen werden, da der Würfel lediglich rotiert werden muss, um eine weiße Farbfläche zu finden. In diesen Beschreibungen wird sich an die Konvention gehalten, mit der weißen Seite zu beginnen. Es kann aber ebenso mit jeder anderen Seite des Würfels begonnen werden. Der  $3 \times 3 \times 3$ -Cube muss entsprechend der Mittelsteine ausgerichtet werden und so ist vorbestimmt, welche Seite die weiße Seite wird. Die weiße Seite muss den weißen Mittelstein enthalten. Bei dem  $2 \times 2 \times 2$ -Cube kann mit jeder beliebigen Seite begonnen werden. Wenn mit einer bestimmten Seite als Oberseite begonnen werden soll, die noch keine weiße Farbfläche hat, so kann die Farbfläche durch maximal zwei Ebenendrehungen an diese Seite gebracht werden.

In Abbildung 33 wird der erste Eckstein der oberen Ebene positioniert. Das kann dort entweder durch den Zug  $R$  oder einer Rotation um die  $y$ -Achse passieren.



Abbildung 33: Ersten Eckstein positionieren

Der zweite Stein kann dann hinzugefügt werden. Für diesen Algorithmus muss sich die weiße Farbfläche des zweiten Steins seitlich an der unteren Ebene befinden. Optimalerweise befindet sich der Stein schon zufällig an der gewünschten, korrekten Position. Ansonsten wird  $D$  ausgeführt, bis der Stein sich unter seiner Zielposition befindet und er wird mit  $L, R, F$  oder  $R$  neben den bereits vorhandenen ersten Eckstein gedreht. Das ist auch in Abbildung 34 zu sehen.



Abbildung 34: Zweiten Eckstein positionieren

Dort sind auch orange und grüne Farbflächen abgebildet. Das gilt analog für die anderen benachbarten Farbflächen. Zu beachten ist, dass die beiden Farbflächen einer Seite auch die gleiche Farbe haben.

Sollte sich die weiße Farbfläche der Ecke unten am Würfel befinden, so kann sie falsch herum ausgerichtet mit der Technik aus Abbildung 34 an die Position gesetzt werden. Dann befindet sich die weiße Farbfläche in der oberen Ebene, aber falsch herum ausgerichtet. Wenn das der Fall ist, kann der Stein mit einem der Züge  $L, R, F$  oder  $B$  herausgedreht werden und mit  $U$  in die untere Ebene geschoben werden. Dieser Vorgang ist auch in Abbildung 35 zu sehen. Danach wird er mit der oben beschriebenen Technik richtig ausgerichtet und positioniert eingefügt (s. Abbildung 34).



Abbildung 35: Zweiter Eckstein: Sonderfall

Die letzten beiden Steine der ersten Ebene lassen sich mit der oben genannten Technik ebenfalls positionieren. Die obere Ebene ist dann gelöst. Die Vektoreinträge  $x_{1-4}$  sind dann  $(0, 0, 0, 0)$ . Bei dem  $2 \times 2 \times 2$ -Würfel entspricht das Lösen der oberen Ebene sogar schon der Hälfte des Würfels. Die Algorithmen für die zweite Ebene sind in Abschnitt 8.8 zu finden.

## 8.8 Algorithmen für die zweite Ebene

Beim Lösen der zweiten Ebene muss beachtet werden, die erste Ebene nicht wieder zu verdrehen. Deshalb sind die Algorithmen hier länger, um spezifische Steine zu bewegen. In Abbildung 36 ist die obere Ebene des Würfels gelöst.



Abbildung 36: Würfel mit gelöster oberer Ebene

Ein Mensch dreht den Würfel zum Lösen der zweiten Ebene meistens um, damit die entsprechenden Steine sichtbar sind. Der Anschaulichkeit halber wird das hier auch gemacht.

Zuerst werden nun alle Steine der zweiten Ebene richtig ausgerichtet, so dass die obere Seite des Würfels ausschließlich gelbe Farbflächen zeigt. Der Vektor  $x$  ist dann 0. Danach werden die Steine getauscht, bis sie richtig angeordnet sind. Dann ist die Permutationsfunktion  $\sigma = 1$ .

Da es viele mögliche Würfelkonfigurationen und Algorithmen zur Lösung dieser gibt, werden die möglichen Steinpositionen und Algorithmen in einer Tabelle aufgeführt. Die

Algorithmen führen alle zu einer Würfelkonfiguration, bei der die untere (bereits gelöste) Ebene unverändert bleibt und die obere Seite ausschließlich gelbe Farbflächen zeigt. Viele dieser Algorithmen enthalten ( $RUR^{-1}U^{-1}$ ), was hier als Kommutator  $[R, U]$  geschrieben wird. Kommutatoren der Würfelzüge wurden in Abschnitt 8.2 behandelt.

Ausgangsposition	Algorithmus
	$F [R, U] [R, U] [R, U] F^{-1}$
	$F [R, U] [R, U] F^{-1}$
	$R U R^{-1} U R UU R^{-1}$
	$L^{-1} U^{-1} L U^{-1} L^{-1} UU L$
	$F [R, U] F^{-1}$
	$[R, U] [R^{-1}, F]$

Ausgangsposition	Algorithmus
	$F^{-1} [R, U] L^{-1} U L$

Die obere Seite des Würfels zeigt nach dem Ausführen dieser Algorithmen auf die entsprechenden Ausgangspositionen ausschließlich gelbe Farbflächen. Die Ausrichtung der Steine ist dann bereits richtig und der Vektor  $x$  somit  $(0, 0, 0, 0, 0, 0, 0, 0)$ . Wenn alle Steine der zweiten Ebene dann bereits richtig zueinander angeordnet sind, muss die Ebene eventuell mit  $U$ ,  $U^{-1}$  oder  $UU$  richtig zur ersten Ebene ausgerichtet werden. Ansonsten werden die Steinpositionen getauscht, bis sie richtig angeordnet sind.

Zum Vertauschen der Steine untereinander, ohne die Ausrichtung zu verändern, gibt es verschiedene Algorithmen. Diese Algorithmen werden im Folgenden in einer Liste aufgeführt. Die Pfeile zeigen an, welche Steine beim Ausführen der Algorithmen an welche Würfelposition gelangen.

Steinpermutation	Algorithmus
	$F R U^{-1} [R^{-1}, U^{-1}] R^{-1} F^{-1} [R, U][R^{-1}, F]$
	$[R, U] R^{-1} F RR U^{-1} [R^{-1}, U^{-1}] R^{-1} F^{-1}$
	$R B^{-1} R FF R^{-1} B R FF RR$

Nach dem Ausführen der passenden Algorithmen sind beide Ebenen gelöst. Eventuell müssen die beiden Ebenen noch durch  $U$ ,  $U^{-1}$  oder  $UU$  richtig zueinander ausgerichtet werden. Dann befindet sich der Würfel im gelösten Zustand und die Würfelkonfiguration ist somit  $(1, 0)$ .

Mit den Algorithmen aus dieser Anleitung kann jede valide Konfiguration eines  $2 \times 2 \times 2$ -Würfels in die Startkonfiguration  $(1, 0)$  überführt werden. Der beschriebene Ansatz ist die Fridrich-Methode.

## 9 Minimale Gruppe

In diesem Kapitel wird die Gruppe des  $2 \times 2 \times 2$ -Würfels mit minimalen Zügen realisiert. Die Gruppe des  $(G_{2 \times 2 \times 2}, \circ)$  ist eine vollständige Abbildung des  $2 \times 2 \times 2$ -Würfels – sie ist aber nicht minimal. Solch eine minimale Abbildung wird in diesem Kapitel definiert. Diese minimale Abbildung ist eine Untergruppe von  $(G_{2 \times 2 \times 2}, \circ)$ . Die Untergruppe der minimalen Abbildung des  $2 \times 2 \times 2$ -Würfels wird  $(G_{min}, \circ)$  genannt. Die Menge  $G_{min}$  enthält die Äquivalenzklassen der minimalen Züge des Würfels. Die Menge der minimalen Grundzüge erzeugt die Untergruppe  $(G_{min}, \circ)$ .

### 9.1 Minimale Grundzüge

Wie bereits in Abschnitt 2.2 beschrieben, sind die Züge  $U, D, R, L, F$  und  $B$  des  $2 \times 2 \times 2$ -Würfels nicht minimal. Die Züge  $U$  und  $D$  beispielsweise sind äquivalent, aber mit einer Rotation des kompletten Würfels. Die Menge der minimalen Züge ist  $\{U, R, F\}$ . Keiner dieser drei Grundzüge lässt sich durch einen anderen Zug oder eine Kombination anderer Züge darstellen. Der Stein  $dbl$  (unten, links, hinten) wird durch keinen dieser minimalen Züge bewegt. Das wird bei der Definition der minimalen Rotation des Würfels (Abschnitt 9.2) genauer beschrieben.

#### Minimale Permutationen

Bei den Permutationen dieser drei Grundzüge handelt es sich um die Permutationsfunktionen  $\sigma$ , die in Abschnitt 4.1 bereits definiert wurden. Es gibt jedoch nur drei statt sechs Funktionen für die Permutationen, da es auch nur drei Grundzüge gibt.

$$\begin{aligned}\sigma_U &= (\textit{ulf} \textit{ulb} \textit{urb} \textit{urf}) \\ \sigma_R &= (\textit{urb} \textit{drb} \textit{drf} \textit{urf}) \\ \sigma_F &= (\textit{ulf} \textit{urf} \textit{drf} \textit{dlf})\end{aligned}$$

#### Minimale Ausrichtung der Steine

In diesem Absatz wird die Ausrichtung der Steine minimal beschrieben. Das erfolgt über einen 8-dimensionalen Vektor  $x$ , der die Ober- und die Unterseite des Würfels und die sich dort befindenden Farbflächen der Steine abbildet. Die Definition des Vektors  $x$  der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  findet sich in Abschnitt 4.2.

Da der Stein an der Position  $dlb$  bei der minimale Untergruppe  $(G_{min}, \circ)$  immer als fest angenommen wird, ist der fünfte Vektoreintrag immer 0. Die Veränderung der Vektoreinträge kann durch die drei folgenden Funktionen vollständig abgedeckt werden.

$$\begin{aligned}\gamma_U ((x_1, x_2, x_3, x_4, 0, x_6, x_7, x_8)) \\ = (x_3, x_1, x_4, x_2, 0, x_6, x_7, x_8)\end{aligned}$$

$$\begin{aligned}\gamma_R ((x_1, x_2, x_3, x_4, 0, x_6, x_7, x_8)) \\ = (x_1, g(x_4), x_3, h(x_8), 0, h(x_2), x_7, g(x_6))\end{aligned}$$

$$\begin{aligned}\gamma_F ((x_1, x_2, x_3, x_4, 0, x_6, x_7, x_8)) \\ = (x_1, x_2, h(x_7), g(x_3), 0, x_6, g(x_8), h(x_4))\end{aligned}$$

## 9.2 Minimale Rotation des Würfels

Da die Grundzüge des Würfels für die minimale Abbildung die Züge  $U$ ,  $R$  und  $F$  sind, bleibt der Stein unten links hinten ( $dlb$ ) immer unbewegt. Keiner der minimalen Grundzüge oder eine Kombination daraus beeinflusst den Stein  $dlb$ . Der Würfel muss demnach nicht rotiert werden, da er anhand des Steines  $dlb$  eine feste Ausrichtung hat. Dieser Stein ist in Abbildung 37 hervorgehoben, der Würfel wird dort von hinten gezeigt. Es handelt sich dabei um den orange-grün-gelben Stein.



Abbildung 37: Würfel von hinten, farbig ist *fester Stein dlb*

Somit ist bei der minimalen Abbildung des  $2 \times 2 \times 2$ -Würfels keine Rotation des Würfels nötig, da sich die Ausrichtung des Würfels anhand des Steins *dlb* immer fest bestimmen lässt.

### 9.3 Erzeuger und Cayleygraph von $G_{min}$

Die Untergruppe  $(G_{min}, \circ)$  wird durch  $\{U, R, F\}$  erzeugt. Der vollständige Cayleygraph dieser Untergruppe hat 3 647 160 Mitglieder. Das ist die Anzahl der validen Würfelkonfigurationen. Da die Generierung des vollständigen Cayleygraphen zu umfangreich für den Rahmen dieser Arbeit ist, zeigt Abbildung 38 lediglich einen Ausschnitt dieses Graphen. Die roten Pfeile repräsentieren den Zug  $F$ .  $R$  wird durch blau repräsentiert und  $U$  durch grün.



Abbildung 38: Cayleygraph der Untergruppe  $G_{min}$

Am Knoten  $FFF$  kann man sehen, dass der Pfeil beim Hinzufügen eines weiteren  $F$  zurück zu  $N$  führt. Das liegt daran, dass  $FFFF$  und  $N$  aus der gleichen Äquivalenzklasse sind und den gleichen Zug repräsentieren. Bei einer Generierung des vollständigen Graphen, würde dieses zyklische Verhalten der Züge häufiger zu sehen sein.

### 9.4 Äquivalenz der Gruppen

In diesem Abschnitt wird bewiesen, dass die Mengen  $G_{2 \times 2 \times 2}$  und  $G_{min}$  gleichmächtig sind und somit beide eine vollständige Abbildung des  $2 \times 2 \times 2$ -Würfels sind.

Dazu wird zuerst gezeigt, dass die Züge der minimalen Untergruppe  $(G_{min}, \circ)$  ausreichen, um alle Züge des Würfels zu repräsentieren. Bei den Elementen der Mengen  $G_{2 \times 2 \times 2}$  und  $G_{min}$  handelt es sich um die Äquivalenzklassen der Züge. Die Elemente der Menge  $G_{2 \times 2 \times 2}$  können aus den Grundzügen  $U, D, R, L, F$  und  $B$  bestehen. Die Rotationen des Würfels werden hier nicht als Züge berücksichtigt, da die Äquivalenzklassen die Gleichheit von zwei Würfelkonfigurationen mit Rotation berücksichtigen. Jeder der Grundzüge  $U, D, R, L, F$  und  $B$  der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  kann durch einen der Grundzüge der minimalen Gruppe  $(G_{min}, \circ)$  dargestellt werden. Der Würfel kann dann verschieden rotiert sein, das wird aber durch die Äquivalenzklassen abgefangen, die die Gleichheit von zwei Zügen mit optionaler Rotation realisieren. In der folgenden Tabelle sind die Züge der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  und die dazugehörigen, minimalen Repräsentanten der Untergruppe  $(G_{min}, \circ)$  dargestellt:

$G_{2 \times 2 \times 2}$	$U$	$D$	$R$	$L$	$F$	$B$
$G_{min}$	$U$	$U$	$R$	$R$	$F$	$F$

So kann jeder Zug aus  $G_{2 \times 2 \times 2}$  mit den Zügen aus  $G_{min}$  dargestellt werden. Dabei muss die Ausrichtung des Würfels aber beachtet werden. Beispielsweise ruft der Zug  $ULF$  bei der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  eine äquivalente Würfelkonfiguration hervor, wie der Zug  $URU$  bei der Untergruppe  $(G_{min}, \circ)$ . Dadurch, dass er Zug nach Ausführen des Zuges  $L$  bzw.  $R$  unterschiedlich rotiert ist, verändert sich der Folgezug.

Wird also beispielweise der Zug  $L$  ausgeführt und in den Zug  $R$  überführt, um der minimalen Abbildung zu entsprechen, so müssen die folgenden Züge entsprechend verändert werden. Bei dem Zug  $L$  werden die Folgezüge wie folgt verändert:

$$\begin{array}{lll} \rho_L(U) = B & \rho_L(D) = F & \rho_L(R) = R \\ \rho_L(L) = L & \rho_L(F) = U & \rho_L(B) = D \end{array}$$

Bei den Zügen  $U, R, F$  bleiben die Folgezüge unverändert, da diese Züge in beiden Gruppen identisch sind. Bei den Zügen  $D, L, B$  werden die Folgezüge aufgrund der Würfelausrichtung verändert. Daraus ergibt sich die Überführung des Zuges  $ULF$  der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  zum Zug  $URU$  bei der minimalen Untergruppe  $(G_{min}, \circ)$ :

$$U \ L \ F \Rightarrow U \ R \ \rho_L(F) \Rightarrow U \ R \ U$$

Die Überführungsfunktionen alle Grundzüge sind im Folgenden definiert:

$$\rho_D(U) = U \quad \rho_D(D) = D \quad \rho_D(R) = F$$

$$\rho_D(L) = B \quad \rho_D(F) = L \quad \rho_D(B) = R$$

$$\begin{array}{lll} \rho_L(U) = B & \rho_L(D) = F & \rho_L(R) = R \\ \rho_L(L) = L & \rho_L(F) = U & \rho_L(B) = D \end{array}$$

$$\begin{array}{lll} \rho_B(U) = R & \rho_B(D) = L & \rho_B(R) = D \\ \rho_B(L) = U & \rho_B(F) = F & \rho_B(B) = B \end{array}$$

Anhand dieser Funktionen lassen sich alle Züge der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  in Züge der minimalen Gruppe  $(G_{min}, \circ)$  überführen. Die Funktionen  $\rho$  werden auf alle Elemente angewendet, die hinter dem entsprechendem Zug ausgeführt werden sollen. Die Funktion kann auch verschachtelt werden. Zur besseren Anschaulichkeit folgt noch ein Beispiel:

$$\begin{aligned} & U \ R \ F \ \mathbf{B} \ R \ L \ F \\ \Rightarrow & U \ R \ F \ F \ \rho_B(R) \ \rho_B(L) \ \rho_B(F) \\ \Rightarrow & U \ R \ F \ F \ \mathbf{D} \ U \ F \\ \Rightarrow & U \ R \ F \ F \ U \ \rho_D(U) \ \rho_D(F) \\ \Rightarrow & U \ R \ F \ F \ U \ U \ \mathbf{L} \\ \Rightarrow & U \ R \ F \ F \ U \ U \ R \end{aligned}$$

Somit kann jeder Zug der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  durch die minimalen Züge der Untergruppe  $(G_{min}, \circ)$  dargestellt werden. Die Mächtigkeit von  $G_{min}$  ist also mindestens so groß wie die von  $G_{2 \times 2 \times 2}$ . Sie kann aber nicht größer sein, da  $G_{2 \times 2 \times 2}$  aufgrund der Äquivalenzklassen genau die Anzahl der möglichen Züge, die nicht gleich sind enthält. Da  $(G_{min}, \circ)$  eine Untergruppe von  $(G_{2 \times 2 \times 2}, \circ)$  ist, kann  $G_{min}$  maximal so viele Elemente wie  $G_{2 \times 2 \times 2}$  enthalten.

Somit enthält auch  $G_{min}$  die Äquivalenzklassen aller möglichen Züge und ist eine vollständige Abbildung des  $2 \times 2 \times 2$ -Würfels.

## 9.5 Minimaler Lösungsweg

In diesem Kapitel wird ein Konzept zum Finden des optimalen Lösungsweges von jeder beliebigen Würfelkonfiguration ausgehend entworfen. Dazu werden verschiedene Bäume

modelliert und verglichen. Um die maximale Größe dieser Bäume zu berechnen, wird die *God's Number* benutzt.

Die *God's Number* des Würfels sagt aus, wie viele Züge zum Lösen des Würfels maximal gebraucht werden. Sie wurde am Ende von Abschnitt 8.4 bereits beschrieben. Bei der *Quarter-Turn* Metrik werden ausschließlich Vierteldrehungen der Ebenen als eine Ebenendrehung gezählt und die *God's Number* ist dann 14 [9]. Bei der *Half-Turn* Metrik werden auch halbe Drehungen einer Ebene als eine Ebenendrehung gewertet und somit ist die *God's Number* dann nur 11 [10].

Die Suche nach dem optimalen Lösungsweg, ausgehend von einer Konfiguration  $C$ , kann durch einen Baum realisiert werden. Um dies effizient zu gestalten, sollte der Baum möglichst klein sein. Im Folgenden werden verschiedene Ansätze für die Umsetzung eines solchen Baumes beschrieben. Die Implementierung dafür überschreitet den Umfang dieser Arbeit. Deshalb wird hier lediglich das Konzept entworfen und die Größe der jeweiligen Bäume berechnet und verglichen.

Ein Baum zum Berechnung der optimalen Lösung enthält eine Konfiguration  $C$  als Wurzel. Von diesem Startknoten ausgehend gibt es eine Kante für jeden möglichen Zug des Würfels. Diese Kanten führen jeweils zu einer Folgekonfiguration  $C_i$ , wobei der Index  $i$  die bisherigen Züge des Pfades im Baum enthält. So folgt dann auf jeden Knoten  $C_i$  über eine Kante  $Z$  ein Knoten  $C_{iZ}$  in der nächsten Ebene. Zu einem Knoten mit der Konfiguration  $C_i = (1, 0)$  führt der Pfad  $i$  im Baum, der einen Lösungsweg repräsentiert. Um die Länge eines Pfades zu bestimmen, muss die Anzahl der Ebenerotationen im Index  $i$  bestimmt werden. Diese Anzahl wird im Folgenden als  $|i|$  bezeichnet. Eine Konfiguration  $C_i$  wird nach  $|i|$  Zügen erreicht. So lässt sich die Länge des optimalen Lösungswegs auslesen.

Die Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  wird durch die Züge  $U, D, R, L, F$  und  $B$  erzeugt. Da diese Züge allerdings nicht minimal sind, reichen für einen Baum drei dieser Züge aus:  $U, R$  und  $F$ . Diese drei Züge erzeugen die Untergruppe  $(G_{min}, \circ)$ . Somit kann der minimale Baum von dieser Untergruppe ausgehend gebildet werden, da sie (genau wie  $(G_{2 \times 2 \times 2}, \circ)$ ) den kompletten Würfel abbildet.

Wenn man jeden möglichen Zug für die *Quarter-Turn* Metrik betrachtet, erhält man sechs Züge, da jede Ebene in zwei Richtungen gedreht werden kann. Es handelt sich dabei um die Züge  $F, F^{-1}, R, R^{-1}, U$  und  $U^{-1}$ .

Von jeder Konfiguration  $C_i$  ausgehend sieht der Baum dann so aus:



Abbildung 39: Lösungsbaum: *Quarter-Turn* Metrik

Jeder der Baumknoten hat demnach 6 Kinder. Da die *God's Number* in der *Quarter-Turn* Metrik 14 ist, ist der Würfel nach spätestens 14 Vierteldrehungen gelöst. Die Würfelkonfiguration ist dann  $C_i = (1, 0)$  mit  $|i| \leq 14$ .  $|i|$  entspricht dabei der Tiefe des Baums. Demnach hat der Baum eine maximale Größe von  $6^{14} = 78\ 364\ 164\ 096$  Knoten.

Für einen Baum mit minimaler Kinderanzahl fallen die Kanten  $F^{-1}$ ,  $R^{-1}$  und  $U^{-1}$  weg. Diese Züge können durch  $FFF$ ,  $RRR$  und  $UUU$  dargestellt werden. Jeder Knoten hat dann nur noch drei Kinder.



Abbildung 40: Lösungsbaum mit minimalen Kanten

Allerdings werden die Züge  $F^{-1}$ ,  $R^{-1}$  und  $U^{-1}$  durch jeweils drei Kanten dargestellt. Dadurch ergibt sich eine maximale Tiefe von  $|i| = 14 \cdot 3 = 42$ . Die maximale Größe des Baums ist somit  $3^{42} = 109\ 418\ 989\ 131\ 512\ 359\ 209$ .

Dementsprechend ist der Baum mit minimaler Kinderanzahl wesentlich größer als der oben beschriebene Baum der *Quarter-Turn* Metrik. Zur Berechnung des optimalen Lösungsweges ist der Baum der *Quarter-Turn* Metrik besser geeignet, da er durch seine geringere Knotenanzahl effizienter berechnet werden kann.

# 10 Fazit

## 10.1 Zusammenfassung und Ergebnis

In dieser Arbeit wurde die Gruppentheorie des  $3 \times 3 \times 3$ -Würfels auf den  $2 \times 2 \times 2$ -Würfel übertragen. Der  $3 \times 3 \times 3$ - wurde im Gegensatz zum  $2 \times 2 \times 2$ -Würfel bereits mehrfach untersucht. Die Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  des  $2 \times 2 \times 2$ -Würfels besteht aus der Menge aller Züge  $(G_{2 \times 2 \times 2})$  und dem Operator  $\circ$ , der zwei Züge aneinander hängt. Die Menge  $G_{2 \times 2 \times 2}$  enthält Äquivalenzklassen und somit werden äquivalente Züge von nur einem Element repräsentiert. Die Mächtigkeit von  $(G_{2 \times 2 \times 2}, \circ)$  ist daher die Anzahl der validen Würfelkonfigurationen, also ist  $|G_{2 \times 2 \times 2}| = 3\,674\,160$ . Die Rotation des kompletten Würfels wurde durch Äquivalenzrelationen realisiert. Außerdem wurden verschiedene Lösungswege für den Würfel beschrieben und auf die *God's Number* eingegangen. Diese ist beim  $2 \times 2 \times 2$ -Würfel 14.

Die Gruppe des  $2 \times 2 \times 2$ -Würfels veranschaulicht die Gruppentheorie an einem komplexen aber greifbaren Beispiel. Es können verschiedene Konzepte angewandt werden, wie Untergruppen, Erzeuger, zyklische Gruppen, Cayleygraphen, Gruppenoperationen, Kommutatoren, Äquivalenzrelationen, Mächtigkeit einer Gruppe, Ordnung von Gruppenelementen, Permutationen und Zykelbeschreibung. Außerdem wurde ein Baumkonzept zum Finden eines optimalen Lösungsweges entworfen.

## 10.2 Ausblick

In dieser Arbeit wurden Erzeuger und deren Cayleygraphen der Gruppe  $(G_{2 \times 2 \times 2}, \circ)$  beschrieben. Die Generierung des Cayleygraphen der kompletten Gruppe wäre eine interessante Idee für eine andere Arbeit. Außerdem könnte eine *GUI* zum Lösen des  $2 \times 2 \times 2$ -Würfels aufschlussreich sein, um effiziente Algorithmen zu finden und die Lösungswege des Würfels zu optimieren. Das kann auch mit dem Baum aus Abschnitt 9.5 realisiert werden. Ein weiterer interessanter Aspekt ist das Finden eines Algorithmus, der die Gleichheit zweier Züge berechnet. Das kann mit einem Termersetzungssystem (*Rewriting*) realisiert werden und wäre nötig, um einen korrekten Cayleygraphen der Gruppe zu generieren.

# Abbildungsverzeichnis

1	Ungelöster und gelöster $2 \times 2 \times 2$ -Würfel . . . . .	3
2	Eckstein und Farbfläche des Würfels . . . . .	4
3	Seite des Würfels . . . . .	4
4	Ungelöster und gelöster $3 \times 3 \times 3$ -Würfel . . . . .	4
5	Kant- und Mittelsteine . . . . .	5
6	Ebene des Würfels . . . . .	5
7	Cayleygraph von $(\mathbb{Z}/6\mathbb{Z}, +)$ mit Erzeuger 1 . . . . .	11
8	Zykel $\pi = (1\ 5\ 2)\ (3\ 4)$ . . . . .	15
9	Namen der Steinpositionen im Würfel . . . . .	18
10	Aufgeklappter Würfel mit Namen der Steinpositionen . . . . .	19
11	Steinpositionen nach Zug $U$ . . . . .	19
12	Markierungen $x_i$ (links), Farbflächennummern (rechts) . . . . .	21
13	Links: $x_1$ bis $x_8$ , rechts: Veränderung nach dem Zug $R$ . . . . .	22
14	Veränderung von Vektoreintrag $x_2$ bei Zug $R$ . . . . .	23
15	Würfel mit $x, y$ und $z$ -Achsen . . . . .	30
16	Würfel nach Rotation um $z$ -Achse . . . . .	31
17	Rotationsmöglichkeiten des Würfels mit der weißen Seite oben . . . . .	35
18	Würfel gelöst, nach Zug $F$ und nach $Z_r L$ . . . . .	36
19	Würfel nach Zügen $FR$ (links) und $RF$ (rechts) . . . . .	43
20	Ordnung des Zuges und der Permutation $LF$ . . . . .	45
21	Graph aller Zugpermutationen . . . . .	48
22	Zykel des Zuges $LLFF$ . . . . .	49
23	Cayleygraph zu Erzeuger $\{F\}$ . . . . .	58
24	Cayleygraph zu Erzeuger $\{FF, RR\}$ . . . . .	59
25	Würfel nach Zug $FUBRF^{-1}$ . . . . .	69
26	Lösung von Mensch: Schritt 1 . . . . .	70
27	Lösung von Mensch: Schritt 2 . . . . .	70
28	Lösung von Mensch: Schritt 3 . . . . .	71
29	Lösung von Mensch: Schritt 4 . . . . .	71
30	Lösung von Mensch: Schritt 5 . . . . .	71
31	Muster des $2 \times 2 \times 2$ -Würfels . . . . .	73
32	Lösung durch Schraubendrehermethode . . . . .	74
33	Ersten Eckstein positionieren . . . . .	75

34	Zweiten Eckstein positionieren . . . . .	75
35	Zweiter Eckstein: Sonderfall . . . . .	76
36	Würfel mit gelöster oberer Ebene . . . . .	76
37	Würfel von hinten, farbig ist <i>fester Stein dlb</i> . . . . .	81
38	Cayleygraph der Untergruppe $G_{min}$ . . . . .	82
39	Lösungsbaum: <i>Quarter-Turn Metrik</i> . . . . .	86
40	Lösungsbaum mit minimalen Kanten . . . . .	86
41	Vektor $x$ nach $\gamma_R(x)$ . . . . .	92
42	Vektor $x$ nach $\gamma_R(\gamma_R(x))$ . . . . .	92
43	Vektor $x$ nach $\gamma_R(\gamma_R(\gamma_R(x)))$ . . . . .	93
44	Vektor $x$ nach $\gamma_R(\gamma_R(\gamma_R(\gamma_R(x))))$ . . . . .	93
45	Rotationsmöglichkeiten des Würfels . . . . .	96

# Literatur

- [1] World Cube Association. *Rekorde*. Weltrekordliste. Online erhältlich unter <https://www.worldcubeassociation.org/results/records>; abgerufen am 09.02.2021.
- [2] Rubik's Brand. *Our heritage*. Website. Online erhältlich unter <https://www.rubiks.com/en-eu/about>; abgerufen am 04.02.2021. 2020 aktualisiert.
- [3] Janet Chen. *Group Theory and the Rubik's Cube*. Online erhältlich unter [http://people.math.harvard.edu/~jjchen/docs/Group\\_Theory\\_and\\_the\\_Rubik's\\_Cube.pdf](http://people.math.harvard.edu/~jjchen/docs/Group_Theory_and_the_Rubik's_Cube.pdf); abgerufen am 05.01.2021.
- [4] Tom Davis. *Group Theory via Rubik's Cube*. Online erhältlich unter <http://www.geometer.org/rubik/group.pdf>; abgerufen am 05.01.2021.
- [5] Daniel Duberg und Jakob Tideström. *Comparison of Rubik's Cube Solving Methods Made for Humans*. Abschlussarbeit. Stockholm, CSC School. 2015.
- [6] Roland Frisch. *Schnelle Lösung für den 2x2x2 Pocket Cube (Ortega Methode)*. Website. Online erhältlich unter <https://freshcuber.de/loesung-2x2x2-ortega/>; abgerufen am 31.01.2021. Publiziert am 19.04.2018.
- [7] Roland Frisch. *Zauberwürfel-Anfängerlösung Teil 1: Erste Ebene (weiß)*. Website. Online erhältlich unter <https://freshcuber.de/zauberwuerfel-loesung-teil1/>; abgerufen am 29.01.2021. Publiziert am 11.12.2017.
- [8] Tobias Glosauer. *Elementar(st)e Gruppentheorie*. Wiesbaden: Springer Spektrum, 2016.
- [9] David Joyner. *Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys*. Online erhältlich unter <https://mike.verdone.ca/media/rubiks.pdf>; abgerufen am 12.01.2021. Baltimore, USA: Johns Hopkins University Press, 2008.
- [10] Ryan Taylor McGregor. *Finding God's Number for the Rubik's Cube Using Computational Analysis*. Hofstra University, 2016.
- [11] Tomas Rokicki. "Towards God's Number for Rubik's Cube in the Quarter-Turn Metric". In: *The College Mathematics Journal* 45.4 (2014), S. 242–253. DOI: [10.4169/college.math.j.45.4.242](https://doi.org/10.4169/college.math.j.45.4.242).
- [12] Erño Rubik. US4378117A. 1983.

- [13] Olivier Sète. *Zur Zyklenschreibweise von Permutationen*. Website. Online erhältlich unter <https://www3.math.tu-berlin.de/Vorlesungen/SS10/LinAlg1/Permutationen.pdf>; abgerufen am 01.03.2021. 2010.
- [14] Anna Tripi. “Cayley Graphs of Groups and Their Applications”. Magisterarb. Missouri State University, 2017.

## A Übergangsfunktionen - Vektor $x$

Im Folgenden wird gezeigt, dass sich der Vektor  $x$  nach dem vierfachen Ausführen einer der Grundzüge wieder in seinem Ausgangszustand befindet.

$$\forall Z \in \{U, D, R, L, F, B\} . (\sigma, x) \cdot Z^4 = (\sigma', x)$$

Die Veränderung des Vektors erfolgt durch die Funktion  $\gamma$ . Diese Funktion wurde für jeden der Grundzüge in Abschnitt 4.2 definiert.

Zuerst wird die Veränderung des Vektors  $x$  anhand des Zuges  $R$  beispielhaft betrachtet. In den folgenden Abbildungen sind die Übergangsfunktionen der Vektoreinträge im Würfel dargestellt:

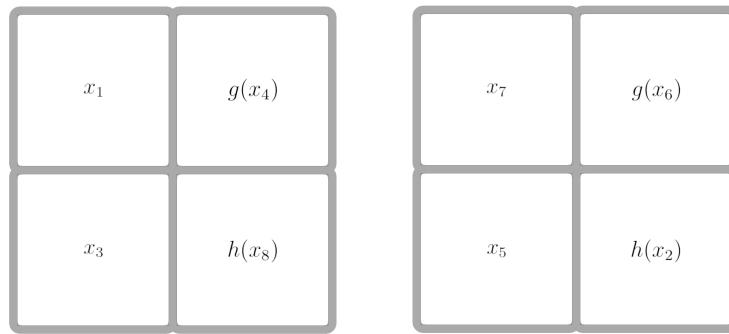


Abbildung 41: Vektor  $x$  nach  $\gamma_R(x)$

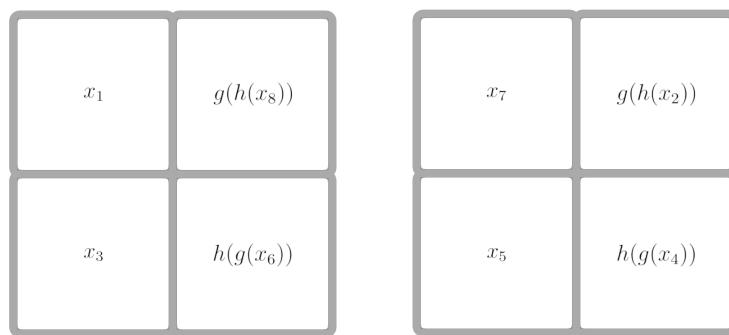


Abbildung 42: Vektor  $x$  nach  $\gamma_R(\gamma_R(x))$

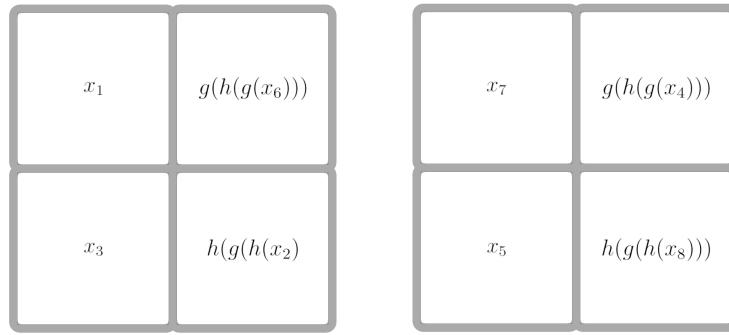


Abbildung 43: Vektor  $x$  nach  $\gamma_R(\gamma_R(\gamma_R(x)))$

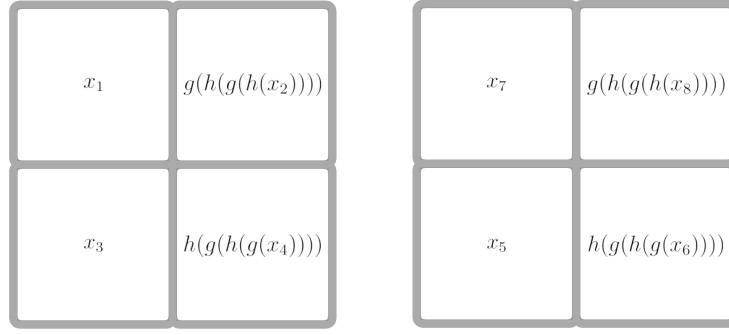


Abbildung 44: Vektor  $x$  nach  $\gamma_R(\gamma_R(\gamma_R(\gamma_R(x))))$

Im Folgenden ist die Veränderung des Vektors  $x$  durch den Zug  $R^4$  zu sehen. Die Funktionen  $g$  und  $h$  werden bei einer Verschachtelung von  $\gamma_R$  ebenfalls verschachtelt.

$$\begin{aligned} & \gamma_R(\gamma_R(\gamma_R(\gamma_R((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8))))) \\ &= (x_1, g(h(g(h(x_2)))), x_3, h(g(h(g(x_4)))), x_5, h(g(h(g(x_6)))), x_7, g(h(g(h(x_8)))) \end{aligned}$$

Die anderen Grundzüge verändern den Vektor bei vierfacher Ausführung folgendermaßen:

$$\begin{aligned} & \gamma_U(\gamma_U(\gamma_U(\gamma_U((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8))))) \\ &= ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \end{aligned}$$

$$\begin{aligned} & \gamma_D(\gamma_D(\gamma_D(\gamma_D((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8))))) \\ &= ((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \end{aligned}$$

$$\begin{aligned}\gamma_R(\gamma_R(\gamma_R((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)))) \\ = (x_1, g(h(g(h(x_2)))), x_3, h(g(h(g(x_4)))), x_5, h(g(h(g(x_6)))), x_7, g(h(g(h(x_8)))))\end{aligned}$$

$$\begin{aligned}\gamma_L((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = ((h(g(h(g(x_1)))), x_2, g(h(g(h(x_3)))), x_4, g(h(g(h(x_5)))), x_6, h(g(h(g(x_7)))), x_8))\end{aligned}$$

$$\begin{aligned}\gamma_F((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (x_1, x_2, h(g(h(g(x_3)))), g(h(g(h(x_4)))), x_5, x_6, g(h(g(h(x_7)))), h(g(h(g(x_8))))\end{aligned}$$

$$\begin{aligned}\gamma_B((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)) \\ = (g(h(g(h(x_1)))), h(g(h(g(x_2)))), x_3, x_4, h(g(h(g(x_5)))), g(h(g(h(x_6)))), x_7, x_8)\end{aligned}$$

Es ist ersichtlich, dass die Veränderungen bei vierfacher Ausführung des gleichen Zuges immer aus den Funktionsverschachtelungen  $g(h(g(h(x))))$  und  $h(g(h(g(x))))$  bestehen.  
Daher: muss folgendes gezeigt werden:

$$g(h(g(h(x)))) = x \quad h(g(h(g(x)))) = x$$

mit

$$g(x) = (x + 2) \bmod 3 \quad h(x) = (x + 1) \bmod 3$$

Dazu werden zuerst  $g(h(x))$  und  $h(g(x))$  berechnet.

$$\begin{array}{ll} g(h(x)) & h(g(x)) \\ = g((x + 1) \bmod 3) & = h((x + 2) \bmod 3) \\ = ((x + 1) \bmod 3) + 2 \bmod 3 & = ((x + 2) \bmod 3) + 1 \bmod 3 \\ = (x \bmod 3) + 1 + 2 \bmod 3 & = (x \bmod 3) + 2 + 1 \bmod 3 \\ = (x \bmod 3) + 3 \bmod 3 & = (x \bmod 3) + 3 \bmod 3 \\ = ((x \bmod 3) \bmod 3) & = ((x \bmod 3) \bmod 3 \\ = x \bmod 3 & = x \bmod 3 \\ = x & = x \end{array}$$

Der Ausdruck  $x \bmod 3$  kann in diesem Fall zu  $x$  umgeformt werden, da  $x \in \{0, 1, 2\}$ .

Da  $g(h(x)) = x$  und  $h(g(x)) = x$  gelten, gilt auch das Folgende:

$$g(h(g(h(x)))) = g(h(x)) = x \quad h(g(h(g(x)))) = h(g(x)) = x$$

Somit gilt:

$$\forall Z \in \{U, D, R, L, F, B\} . (\sigma, x) \cdot Z^4 = (\sigma', x)$$

## B Alle Rotationen des Würfels

Abbildung 45 zeigt alle Rotationsmöglichkeiten des Würfels. Der Würfel hat sechs Seiten, diese können jeweils vier Ausrichtungen haben. Die Rotationen wurden in Kapitel 5.2 definiert.

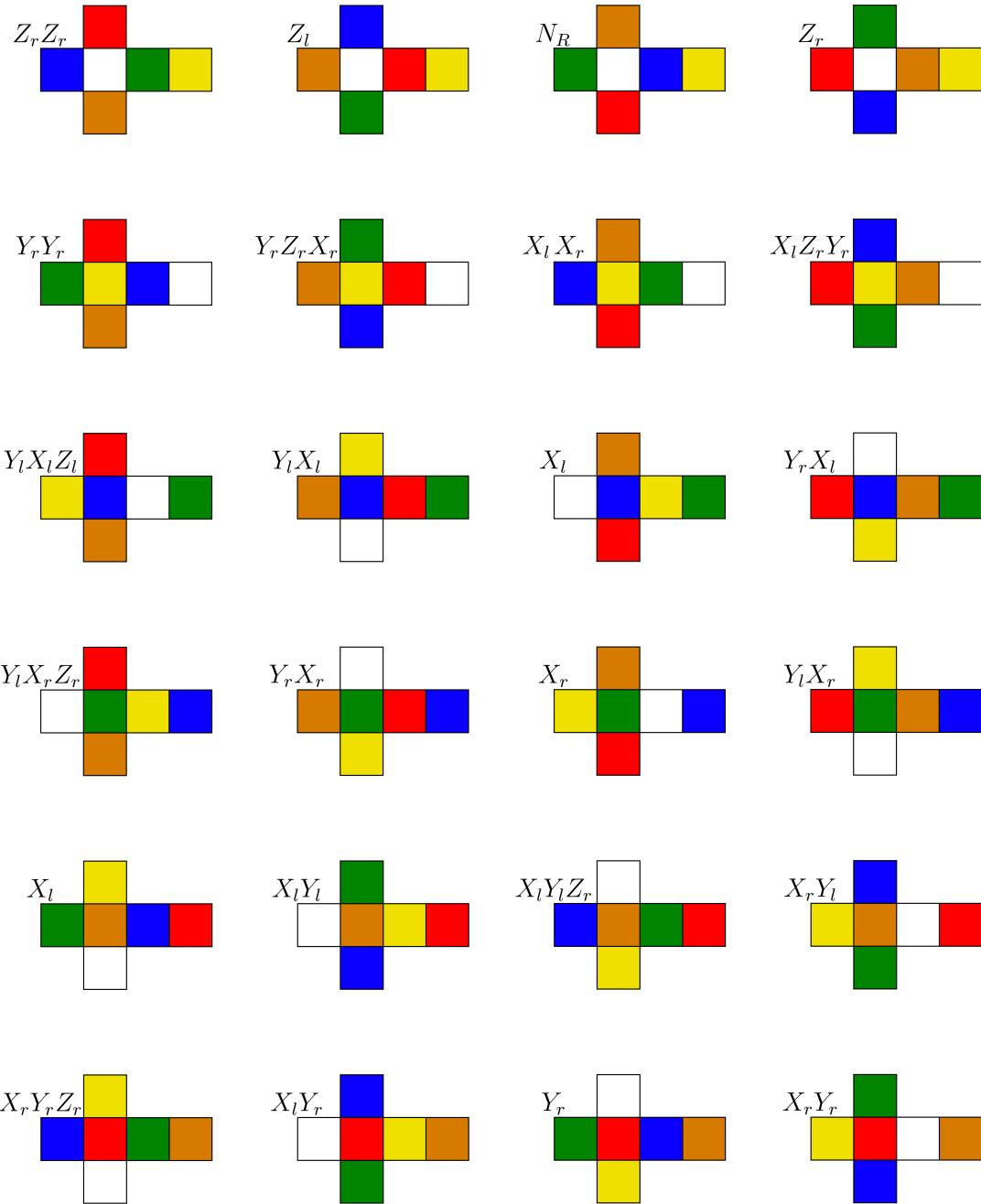


Abbildung 45: Rotationsmöglichkeiten des Würfels

In der folgenden Verknüpfungstafel sind alle Rotationsmöglichkeiten des Würfels abgebildet. Dafür wurde eine Tabelle von Tom Davis aus *Group Theory via Rubik's Cube* [4] auf die Syntax der Rotationen dieser Arbeit übertragen.

	$N_R$	$X_r$	$Y_r$	$Z_r$	$X_l$	$Y_l$	$Z_l$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$
$N_R$	$N_R$	$X_r$	$Y_r$	$Z_r$	$X_l$	$Y_l$	$Z_l$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$
$X_r$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_l$	$Y_l$	$Z_l$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$	
$Y_r$	$X_r Y_r$	$Y_r Y_r$	$Z_r Z_r$	$X_l$	$Y_l$	$Z_l$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$	
$Z_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r X_r$	$Z_l$	$Z_l$	$Y_l$	$Z_r Z_r$	$Y_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_l Y_l$	$Z_l Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_l Y_l$	$X_r X_r$	$Y_r Y_r$	$X_l X_r$	$Y_l Y_r$	$X_r X_r$	$Y_r Y_r$
$X_l$	$X_l N_R$	$X_l Y_l$	$X_l X_r$	$Y_l$	$X_l$	$Y_l$	$X_l N_R$	$X_l Y_l$	$X_l X_r$	$Y_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$						
$Y_l$	$X_l Y_l$	$X_l N_R$	$X_l X_r$	$Y_l$	$X_l$	$Y_l$	$X_l N_R$	$X_l Y_l$	$X_l X_r$	$Y_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$						
$Z_l$	$Z_l Y_l$	$X_l Y_l$	$X_l X_r$	$Y_l$	$X_l$	$Y_l$	$Z_l Y_l$	$X_l Y_l$	$X_l X_r$	$Y_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$	$X_l Z_r$	$X_l Y_l$						
$X_r X_r$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r$	$Y_r$	$Z_r$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$	$X_l Y_l Z_r$
$Y_r Y_r$	$Y_r Y_r$	$X_r X_r$	$Z_r Z_r$	$X_r$	$Y_r$	$Z_r$	$X_r X_r$	$Y_r Y_r$	$Z_r Z_r$	$X_r Y_r$	$Y_r X_l$	$X_l Y_l$	$X_l X_r$	$Y_l Y_r$	$X_r Y_l$	$X_l Y_r$	$X_r Z_r$	$Y_r Z_r X_r$	$Y_l X_l Z_l$	$X_l Z_l Y_r$	$Y_l X_r Z_r$	$X_l Y_l Z_r$	$X_l Y_l Z_r$
$Z_r Z_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r X_r$	$Z_r$	$Z_r$	$Y_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$
$X_r Y_r$	$X_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r$	$X_r$	$Y_r$	$X_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$
$Y_r X_r$	$Y_r X_r$	$X_r X_r$	$Z_r Z_r$	$Y_r$	$X_r$	$Y_r$	$Y_r X_r$	$X_r X_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$
$Z_r Y_r$	$Z_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r$	$X_r$	$Y_r$	$Z_r Y_r$	$X_r X_r$	$Z_r Z_r$	$Y_r Y_r$	$X_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$	$X_l Y_l$	$Z_r Y_l$	$Z_r Z_r$	$Y_r Y_r$
$X_l Y_l$	$X_l Y_l$	$X_l X_r$	$Z_l Z_l$	$Y_l$	$X_l$	$Y_l$	$X_l Y_l$	$X_l X_r$	$Z_l Z_l$	$Y_l Y_r$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$						
$Y_l X_l$	$Y_l X_l$	$X_l X_r$	$Z_l Z_l$	$Y_l$	$X_l$	$Y_l$	$Y_l X_l$	$X_l X_r$	$Z_l Z_l$	$Y_l Y_r$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$						
$Z_l Z_l$	$Z_l Z_l$	$Y_l X_l$	$X_l X_r$	$Y_l$	$X_l$	$Y_l$	$Z_l Z_l$	$Y_l Y_r$	$X_l X_r$	$Z_l Z_l$	$Y_l Y_r$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$	$X_l Y_l$	$X_l Z_l$
$X_l Y_r$	$X_l Y_r$	$X_l X_r$	$Z_l Z_l$	$Y_r$	$X_l$	$Y_r$	$X_l Y_r$	$X_l X_r$	$Z_l Z_l$	$Y_r Y_r$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$						
$Y_l X_r$	$Y_l X_r$	$X_l X_r$	$Z_l Z_l$	$Y_r$	$X_l$	$Y_r$	$Y_l X_r$	$X_l X_r$	$Z_l Z_l$	$Y_r Y_r$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$						
$Z_l Y_r$	$Z_l Y_r$	$X_l X_r$	$Z_l Z_l$	$Y_r$	$X_l$	$Y_r$	$Z_l Y_r$	$X_l X_r$	$Z_l Z_l$	$Y_r Y_r$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$	$X_l Z_l$	$X_l Y_r$						
$X_l Z_r$	$X_l Z_r$	$Y_l X_r$	$X_l X_r$	$Y_r$	$Y_l$	$X_r$	$X_l Z_r$	$Y_l X_r$	$X_l X_r$	$Y_r Y_r$	$Y_l X_r$	$Z_r X_r$	$X_l Z_r$	$Y_r Y_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$
$Y_l X_r$	$Y_l X_r$	$X_l X_r$	$Y_l Z_r$	$Z_r$	$Y_l$	$X_r$	$Y_l X_r$	$X_l X_r$	$Y_l Z_r$	$Z_r Y_r$	$Y_l X_r$	$Z_r X_r$	$X_l Z_r$	$Y_r Y_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$
$Z_l Z_r$	$Z_l Z_r$	$Y_l X_r$	$X_l X_r$	$Z_r$	$Y_l$	$X_r$	$Z_l Z_r$	$Y_l X_r$	$X_l X_r$	$Z_r Y_r$	$Y_l X_r$	$Z_r X_r$	$X_l Z_r$	$Y_r Y_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$	$Z_r X_r$	$Y_l X_r$
$X_l Y_l$	$X_l Y_l$	$X_l X_r$	$Z_l Z_r$	$Y_l$	$X_l$	$Y_l$	$X_l Y_l$	$X_l X_r$	$Z_l Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$
$Y_l Y_l$	$Y_l Y_l$	$X_l X_r$	$Z_l Z_r$	$Y_l$	$X_l$	$Y_l$	$Y_l Y_l$	$X_l X_r$	$Z_l Z_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$
$Z_l Y_l$	$Z_l Y_l$	$Y_l X_r$	$X_l X_r$	$Y_l$	$Y_l$	$X_r$	$Z_l Y_l$	$Y_l X_r$	$X_l X_r$	$Y_l Y_r$	$Y_l X_r$	$Z_r X_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$Y_l X_r$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$	$Y_l Y_r$	$X_l Y_l$	$Z_r X_r$

## C Persönliche Korrespondenz mit Jessica Fridrich

Da aus den verfügbaren Quellen nicht eindeutig hervorgeht, dass Jessics Fridrich die *CFOP-Methode* bzw. *Fridrich-Methode* erfunden hat, wurde sie persönlich per E-Mail gefragt. Im Folgenden ist ihre Antwort eingebunden.

**Betreff:** Re: [External Email] Fridrich method (cubing)

**Von:** "Jessica Fridrich" <fridrich@binghamton.edu>

**Datum:** Fr, 07.05.2021, 18:34

**An:** pina.kolling@tu-dortmund.de

Hi Pina,

thanks for writing. Yes, I indeed developed the CFOP method and also published it in 1983 in a Czech magazine Mlady Svet. I have copies of this. Plus, I have my old cubing notebook with hand-written notes that show all permutations and orientations with their probabilities and the shortest algorithms that I found. I attached a scan of a page from my 1982-83 cube notebook.

I am sure I am not the only one who co-invented a similar approach. I was the first one to popularize it on the Internet in 1997 though. Many times in science good ideas get reinvented.

Good luck with your project!

Jessica

## D Eidesstattliche Versicherung

### Eidesstattliche Versicherung (Affidavit)

Name, Vorname  
(Last name, first name)

Matrikelnr.  
(Enrollment number)

Ich versichere hiermit an Eides statt, dass ich die vorliegende Bachelorarbeit/Masterarbeit\* mit dem folgenden Titel selbstständig und ohne unzulässige fremde Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie wörtliche und sinngemäß Zitate kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

I declare in lieu of oath that I have completed the present Bachelor's/Master's\* thesis with the following title independently and without any unauthorized assistance. I have not used any other sources or aids than the ones listed and have documented quotations and paraphrases as such. The thesis in its current or similar version has not been submitted to an auditing institution.

Titel der Bachelor-/Masterarbeit\*:  
(Title of the Bachelor's/ Master's\* thesis):

\*Nichtzutreffendes bitte streichen  
(Please choose the appropriate)

Ort, Datum  
(Place, date)

Unterschrift  
(Signature)

#### Belehrung:

Wer vorsätzlich gegen eine die Täuschung über Prüfungsleistungen betreffende Regelung einer Hochschulprüfungsordnung verstößt, handelt ordnungswidrig. Die Ordnungswidrigkeit kann mit einer Geldbuße von bis zu 50.000,00 € geahndet werden. Zuständige Verwaltungsbehörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten ist der Kanzler/die Kanzlerin der Technischen Universität Dortmund. Im Falle eines mehrfachen oder sonstigen schwerwiegenden Täuschungsversuches kann der Prüfling zudem exmatrikuliert werden. (§ 63 Abs. 5 Hochschulgesetz - HG -).

Die Abgabe einer falschen Versicherung an Eides statt wird mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe bestraft.

Die Technische Universität Dortmund wird ggf. elektronische Vergleichswerkzeuge (wie z.B. die Software „turnitin“) zur Überprüfung von Ordnungswidrigkeiten in Prüfungsverfahren nutzen.

Die oben stehende Belehrung habe ich zur Kenntnis genommen:

#### Official notification:

Any person who intentionally breaches any regulation of university examination regulations relating to deception in examination performance is acting improperly. This offense can be punished with a fine of up to €50,000.00. The competent administrative authority for the pursuit and prosecution of offenses of this type is the chancellor of TU Dortmund University. In the case of multiple or other serious attempts at deception, the examinee can also be unenrolled, section 63, subsection 5 of the North Rhine-Westphalia Higher Education Act (*Hochschulgesetz*).

The submission of a false affidavit will be punished with a prison sentence of up to three years or a fine.

As may be necessary, TU Dortmund will make use of electronic plagiarism-prevention tools (e.g. the "turnitin" service) in order to monitor violations during the examination procedures.

I have taken note of the above official notification:\*\*

Ort, Datum  
(Place, date)

Unterschrift  
(Signature)

\*\*Please be aware that solely the German version of the affidavit ("Eidesstattliche Versicherung") for the Bachelor's/ Master's thesis is the official and legally binding version.