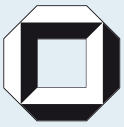
Robert Michael Zeier

Lie-theoretischer Zugang zur Erzeugung unitärer Transformationen auf Quantenrechnern



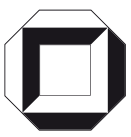
universitätsverlag karlsruhe

Robert Michael Zeier

Lie-theoretischer Zugang zur Erzeugung unitärer Transformationen auf Quantenrechnern

Lie-theoretischer Zugang zur Erzeugung unitärer Transformationen auf Quantenrechnern

von
Robert Michael Zeier



universitätsverlag karlsruhe

Dissertation, Universität Karlsruhe (TH)
Fakultät für Informatik, 2006

Impressum

Universitätsverlag Karlsruhe
c/o Universitätsbibliothek
Straße am Forum 2
D-76131 Karlsruhe
www.uvka.de

Universitätsverlag Karlsruhe 2006
Print on Demand

ISBN-13: 978-3-86644-081-4
ISBN-10: 3-86644-081-2

Lie-theoretischer Zugang zur Erzeugung unitärer Transformationen auf Quantenrechnern

zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften

von der Fakultät für Informatik
der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

Dissertation

von

Robert Michael Zeier

aus Großau

Tag der mündlichen Prüfung: 28.07.2006

Erster Gutachter: Prof. Dr. Jacques Calmet

Zweiter Gutachter: Prof. Dr. Steffen Glaser

Dritter Gutachter: Prof. Dr. Peter Sanders

Dank

An erster Stelle gilt mein Dank Professor Dr. Thomas Beth (1949-2005), der mich bei der Anfertigung dieser Arbeit unterstützt und bestärkt hat. Leider konnte er die Fertigstellung der Arbeit nicht mehr selbst miterleben. Seine algebraische Sicht auf die Informatik hat meine Denkweise und die vorliegende Arbeit entscheidend mitgeprägt.

Professor Dr. Jacques Calmet danke ich sowohl für die Übernahme des Referats als auch für die herzliche Unterstüzung in der Schlußphase der Dissertation und darüber hinaus. Besonders sein Vertrauen half mir in der Schlußphase der Dissertation. Weiter danke ich dem Korreferenten Professor Dr. Steffen Glaser für Diskussionen und Erläuterungen zum Thema der Arbeit, für die Begutachtung sowie für seine andauerende Unterstützung. Dem Korreferenten Professor Dr. Peter Sanders bin ich für die Begutachtung zu Dank verpflichtet.

Für ungezählte Diskussionen danke ich Dr. Markus Grassl: er ist immer bereit über Ideen zu diskutieren, Fragen zu beantworten und sein Wissen weiterzugeben. Für seine Hilfe und seinen Ratschlag vor, während und nach meiner Promotionszeit bin ich besonders dankbar. Weiterhin danke ich Dr. Dominik Janzing für viele Diskussionen und für sein Interesse an meiner Forschung. Dr. Thomas Schulte-Herbrüggen danke ich für viele Diskussionen und für die Einführung in (für mich) neue Sichtweisen und Fragestellungen.

Für die Auf- und Ermunterung bin ich Professor Dr. Dejan Lazic und Professor Dr. Hans-Hellmut Nagel verbunden. Professor Dr. Roland Vollmar danke ich für die Begleitung und die Unterstützung während der Schlußphase der Dissertation.

Meinen ehemaligen und aktuellen Kollegen aus der „Quantum Computing“-Gruppe Prof. Dr. Andreas Klappenecker, Dr. Jörn Müller-Quade, Dr. Martin Rötteler, Dr. Frank Schmüser und Professor Dr. Pawel Wocjan danke ich für die freundschaftliche Zusammenarbeit. Meinem Kollegen Dr. Thomas Decker danke ich für die Unterstüzung, insbesondere bei der (gemeinsamen) Bewältigung der Schlußphase der Promotionszeit. Professor Dr. Rainer Steinwandt danke ich für interessante Diskussionen über Fragen der Algebra. Bei allen meinen Kollegen bedanke ich mich für die freundschaftliche und aufgeschlossene Atmosphäre am Institut für Algorithmen und Kognitive Systeme. Den Sekretärinnen Carmen Helsberg, Rita Henke und Helga Scherer danke ich für ihre Hilfe bei organisatorischen Angelegenheiten.

Meinen Freunden Frank Dinies, Julian und Marc Endres, Christian Heuberger sowie Jürgen Lutz danke ich für viele Gelegenheiten zur Ablenkung und für ihr Verständnis für meine häufige Abwesenheit. Besonders dankbar bin ich meinen Eltern Michael und Susanna Zeier für ihre uneingschränkte Unterstützung und ihr Verständnis. Meinem Bruder Klaus Zeier danke ich für ungezählte Gespräche und für die damit verbundene Ablenkung.

Inhaltsverzeichnis

Einleitung

Eine zentrale Fragestellung der Informatik beschäftigt sich mit der effizienten Realisierung von Algorithmen auf Rechnern unter Verwendung einer gegebenen Menge von Grundoperationen. Im Kontext der Informationsverarbeitung mit Quantenrechnern untersucht diese Arbeit effiziente Methoden zur Erzeugung unitärer Transformationen. Nach den Gesetzen der Quantenmechanik bilden dabei die unitären Transformationen die durchführbaren Operationen und zugleich eine Beschreibungssprache für Algorithmen auf einem Quantenrechner. Die Menge der zu realisierenden Transformationen ist bei einem Quantenrechner kontinuierlich und nicht wie bei einem klassischen Rechner diskret. Aus diesem Grund bilden Methoden der Lie-Theorie zur Strukturanalyse von kontinuierlichen Gruppen eine wesentliche Grundlage für diese Arbeit.

In Abhängigkeit von einer gegebenen Menge von Grundoperationen werden unter anderem besonders kurze (in der Tiefe der Zerlegung) oder besonders zeiteffiziente Zerlegungen von unitären Transformationen in Grundoperationen untersucht. Diese Zerlegungen sind für Quantenrechner wesentlich beim Entwurf von effizienten Algorithmen sowie bei der experimentellen Umsetzung. Bei einer kontinuierlichen Menge von Grundoperationen führen effiziente Implementierungen zu kontrolltheoretischen Fragestellungen. Eine optimale Implementierung entspricht dann einem kürzesten Weg in der unitären Gruppe.

Ausgehend von niedrigdimensionalen Beispielen werden Methoden zur Lie-theoretisch motivierten Strukturanalyse der zugrundeliegenden Dynamiken entwickelt. Hierbei zielt die Strukturanalyse nicht nur darauf ab, effiziente Zerlegungen zu finden, sondern es gilt insbesondere auch, die unitären Transformationen mit hoher Implementierungskomplexität zu identifizieren sowie Eigenschaften zu untersuchen, die diese Transformationen kennzeichnen. Die vorliegende Arbeit leistet einen Beitrag zu einem besseren Verständnis der zugrundeliegenden Lie-theoretischen Struktur der Komplexität unitärer Transformationen und legt damit einen Grundstein für die Lösung hochdimensionaler Kontrollprobleme in der Quanteninformatik.

In **Kapitel 1** wird das mathematische Modell eingeführt, das dieser Arbeit zugrunde liegt. Zusätzlich werden die mit dem Modell verbundenen Fragestellungen diskutiert und exemplarisch am Beispiel der Quantenschaltkreise motiviert. Die kontrolltheoretische Natur der behandelten Fragestellungen wird durch eine Reduktion auf Kontrollprobleme in Lie-Gruppen aufgezeigt. Darauf aufbauend wird eine systematische Theorie entwickelt, die die Frage beantwortet, unter welchen Bedingungen eine Zerlegung unitärer Transformationen in Produkte von Elementen aus Einparameter-Gruppen (bzw. aus Einparameter-Halbgruppen) endlicher oder gleichmäßig beschränkter Anzahl möglich ist. Hierfür werden bekannte Ergebnisse verfeinert und ergänzt.

In Fortsetzung des Ansatzes aus dem voherigen Kapitel werden in **Kapitel 2** Ein-Qubit-Syteme behandelt. Ein-Qubit-Systeme sind in Anlehnung an das klassische Bit die kleinsten vorkommenden Systeme und bilden im allgemeinen die Grundbausteine von

Quantenrechnern. Wir beginnen mit einer Beschreibung der Geometrie der unitären Transformationen auf Ein-Qubit-Systemen, wobei wir damit insbesondere eine Sammlung von Analysewerkzeugen bereitstellen. Anschließend diskutieren wir ausgewählte Ansätze zur Erzeugung von unitärer Transformationen auf Ein-Qubit-Systemen. Für konkrete Beispiele bestimmen wir die minimale Anzahl von Elementen, die notwendig ist, jede unitäre Transformation auf Ein-Qubit-Systemen in Produkte von Elementen aus Einparameter-Gruppen zu zerlegen.

Das **Kapitel 3** beschäftigt sich mit diskreten Mengen von Grundoperationen. In diesem Fall können beliebige unitäre Transformationen bestenfalls approximiert werden. Wir untersuchen die Approximierbarkeit aller unitären Transformationen bezüglich einer gegebenen Menge von Grundoperationen und geben einen ausführlicheren und verfeinerten Beweis für ein aus der Literatur bekanntes Kriterium zur Approximierbarkeit an. Ist die Approximierbarkeit einer diskreten Menge von Grundoperationen gesichert, stellt sich die Frage nach einer (in der Tiefe der Zerlegung) effizienten Approximation aller speziell unitären Transformationen. Wir zeigen, daß die effiziente Approximierbarkeit für spezielle Mengen von Grundoperationen gefolgert werden kann, und wir erweitern damit ein in der Literatur bekanntes Ergebnis für die speziell unitäre Gruppe auf eine allgemeine Klasse von Lie-Gruppen.

In **Kapitel 4** werden Kontrollsysteme auf zwei oder mehreren Quantenbits betrachtet, wobei die Kontrollsysteme durch die Schrödingergleichung eine Zeitentwicklung erfahren. Zusätzlich wird angenommen, daß unitäre Transformationen, die nur auf einzelnen Quantenbits operieren, eine vernachlässigbare Zeitkomplexität besitzen. Bereits die effiziente Ereugung unitärer Transformationen auf Zwei-Qubit-Systemen ist von besonderem Interesse, da die Anwendung dieser Transformationen auf Quantensystemen mit mehreren Quantenbits die Erzeugung beliebiger unitärer Transformationen ermöglicht. Unter den gegebenen Annahmen werden Kriterien zur Charakterisierung und zur Bestimmung der Zeitkomplexität einer optimalen Kontrolle für die Erzeugung beliebiger unitärer Transformationen entwickelt. In diese Untersuchungen gehen die Lietheoretischen Methoden wesentlich ein. Im Fall von Zwei-Qubit-Systemen werden verschiedene Ansätze, die unter Benutzung unterschiedlichen Methoden von verschiedenen Autoren entwickelt wurden, auf Lie-theoretische Weise vereinheitlicht, und dabei können durch eine Unterscheidung nach infinitesimaler und globaler Zeitoptimalität in dem globalen Kontrollproblem weitere Freiheitsgrade identifiziert werden, die sich nicht in dem infinitesimalen Kontrollproblem widerspiegeln. Die zugrundeliegende Struktur der Kontrollprobleme kann Lie-theoretisch durch die Struktur eines symmetrischen Raumes beschrieben werden. In Kontrollsystemen mit mehr als zwei Quantenbits ist die Struktur des symmetrischen Raumes nur noch in einem sehr eingeschränkten Sinn vorhanden. Diese eingeschränkte Struktur eines symmetrischen Raumes kann aber dennoch in Verallgemeinerung eines in der Literatur bekannten Ansatzes von einer geraden auf eine allgemeine Anzahl von Quantenbits für die Bestimmung von unteren Schranken für die Zeitkomplexität verwendet werden. Zusätzlich kann dargelegt werden, daß die verwendeten Aspekte der symmetrischen Räume auch spezielle Verschränkungsmaße zur Charakterisierung von Quantenzuständen kennzeichnen.

Motiviert aus dem vorherigen Kapitel werden in **Kapitel 5** Methoden zur Analyse von Nebenklassen von allgemeinen unitären Transformation bezüglich der Untergruppe der auf einzelnen Quantenbits operierenden Transformationen entwickelt. Insbesondere

wird für die Nebenklassen die de-Rham-Kohomologie für den Fall von Quantensystemen mit zwei und drei Quantenbits bestimmt. Dabei werden insbesondere Aspekte der Lie-Theorie verwendet, die im **Anhang** systematisch eingeführt werden. In **Kapitel 6** geben wir einen Überblick über die Ergebnisse der Arbeit und einen Ausblick.

1. Modelle, Komplexitätsmaße und Grundoperationen

1.1. Zeitentwicklung und Zustandsübergang

Wir betrachten im folgenden endlichdimensionale und reine Quantensysteme, deren Quantenzustände durch Vektoren aus einem endlichdimensionalen komplexen Vektorraum mit Skalarprodukt (Hilbertraum) beschrieben werden (vgl. [Mes61, S. 245] und [Sak94, S. 11]). Falls ein Quantensystem sich zum Zeitpunkt t_0 im Zustand $|\alpha\rangle$ befindet, bezeichnen wir dies mit dem Zustand-Zeit-Tupel $|\alpha, t_0\rangle$. Die Zeitentwicklung eines reinen Quantenzustandes wird durch den Zeitentwicklungsoperator $\mathcal{U}(t_1, t_0)$ $(t_1 \geq t_0)$ beschrieben (vgl. [Mes61, S. 310] und [Sak94, S. 69]): $|\alpha', t_1\rangle = \mathcal{U}(t_1, t_0)|\alpha, t_0\rangle$. Der Zeitentwicklungsoperator genügt für $t_2 \geq t_1 \geq t_0$ den Gleichungen (siehe [Mes61, S. 311] und [Sak94, S. 70]):

$$\mathcal{U}(t_1, t_1) = \mathrm{Id}, \tag{1.1a}$$

$$\mathcal{U}(t_2, t_0) = \mathcal{U}(t_2, t_1)\mathcal{U}(t_1, t_0), \tag{1.1b}$$

$$(\mathcal{U}(t_1, t_0))^\dagger \mathcal{U}(t_1, t_0) = \mathrm{Id}. \tag{1.1c}$$

Ein Operator wird durch die Operation $()^\dagger$ transponiert und komplex konjugiert. Aufgrund von Gleichung (1.1c) bezeichnen wir den Zeitentwicklungsoperator $\mathcal{U}(t_1, t_0)$ als unitär (vgl. Anhang A.3). Durch die Schrödinger-Gleichung des Zeitentwicklungsoperators $\mathcal{U}(t, t_0)$ (siehe [Mes61, S. 311] und [Sak94, S. 72])

$$\frac{d}{dt}\mathcal{U}(t, t_0) = (-iH(t))\mathcal{U}(t, t_0) \tag{1.2}$$

ist die Zeitentwicklung eines Quantensystems unter Zuhilfenahme eines im allgemeinem zeitabhängigen Hamilton-Operators $H(t)$ festgelegt. Der Hamilton-Operator $H(t)$ wird als hermitesch $(H(t) = (H(t))^\dagger)$ vorausgesetzt (vgl. [Mes61, S. 312] und [Sak94, S. 71]) und wir verwenden die Konvention $\hbar = 1$, die auch in Gleichung (1.2) gilt.

Quantenzustände $|\alpha\rangle$ und $|\alpha'\rangle$ bezeichnen wir im folgenden als äquivalent $(\simeq)$, falls $|\alpha'\rangle = c|\alpha\rangle$ $(0 \neq c \in \mathbb{C})$ gilt. Wir erweitern diesen Äquivalenzbegriff auf Zustand-Zeit-Tupel: Verschiedene Zustand-Zeit-Tupel $|\alpha, t\rangle$ und $|\alpha', t'\rangle$ betrachten wir als äquivalent $(\simeq)$, falls $|\alpha'\rangle \simeq |\alpha\rangle$ gilt. Wir definieren eine Äquivalenzrelation $(\equiv)$ auf Zeitentwicklungsoperatoren: Die Zeitentwicklungsoperatoren $\mathcal{U}(t_2, t_1)$ und $\mathcal{U}(t_4, t_3)$ sind äquivalent, falls die Zustand-Zeit-Tupel $(\mathcal{U}(t_2, t_1)|\alpha, t_1\rangle)$ und $(\mathcal{U}(t_4, t_3)|\alpha, t_3\rangle)$ für alle Quantenzustände $|\alpha\rangle$ äquivalent sind.

Definition 1.1 (Zustandsübergangsoperator)**.** Eine Äquivalenzklasse von Zeitentwicklungsoperatoren (bzgl. $\equiv$) wird als Zustandsübergangsoperator bezeichnet.

Im Gegensatz zu [Gra01, S. 12] sprechen wir von einer kontinuierlichen Zeitentwicklung und einem diskretem Zustandsübergang. Der Zustandsübergangsoperator wird durch einen unitären Operator beschrieben. Da der Quantenzustand eines reinen Quantensystems nur bis auf ein globale Phase bestimmt ist (vgl. [Mes61, S. 296] und [Sak94, S. 11]), können wir den Zustandsübergangsoperator als Element der speziell unitären Gruppe (siehe Anhang A.3) wählen. Wir definieren auf der unitären Gruppe und der speziell unitären Gruppe eine Operatornormtopologie (siehe Anhang A.3).

Definition 1.2 (Implementierung)**.** Wird aus der Äquivalenzklasse eines Zustandsübergangsoperators U ein Zeitentwicklungsoperator $\mathcal{U}(t_1, t_0)$ ausgewählt, so daß die Bedingungen $|\alpha'\rangle \simeq U|\alpha\rangle$ und $|\alpha', t_1\rangle \equiv (\mathcal{U}(t_1, t_0)|\alpha, t_0\rangle)$ erfüllt sind, so wird der Zeitentwicklungsoperator $\mathcal{U}(t_1, t_0)$ als Implementierung des Zustandsübergangsoperators U mit der Implementierungszeit $\tau = (t_1 - t_0)$ bezeichnet.

Da die unitäre Gruppe nicht kommutativ ist, schränken wir die Bedeutung des Symbols $\prod$ für Elemente V_j aus der unitären Gruppe auf die folgende Bedeutung ein ($e, f \in \mathbb{Z}$):

$$\prod_{j=e}^{f} V_j := \begin{cases} \left(\prod_{j=e+1}^{f} V_j \right) V_e & \text{für } f \geq e, \\ \mathrm{Id} & \text{für } f < e. \end{cases}$$

Falls $f = \infty$, beschreibt das Symbol $\prod$ ein Element aus dem Abschluß konvergenter Produkte.

Definition 1.3 (Zerlegung)**.** Eine Zerlegung eines Zustandsübergangsoperators U in Zustandsübergangsoperatoren $\{V_i\}$ ist durch die Gleichung $U = \prod_{j=1}^{f} V_j$ ($f \in \mathbb{N} \cup \{\infty\}$) gegeben. Wir sprechen von f Zerlegungsschritten ($f \in \mathbb{N}$) oder von unendlich vielen Zerlegungsschritten ($f = \infty$).

Die zulässigen Zustandsübergangsoperatoren $\{V_i\}$ für eine Zerlegung werden aus einer Untermenge $\mathrm{U_{zul}}$ der unitären Gruppe gewählt, und wir verwenden in Abhängigkeit von $\mathrm{U_{zul}}$ die Anzahl der Zerlegungsschritte als Komplexitätsmaß $\xi_{\mathrm{U_{zul}}} := f$ für eine Zerlegung. Wir betrachten auch den Fall einer Zerlegung und anschließender Implementierung aller Zerlegungsschritte mit den jeweiligen Implementierungszeiten τ_i ($i \in \{1, \ldots, \xi_{\mathrm{U_{zul}}}\}$). In diesem Fall sprechen wir von einer Zerlegung mit der Implementierungszeit

$$\tau = \sum_{i=1}^{\xi_{\mathrm{U_{zul}}}} \tau_i.$$

Alle drei Fälle (Implementierung, Zerlegung und der Zerlegung mit anschließender Implementierung der Zerlegungsschritte) betrachten wir als Kontrollalgorithmen. Dabei unterscheiden wir die beiden Komplexitätsmaße Implementierungszeit τ und Anzahl der Zerlegungsschritte $\xi_{\mathrm{U_{zul}}}$.

Bemerkung. In dieser Arbeit bezeichnen wir einen Quantenrechner als einen Rechner, dessen Zustandsmenge die Menge der reinen Quantenzustände aus einem endlichdimensionalen komplexen Vektorraum ist und dessen Transformationen die unitäre (oder speziell unitäre) Gruppe bilden.

1.2. Quantengatter, Quantenschaltkreise und Universalität

Sei im folgenden ein endlichdimensionales Quantensystem $\mathcal{H}$ mit $\dim \mathcal{H} = d$ gegeben.

Definition 1.4 (Quantengatter)**.** Ein Quantengatter U ist ein unitärer Operator, der auf einem k-dimensionalen ($k \leq d$) komplexen Vektorraum operiert.

Andere Definitionen des Quantengatters sind in [Gru99, S. 81], [Gra01, S. 32] und [Röt01, S. 9] zu finden. Wir beschäftigen uns nun mit der Frage, wie eine Operation des Quantengatters U auf dem Quantensystem $\mathcal{H}$ definiert werden kann. Zuerst definieren wir eine Tensorproduktstruktur $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ auf $\mathcal{H}$, wobei $\mathcal{H}_i \otimes \mathcal{H}_j$ das Tensorprodukt (siehe z. B. [Bou74, Kap. II, §3.1, Def. 1]) der Vektorräume $\mathcal{H}_i$ und $\mathcal{H}_j$ bezeichnet. Dabei besteht $\mathcal{H}_i \otimes \mathcal{H}_j$ aus allen formalen $\mathbb{Z}$-linearen Kombinationen von Paaren $x \otimes y = (x, y) \in \mathcal{H}_i \times \mathcal{H}_j$, so daß für alle $x, x_1, x_2 \in \mathcal{H}_i$, $y, y_1, y_2 \in \mathcal{H}_j$ und $\lambda \in \mathbb{C}$ die Gleichungen $(x_1 + x_2) \otimes y = (x_1 \otimes y) + (x_2 \otimes y)$, $x \otimes (y_1 + y_2) = (x \otimes y_1) + (x \otimes y_2)$ und $(\lambda x) \otimes y = x \otimes (\lambda y)$ gelten. Wir erhalten, daß $\mathcal{H}_i \otimes \mathcal{H}_j$ ein (komplexer) Vektorraum der Dimension $\dim(\mathcal{H}_i) \cdot \dim(\mathcal{H}_j)$ ist. Und die Elemente $x_i \otimes y_j$ bilden für $i \in \{1, \ldots, \dim(\mathcal{H}_i)\}$ und $j \in \{1, \ldots, \dim(\mathcal{H}_j)\}$ eine Basis von $\mathcal{H}_i \otimes \mathcal{H}_j$, falls die Elemente x_i eine Basis von $\mathcal{H}_i$ und die Elemente y_j eine Basis von $\mathcal{H}_j$ bilden.

Definition 1.5 (Tensorproduktstruktur)**.** Eine Tensorproduktstruktur definiert auf einem endlichdimensionalen Quantensystem $\mathcal{H}$ eine Tensorzerlegung

$$\mathcal{H} = \bigotimes_{i \in [1,\ldots,n]} \mathcal{H}_i := \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$$

in die Quantensysteme $\mathcal{H}_i$, wobei $[1, \ldots, n]$ eine (geordnete) Sequenz bezeichnet.

Im folgenden verwenden wir oft Quantensysteme $\mathcal{H}$, die eine Tensorproduktstruktur $\mathcal{H} = \bigotimes_{i=1}^{n} \mathbb{C}^2$ besitzen. Wir folgen Schumacher und Wootters [Sch95, S. 2747] und bezeichnen in diesem Fall eine einzelne Tensorkomponente $\mathbb{C}^2$ als Qubit (Quantenbit). Gegeben eine (geordnete) Sequenz $I := [i_1, \ldots, i_{|I|}]$, sei $J := [i_{l_1}, \ldots, i_{l_m}]$ ($1 \leq l_1 < \ldots < l_m \leq |I|$) eine (geordnete) Teilsequenz von I. Wir benutzen die Notation $J \sqsubset I$, falls J eine (geordnete) Teilsequenz der (geordneten) Sequenz I ist. Weiterhin bedeutet die Notation $J \sqsubset \{1, \ldots, n\}$, daß J eine (geordnete) Teilsequenz einer Permutation von $[1, \ldots, n]$ ist. Zusätzlich benötigen wir die Delta-Funktion $\delta_{x,y}$ mit dem Wert 1 falls $x = y$ und dem Wert 0 sonst. Nun sind wir in der Lage, eine Operation des Quantengatters U auf dem Quantensystem $\mathcal{H}$ festzulegen:

Definition 1.6 (Einbettung)**.** Sei U ein Quantengatter, das auf einem k-dimensionalen ($k \leq d$) komplexen Vektorraum $\mathcal{H}$ mit Tensorproduktstruktur $\mathcal{H} = \bigotimes_{j=1}^{n} \mathcal{H}_j$ operiert, und sei $J \sqsubset \{1, \ldots, n\}$ eine (geordnete) Teilsequenz, so daß $\prod_{j \in J} \dim \mathcal{H}_j = k$ gilt. Wir bezeichnen $U[J]$ als eine Einbettung des Quantengatters U in das Quantensystem $\mathcal{H}$. Dabei operiert U auf dem Quantensystem $\bigotimes_{j \in J} \mathcal{H}_j$. Wir geben $U[J]$ explizit als unitären Operator auf $\mathcal{H}$ an:
Wir bezeichnen die Koordinaten von $U[J]$ mit $v, w \in \{0, \ldots, d-1\}$ und die Koordinaten von U mit $a, b \in \{0, \ldots, k-1\}$. Ferner sei $I := [1, \ldots, n]$ und $J = [j_1, \ldots, j_{|J|}]$. Für $i \in I$

durchlaufen die Zahlen $a_i, b_i \in \mathbb{N} \cup \{0\}$ die Werte 0 bis $(\dim \mathcal{H}_i - 1)$. Weiterhin definieren wir die Hilfswerte $p_i := \prod_{i'=i+1}^{n} \dim \mathcal{H}_{i'}$ $(i \in I;\ p_n = 1)$ und $q_l := \prod_{l'=l+1}^{|J|} \dim \mathcal{H}_{j_{l'}}$ $(l \in \{1, \ldots, |J|\};\ q_{|J|} = 1)$. Falls eine Belegung der a_i und b_i existiert, so daß $\sum_{i \in I} a_i p_i = v$, $\sum_{i \in I} b_i p_i = w$, $\sum_{l \in \{1,\ldots,|J|\}} a_{j_l} q_l = a$ und $\sum_{l \in \{1,\ldots,|J|\}} b_{j_l} q_l = b$ gilt, dann erhalten wir $(U[J])_{v,w} = U_{a,b}$, sonst erhalten wir $(U[J])_{v,w} = \delta_{v,w}$.

Bemerkung. Bei einer Einbettung werden Tensorkomponenten ausgewählt, auf denen das Quantengatter operieren kann. Dabei spezifiziert die Einbettung die Operation des Quantengatters auf dem Gesamtsystem, wobei die Operation von der Wahl des Quantengatters und der Tensorkomponenten abhängt.

Weiterhin erlauben wir auch, daß mehrere Quantengatter U_1 und U_2 gleichzeitig auf dem Quantensystem $\mathcal{H}$ operieren, falls die (geordneten) Sequenzen J_1 und J_2 keine gemeinsamen Elemente besitzen. Die gemeinsame Einbettung von U_1 und U_2 ist dann durch das Produkt $(U_1[J_1])\,(U_2[J_2])$ gegeben. Vergleichbare Methoden zur Angabe einer Einbettung eines Quantengatters sind in [Röt01, S. 9] und [KSV02, S. 58] zu finden. Dabei ist in [Röt01] (für Qubitsysteme) die Einbettung mittels einer Permutation der Tensorkomponenten definiert. In Ref. [KSV02, S. 58] wird (für Qubitsysteme) die Einbettung unter Benutzung einer Darstellung des Quantengatters in einer Tensorpoduktbasis definiert.

Definition 1.7 (Quantenschaltkreise)**.** Eine Zerlegung (Def. 1.3) eines Zustandsübergangsoperators $U = \prod V_i[J_i]$ in Produkte von Einbettungen $V_i[J_i]$ (Def. 1.6) der Quantengatter V_i (Def. 1.4) bezeichnen wir als Quantenschaltkreis.

Zwei aufeinanderfolgende Einbettungen $V_i[J_i]$ und $V_{i+1}[J_{i+1}]$ der Quantengatter V_i und V_{i+1} lassen sich zu einer Einbettung zusammenziehen und werden als äquivalent bezeichnet, falls die (geordneten) Sequenzen J_i und J_{i+1} keine gemeinsamen Elemente besitzen. In diesem Fall wird eine Zerlegung mit m Zerlegungsschritten in eine Zerlegung mit $m-1$ Zerlegungsschritten überführt. Die minimale Anzahl von Zerlegungsschritten eines äquivalenten Schaltkreises bezeichnen wir als die Tiefe des Schaltkreises. Wir bezeichnen die Tiefe eines Schaltkreises mit $\Xi_{\mathrm{U_{zul}}}$. Die Anzahl κ der Quantengatter eines Schaltkreises bezeichnen wir als die Größe des Schaltkreises. Bzgl. der Tiefe und Größe eines Schaltkreises verweisen wir zusätzlich auf [Gru99, S. 83], [Gra01, S. 32], [Röt01, S. 10] und [KSV02, S. 60].

Nun sind wir in der Lage, Grundoperationen für Quantenschaltkreise anzugeben: Als Grundoperationen wählen wir eine Teilmenge der Menge der Quantengatter. Wir verfeinern das Komplexitätsmaß der Anzahl κ der Gatter eines Quantenschaltkreises, indem wir die Menge der zu zählenden Quantengatter einschränken und die Anzahl κ_{G} der Quantengatter aus einer Teilmenge G der Grundoperationen zählen. Dabei können gleichzeitig unterschiedliche Komplexitätsmaße κ_{G_i} bzgl. verschiedenen Teilmengen G_i betrachtet werden.

Ausgangspunkt für die Einführung von Quantenschaltkreisen waren die Arbeiten von Toffoli und Fredkin [Tof80; Tof81; FT82] (vgl. auch [Ben73]) zur Analyse von klassischen reversiblen Schaltkreisen. Bei klassisch reversiblen Schaltkreisen zeichnet sich das Toffoli-Gatter $T(x, y, z) := (x, y, z + xy \mod 2)$ $(x, y, z \in \mathrm{GF}(2))$ als universelles Element aus ([Tof80, Thm. 5.3]): Jedes klassisch reversibles Gatter kann unter ausschließlicher Verwendung des Toffoli-Gatters, von Konstanten und ggf. unter Verwendung einer

Einbettung in einen größeren Schaltkreis realisiert werden. Da unitäre Operatoren reversibel sind, lassen sich klassisch reversible Gatter formal als unitäre Operatoren angeben, die nur auf der Standardbasis des komplexen Vektorraums operieren. Diese unitäre Operatoren führte Feynman [Fey85; Fey86] als Beispiele für Quantengattern ein. Zusätzlich zu den Quantenversionen der klassisch reversiblen Gatter sind nun aber alle unitäre Operatoren als Quantengatter denkbar (vgl. Def. 1.4).

Definition 1.8 (Universalität)**.** Eine Mengen von Grundoperationen ist universell, falls sich jede unitäre Operation durch Quantenschaltkreise unter ausschließlicher Verwendung der Grundoperationen darstellen läßt.

Falls wir Quantensysteme mit $\mathcal{H} = \bigotimes_{i=1}^{n} \mathbb{C}^2$ betrachten, sprechen wir von der Universalität für Qubitsysteme. Mit $\Lambda_k(U) := \mathrm{Id}_{n(2^k-1)} \oplus U$ (vgl. [Röt01, S. 129]) bezeichnen wir die von k Qubits kontrollierte Operation ([BBC$^+$95, S. 3458]) des Quantengatters $U \in \mathrm{U}(n)$. Aus ersten Quantenschaltkreisen [DS94; CW95; SW95a; SD96] wurde eine systematische Theorie [BBC$^+$95] (siehe auch [Cyb01]) zur Entwicklung von Quantenschaltkreisen mit einer geringen Anzahl κ von Gattern:

Faktum 1.9 ([BBC$^+$95])**.** Das Quantengatter $\Lambda_1(\sigma_\mathrm{x})$ ist zusammen mit allen auf einem Qubit operierenden Quantengatter (für Qubitsysteme) universell.

Wir erhalten insbesondere, daß die Menge der auf zwei Qubits operierenden Quantengatter (für Qubitsysteme) universell ist (vgl. auch die Ergebnisse zur approximativen Universalität in Abschnitt 3.1). Knill [Kni95] (siehe auch [AS03]) verbesserte für unitäre Operatoren $U \in \mathrm{U}(2^n)$ eine obere Schranke (aus [BBC$^+$95]) für κ in Abhängigkeit von n. Die folgende obere Schranke stimmt (für Qubitsysteme) asymptotisch mit der unteren Schranke $\kappa(U) \geq \lceil (4^n - 3n - 1)/4 \rceil$ aus [SMB04] überein.

Faktum 1.10 ([VMS04])**.** Für Qubitsysteme gilt: $\kappa(U) \in O(4^n)$ $(U \in \mathrm{U}(2^n))$.

Weitere Ergebnisse für Schaltkreise sind für zwei Qubits in den Arbeiten [SK03; BM03; SBM04; VD04; VW04; SS03; ZVSW03; ZVSW04b; ZVSW04a; SM05] zu finden. Mehr als zwei Qubits wurden in [BM04; MVBS04] untersucht. In der Arbeit [DBE95] wurde die Frage nach den nicht universellen Quantengattern gestellt:

Faktum 1.11 ([BB02b], vgl. auch [BDD$^+$02])**.** Gegeben sei ein d-dimensionaler komplexer Vektorraum $\mathcal{H}$ mit Tensorproduktstruktur $\mathcal{H} = \bigotimes_{j=1}^{n} \mathcal{H}_j$ $(\dim \mathcal{H}_j = k;\ n > 2)$. Eine diskrete Menge M von auf zwei Tensorkomponenten operierenden Quantengattern ist zusammen mit allen auf einer Tensorkomponente operierenden Quantengattern genau dann universell, falls M ein auf zwei Tensorkomponenten operierendes Quantengatter V enthält, das weder in seine Tensorkomponenten zerfällt $(V \neq V_1 \otimes V_2; V_1, V_2 \in \mathrm{U}(k))$ noch eine Komposition $(V \neq (V_1 \otimes V_2)P)$ eines in seine Tensorkomponenten zerfallenden Quantengatters mit einer (unitären) Permutation P der Tensorkomponenten ist.

1.3. Kontrollsysteme auf Lie-Gruppen

In den Arbeiten [RSD$^+$95; RR96; Llo96; Wea00a] (siehe auch [SH98, Anhang A]) wurde festgestellt, daß in der Quanteninformatik und bei Kontrollsystemen (vgl. [Jur97;

Sas99; HM94; Isi95; BK00]) auf Lie-Gruppen entsprechende Begriffsbildungen existieren. In der Quanteninformatik wird von der Universalität gesprochen, und dies entspricht der Kontrollierbarkeit für Kontrollsysteme auf Lie-Gruppen. Dabei behandelt schon die zentrale Arbeit von Jurdjevic und Sussmann [JS72] für die Quanteninformatik wesentliche Fragestellungen in einer kontrolltheoretischen Sprache. Wir führen das Konzept eines rechtsinvarianten Kontrollsystems auf einer Lie-Gruppe G mit der zugehörigen Lie-Algebra $\mathfrak{g}$ ein:

$$X(t) = X_0 + \sum_{j=1}^{m} v_j(t) X_j, \tag{1.3a}$$

$$\frac{d}{dt}x(t) = (X(t))x(t). \tag{1.3b}$$

Gleichung (1.3) definiert ein rechtsinvariantes Kontrollsystem $\mathbf{X} := (X_0, X_1, \ldots, X_m)$ auf einer Lie-Gruppe G, wobei $t \in \mathbb{R}$, $X(t), X_0, X_j \in \mathfrak{g}$, $x(t) \in \mathrm{G}$ und $v_j(t)$ Elemente einer Klasse von zulässigen Kontrollfunktionen sind. Zulässige Kontrollfunktionen sind Funktionen mit Werten aus einer festgelegten Teilmenge des $\mathbb{R}^m$ (vgl. [JS72, S. 315]). Wir sprechen von „Bang-Bang"-Kontrollfunktionen, falls die Kontrollfunktionen stückweise konstante Funktionen $v_j(t)$ sind, wobei $t \geq 0$ und $v_j(t)$ die Werte -1 oder $+1$ hat ([JS72, S. 315]). Allgemeiner können „Bang-Bang"-Kontrollfunktionen auch als meßbare Funktionen gewählt werden, deren Wertebereich aus dem Rand eines kompakten Gebietes besteht ([Jur97, S. 136]). Der Name „Driftterm" wird für X_0 verwendet, da dieser die Richtung beschreibt, in die sich das Kontrollsystem ohne Kontrolle entwickelt. Falls der Driftterm verschwindet, wird das Kontrollsystem homogen genannt. Der Ausdruck „rechtsinvariant" besagt, daß für $t' \leq t''$ jede Lösung von Gleichung (1.3) bzgl. den Randbedingungen $x(t') = g' \in \mathrm{G}$ und $x(t'') = g'' \in \mathrm{G}$ gleichzeitig für alle $g \in \mathrm{G}$ eine Lösung von Gleichung (1.3) bzgl. den Randbedingungen $x(t') = g'g$ und $x(t'') = g''g$ ist. Bezüglich eines Kontrollsystems $\mathbf{X}$ wird ein Element g'' einer Lie-Gruppe G als von $g' \in \mathrm{G}$ aus erreichbar bezeichnet, falls die Gleichung (1.3) für $t' \leq t''$ eine Lösung bzgl. den Randbedingungen $x(t') = g'$ und $x(t'') = g''$ hat. In Entsprechung zu dem Konzept der Universalität wird ein Kontrollsystem als „kontrollierbar" definiert, falls jedes Element der Lie-Gruppe von jedem anderen Element aus erreichbar ist.

Die Schrödinger-Gleichung (vgl. Gleichung (1.2)) paßt in das Konzept der Kontrollsysteme auf Lie-Gruppen:

$$H(t) = H_0 + \sum_{j=1}^{m} v_j(t) H_j, \tag{1.4a}$$

$$\frac{d}{dt}U(t) = (-iH(t))U(t). \tag{1.4b}$$

Dabei bezeichnet $U(t)$ einen unitären Operator, $v_j(t)$ die Kontrollfunktionen und $H(t)$ den zeitabhängigen Hamilton-Operator mit dem freien (oder Drift-) Hamilton-Operator H_0 und den Kontroll-Hamilton-Operatoren (diese werden auch rf-Hamilton-Operatoren genannt) H_j. Die kontrolltheoretischen Arbeiten [BS80; HTC83] haben die Anwendbarkeit von kontrolltheoretischen Methoden in der Quantenmechanik hervorgehoben.

Es bezeichne $\langle\langle X_1, \ldots, X_m \rangle\rangle$ die von der Menge $\{X_1, \ldots, X_m\}$ erzeugte Lie-Algebra und $\langle g_1, \ldots, g_m \rangle$ die von der Menge $\{g_1, \ldots, g_m\}$ erzeugte Lie-Gruppe.

Faktum 1.12 ([JS72, Theorem 7.1])**.** Eine notwendige Bedingung für die Kontrollierbarkeit eines Kontrollsystems **X** ist, daß die Lie-Gruppe G zusammenhängend ist und daß $\langle\langle X_0, X_1, \ldots, X_m\rangle\rangle = \mathfrak{g}$ gilt. Falls die Lie-Gruppe G zusätzlich kompakt oder das Kontrollsystem homogen ist, so ist die Bedingung sogar hinreichend.

Faktum 1.12 basiert auf der Arbeit von Chow [Cho39]. Dabei kann der wesentliche Inhalt von Faktum 1.12 durch die „Lie-Algebra-Rang-Bedingung“ ausgedrückt werden: Ein Kontrollsystem **X** auf einer zusammenhängenden und kompakten Lie-Gruppe G ist genau dann kontrollierbar, wenn der Rang der von $\{X_0, X_1, \ldots, X_m\}$ erzeugten Lie-Algebra gleich dem Rang der Lie-Algebra $\mathfrak{g}$ ist.

Einen Überblick und eine Vereinheitlichung verschiedenster Ansätze für einfach überprüfbare Bedingungen zur Kontrollierbarkeit (insbesondere in ausgewählten und konkreten Kontrollsystemen) gibt die Arbeit [Alt02].

1.4. Einparameter-Gruppen

Wir bezeichnen das Bild einer Lie-Gruppe G_1 unter einem Lie-Homomorphismus von G_1 in die Lie-Gruppe G_2 als virtuelle Lie-Untergruppe von G_2 (siehe [OV93, S. 38], [HHL89, S. 373] und [Bou89b, Kap. III, §6.2]). Eine virtuelle Lie-Untergruppe ist nicht notwendigerweise eine Lie-Untergruppe der Lie-Gruppe G_2 (vgl. [OV93, S. 14] und [Bou89b, Kap. III, §6.2, Prop. 2]). Als wichtigen Spezialfall betrachten wir Einparameter-Gruppen: diese entstehen als das Bild der Lie-Gruppe $\mathbb{R}$ unter einem Lie-Homomorphismus (vgl. [OV93, S. 44] und [Bou89b, S. 306]). Den Lie-Homomorphismus einer Einparameter-Gruppe bezeichnen wir oft auch als Einparameter-Gruppe. Ist X ein Element aus der Lie-Algebra $\mathfrak{g}$ von G, so können wir X eine Einparameter-Gruppe $t \mapsto \exp(tX)$ $(t \in \mathbb{R})$ zuordnen. Eine Einparameter-Gruppe $t \mapsto \exp(tX)$ gilt als kompakt, falls die Menge $\{\exp(tX) | \, t \in \mathbb{R}\}$ eine endliche Überdeckung mit Mengen der Form $\{\exp(tX) | \, r_1 < t < r_2\}$ $(r_1, r_2 \in \mathbb{R})$ besitzt (vgl. z. B. [Bou89a, Kap. I, §9.1, Axiom C''']).

Theorem 1.13 (vgl. [JS72, Lemma 6.2])**.** Sei G eine reelle, endlichdimensionale und zusammenhängende Lie-Gruppe. Wird die zugehörige Lie-Algebra $\mathfrak{g}$ von der Menge $\{X_j | \, 1 \leq j \leq m\}$ $(X_j \in \mathfrak{g})$ erzeugt, so kann jedes Element der Lie-Gruppe G als ein endliches Produkt von k Elementen der Form $\exp(t_i X_{j_i})$ $(t_i \in \mathbb{R};\ j_i \in \{1, \ldots, m\};$ $1 \leq i \leq k)$ dargestellt werden.

Beweis. Sei M die Gruppe endlicher Produkte von Elementen der Form $\exp(t_i X_{j_i})$. Da M wegzusammenhängend ist, ist M auch eine virtuelle Lie-Untergruppe von G ([Yam50; Got69], siehe auch [OV93, Thm. 2.4, S. 39], [HHL89, Thm. V.1.1] und [Bou89b, Kap. III, §8, Übungsaufgabe 4]). Aus den Voraussetzungen für G folgt (siehe [Bou89b, Kap. III, §1.1, Kor. zu Prop. 2], vgl. auch [Bou89a, Kap. I, §11.7]), daß die Topologie von M eine abzählbare Basis besitzt, d. h., es gibt eine abzählbare Menge T von offenen Teilmengen von M, so daß jede offene Teilmenge von M eine Vereinigung von Mengen aus T ist ([Bou89a, Kap. 1, §1.4, Def. 6]). Damit folgt insbesondere ([Bou89b, Kap. III, §6.4, Kor. 2 zu Prop. 10]), daß a genau dann in der Lie-Algebra $\mathfrak{l}(M)$ (vgl. z. B. [Bou89b, S. 306]) von M liegt, falls $\exp(ta)$ für alle $t \in \mathbb{R}$ in G liegt. Alle X_j $(1 \leq j \leq m)$ sind damit Elemente von $\mathfrak{l}(M)$. Da die Elemente X_j die Lie-Algebra $\mathfrak{g}$ erzeugen, gilt $\mathfrak{g} \subset \mathfrak{l}(M)$

(und insbesondere $\mathfrak{g} = \mathfrak{l}(M)$). Mit Hilfe von [Bou89b, Kap. III, §6.4, Kor. 2 zu Prop. 1] folgern wir, daß G eine virtuelle Lie-Untergruppe von M ist. Damit gilt $M = \mathrm{G}$ als Mengen und als Lie-Gruppen ([Bou89b, Kap. III, §6.2, Kor. 3 zu Prop. 13]). □

Bemerkung. Unter Verweis auf [Yam50] wurde im Beweis in [JS72] irrtümlicherweise direkt aus der Tatsache, daß M wegzusammenhängend ist, gefolgert, daß M eine Lie-Untergruppe ist.

Nach Lowenthal [Low71] bezeichnen wir eine Lie-Gruppe G von einer Menge von Einparameter-Gruppen $t \mapsto \exp(tX_j)$ ($t \in \mathbb{R}$; $X_j \in \mathfrak{g}$; $1 \leq j \leq m$) als gleichmäßig endlich erzeugt, falls ein $k \in \mathbb{N}$ existiert, so daß sich jedes Element der Lie-Gruppe G als ein Produkt von maximal k Elementen der Form $\exp(t_i X_{j_i})$ ($t_i \in \mathbb{R}$; $j_i \in \{1, \ldots, m\}$) darstellen läßt. Hierbei handelt es sich um eine endliche Zerlegung im Sinne von Def. 1.3. Das kleinstmögliche k ist eine obere Schranke für die Anzahl der Schritte $\xi_{\mathrm{U_{zul}}}$ der Zerlegung. Falls die Lie-Gruppe G von einer Menge von Einparameter-Gruppen $t \mapsto \exp(tX_j)$ ($t \in \mathbb{R}$; $X_j \in \mathfrak{g}$; $1 \leq j \leq m$) gleichmäßig endlich erzeugt wird, bezeichnen wir das kleinstmögliche k als die Ordnung $\mathrm{ord} = \mathrm{ord}(\mathrm{G}, \{X_j | \, 1 \leq j \leq m\})$ von G und der Menge der X_j. Falls kein endliches k existiert, legen wir die Ordnung als unendlich fest ($\mathrm{ord} = \infty$). Allgemein gilt (siehe z. B. [Sil86, S. 329]): $\mathrm{ord} \geq \dim(\mathrm{G})$.

Das Konzept der gleichmäßigen endlichen Erzeugung ist eng verwandt mit dem Konzept der Kontrollierbarkeit in einer beschränkten Anzahl von Schritten ([Kre74; Sus79; Sus83; Sus85; Vak98], vgl. auch [CS83; Sil85b; Sil85a; Sil86; D'A02]).

Aufbauend auf Teilergebnissen aus [Low71; Sil85b; Sil91a] zeigte D'Alessandro:

Faktum 1.14 ([D'A02, Thm. 2])**.** Sei G eine endlichdimensionale, zusammenhängende, reelle und kompakte Lie-Gruppe. Wird die zugehörige Lie-Algebra $\mathfrak{g}$ von der Menge $M := \{X_j | \, X_j \in \mathfrak{g}, \, 1 \leq j \leq m\}$ erzeugt, so wird G von den zugehörigen Einparameter-Gruppen gleichmäßig endlich erzeugt.

1.5. Einparameter-Halbgruppen

Wir sprechen von einer Einparameter-Halbgruppe, falls wir den Parameter t einer Einparameter-Gruppe auf positive ($t \geq 0$) Werte einschränken. Die Entsprechung von Theorem 1.13 ist für Einparameter-Halbgruppen falsch:

Beispiel 1.1. Wir führen die Lie-Gruppe

$$\mathrm{SL}(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R}; ad - bc = 1 \right\}$$

und deren Lie-Algebra

$$\mathfrak{sl}(2, \mathbb{R}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} \middle| \, \alpha, \beta, \gamma \in \mathbb{R} \right\}$$

ein. Die Lie-Algebra $\mathfrak{sl}(2, \mathbb{R})$ wird von den Elementen $X_1 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ und $X_2 = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ erzeugt (vgl. [Bou05, S. 70]). Aber das Element $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ der Lie-Gruppe $\mathrm{SL}(2, \mathbb{R})$ liegt nicht in der von den Einparameter-Halbgruppen (vgl. [Bou05, S. 75])

$$\exp(t_1 X_1) = \begin{pmatrix} 1 & t_1 \\ 0 & 1 \end{pmatrix} \; (t_1 \geq 0) \quad \text{und} \quad \exp(t_2 X_2) = \begin{pmatrix} 1 & 0 \\ t_2 & 1 \end{pmatrix} \; (t_2 \geq 0)$$

erzeugten Halbgruppe.

Wir werden nun untersuchen, welche mit Abschnitt 1.4 vergleichbare Aussagen noch für Einparameter-Halbgruppen gelten. Wir bezeichnen das Innere $\mathrm{int}(D)$ einer Teilmenge $D \subset \mathrm{G}$ einer Lie-Gruppe G als die Vereinigung aller (in G) offenen Teilmengen von D (vgl. [Bou89a, Kap. I, §1.6]). Mit Hilfe von [SJ72, Thm. 3.1] zeigte Hirschorn (vgl. auch die Bemerkung in [JS72, S. 321]):

Faktum 1.15 ([Hir73, Prop. 5], [HHL89, S. 377])**.** Ist G eine endlichdimensionale Lie-Gruppe und wird die zugehörige Lie-Algebra $\mathfrak{g}$ von einer Teilmenge $s \subset \mathfrak{g}$ erzeugt ($\mathfrak{g} = \langle\langle s \rangle\rangle$), dann ist das Innere $\mathrm{int}(D)$ von $D := \langle \exp(s) \rangle$ nicht leer ($\mathrm{int}(D) \neq \emptyset$).

Für zusammenhängende und kompakte Lie-Gruppen gilt weiterhin:

Faktum 1.16 ([HHL89, Prop. V.0.18])**.** Sei G eine zusammenhängende und kompakte Lie-Gruppe. Ist $S \subset \mathrm{G}$ eine Halbgruppe mit $\mathrm{int}(S) \neq \emptyset$, so gilt $S = \mathrm{G}$.

Aus Faktum 1.15 und Faktum 1.16 erhalten wir direkt folgende (eingeschränkte) Entsprechung zu Theorem 1.13:

Theorem 1.17 (vgl. auch [D'A02, Thm. 3])**.** Sei G eine reelle, endlichdimensionale, zusammenhängende und kompakte Lie-Gruppe. Wird die zugehörige Lie-Algebra $\mathfrak{g}$ von der Menge $\{ X_j | \, 1 \leq j \leq m \}$ ($X_j \in \mathfrak{g}$) erzeugt, so kann jedes Element der Lie-Gruppe G als ein endliches Produkt von k Elementen der Form $\exp(t_i X_{j_i})$ ($t_i \geq 0$; $j_i \in \{1, \ldots, m\}$; $1 \leq i \leq k$) dargestellt werden.

Weaver [Wea00b] zeigte im Spezialfall der unitären Gruppe: Die Menge der Paare von Einparameter-Halbgruppen, mit deren Hilfe nicht alle Elemente der unitären Gruppe als endliches oder unendliches Produkt darstellen werden können, ist vom Maß null in der Menge aller Paare von Einparameter-Halbgruppen.

Analog zu Einparameter-Gruppen bezeichnen wir eine Lie-Gruppe G von einer Menge von Einparameter-Halbgruppen $t \mapsto \exp(tX_j)$ ($t \geq 0$; $X_j \in \mathfrak{g}$; $1 \leq j \leq m$) als gleichmäßig endlich erzeugt, falls ein $k \in \mathbb{N}$ existiert, so daß sich jedes Element der Lie-Gruppe G als ein Produkt von maximal k Elementen der Form $\exp(t_i X_{j_i})$ ($t_i \geq 0$; $j_i \in \{1, \ldots, m\}$) darstellen läßt. Falls die Lie-Gruppe G von einer Menge von Einparameter-Halbgruppen $t \mapsto \exp(tX_j)$ ($t \geq 0$; $X_j \in \mathfrak{g}$; $1 \leq j \leq m$) gleichmäßig endlich erzeugt wird, bezeichnen wir das kleinstmögliche k als die (positive) Ordnung $\mathrm{ord}_+ = \mathrm{ord}_+(\mathrm{G}, \{ X_j | \, 1 \leq j \leq m \})$ von G und der Menge der X_j. Falls kein endliches k existiert, legen wir die Ordnung als unendlich fest ($\mathrm{ord}_+ = \infty$). Wir benötigen das folgende Ergebnis von Krener [Kre74, Thm. 1], und für Beweise beziehen wir uns auf [Sus85, S. 521], [Jak02, Thm. 3.10] und [AS04, Thm. 8.1].

Faktum 1.18 (Beweis von [Kre74, Thm. 1], vgl. auch [HHL89, Lemma IV.5.17])**.** Sei G eine reelle und endlichdimensionale Lie-Gruppe, wobei die zugehörige Lie-Algebra $\mathfrak{g}$ ($\dim(\mathfrak{g}) = n$) von der Menge $M := \{ X_j | \, X_j \in \mathfrak{g}, 1 \leq j \leq m \}$ erzeugt wird. Ferner bezeichne M' die Menge der Produkte von n Elementen der Form $\exp(t_i X_{j_i})$ ($t_i \geq 0$; $j_i \in \{1, \ldots, m\}$; $1 \leq i \leq n$) mit $\sum_{i=1}^{n} t_i < t$. Es gibt eine offene Umgebung U der Identität in G, so daß für jedes $t > 0$ gilt: $\mathrm{int}(M' \cap U) \neq \emptyset$.

Wir erhalten folgende Verallgemeinerung von Faktum 1.14:

Theorem 1.19 (vgl. [D'A02, Thm. 4])**.** Sei G eine reelle, endlichdimensionale, zusammenhängende und kompakte Lie-Gruppe. Wird die zugehörige Lie-Algebra $\mathfrak{g}$ von der Menge $M := \{X_j | X_j \in \mathfrak{g}, 1 \leq j \leq m\}$ erzeugt, so wird G von den zugehörigen Einparameter-Halbgruppen gleichmäßig endlich erzeugt.

Beweis. Sei $n = \dim(\mathfrak{g})$ und bezeichne M' die Menge der Produkte von n Elementen der Form $\exp(t_i X_{j_i})$ $(t_i \geq 0;\ j_i \in \{1, \ldots, m\};\ 1 \leq i \leq n)$ mit $\sum_{i=1}^{n} t_i < t$. Es gibt eine offene Umgebung U der Identität in G, so daß für jedes $t > 0$ gilt: $M'' := \mathrm{int}(M' \cap U) \neq \emptyset$ (Faktum 1.18). Wir erhalten:

$$\mathrm{G} = \bigcup_{G \in \mathrm{G}} GM''.$$

Da G kompakt ist, existiert eine endliche Zerlegung ([Bou89a, S. 84]):

$$\mathrm{G} = \bigcup_{i=1}^{k} G_i M'' \quad (G_i \in \mathrm{G}). \tag{1.5}$$

Nach Theorem 1.17 können alle G_i als endliches Produkt dargestellt werden und wir erhalten aufgrund von Gleichung (1.5), daß G gleichmäßig endlich erzeugt wird. □

In [D'A02, Thm. 4] findet sich ein ähnliches Ergebnis, aber wir zeigen hier Theorem 1.19 auf systematischere und andere Weise unter Benutzung von Faktum 1.18. Zustätzlich haben wir für Theorem 1.17 einen unabhängigen Beweis angegeben, der auf Faktum 1.15 und Faktum 1.16 beruht. In den Formulierungen fordern wir weiter explizit, daß die zugehörigen Lie-Gruppen endlichdimensional sind. Im Gegensatz zu [D'A02] benötigen wir nicht die Voraussetzung, daß die Erzeuger X_j linear unabhängig sind.

2. Kontrolle von Ein-Qubit-Systemen

2.1. Geometrie der Ein-Qubit-Operationen

Wir berichten in diesem Abschnitt über die Geometrie der Ein-Qubit-Operationen. Insbesondere erinnern wir an die Eigenschaften der Gruppen SU(2) und SO(3). Für die folgende Beschreibung haben wir die Referenzen [Gol50; May60; Pio66; Rob68; Bou71c; Kle79; Gra80; SW86; Alt05; Alt89; CG89; BIM90; Shu02; Shu93; Kle93; Rao96; Cox98; DK00; Mal00; PHG01; Cap02; Ver03; BS05] konsultiert. Diese Referenzen dienten als Überblick und Leitfaden zur Orginalliteratur, und wir verweisen auf diese Referenzen für eine ausführlichere Darstellung.

2.1.1. Rotationen und die Gruppe $\mathrm{SO}(3)$

Wir bezeichnen die Menge der Rotationen als die Menge der Transformationen, die den Abstand zu einem vorgegeben Punkt (z. B. den Ursprung) des Raumes fix lassen. Im folgenden sei der vorgegebene Punkt der Ursprung und der Abstand eines Punktes $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ zum Ursprung ist $|x| = \sqrt{x_1^2 + x_2^2 + x_3^2}$. Wir beginnen mit der Charakterisierung der Rotationen in einem dreidimensionalen reellen Vektorraum:

Theorem 2.1 ([Eul76a, §4-§12])**.** Alle Rotationen in einem dreidimensionalen reellen Vektorraum, die den Ursprung fix lassen, können durch Matrizen

$$M = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}$$

mit reellen Einträgen darstellen werden, so daß $M^T M = \mathrm{Id}$ gilt.

Beweis. Wir folgen [Eul76a] und betrachten für die Transformation $y = Mx$ mit $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ und $y = (y_1, y_2, y_3)^T \in \mathbb{R}^3$ die folgende Spezialfälle: Fall 1: $x_2 = x_3 = 0$ und $x_1 \neq 0$; Fall 2: $x_1 = x_3 = 0$ und $x_2 \neq 0$; Fall 3: $x_1 = x_2 = 0$ und $x_3 \neq 0$; Fall 4: $x_1 = 0$, $x_2 \neq 0$ und $x_3 \neq 0$; Fall 5: $x_1 \neq 0$, $x_2 = 0$ und $x_3 \neq 0$; Fall 6: $x_1 \neq 0$, $x_2 \neq 0$ und $x_3 = 0$. Da $|x| = |y|$ gilt, erhalten wir in den ersten drei Fällen die folgenden Gleichungen: 1. $A^2 + D^2 + G^2 = 1$; 2. $B^2 + E^2 + H^2 = 1$; 3. $C^2 + F^2 + I^2 = 1$. Im 6. Fall erhalten wir die Gleichung $x_1^2 + x_2^2 = (A^2 + D^2 + G^2)x_1^2 + (B^2 + E^2 + H^2)x_2^2 + 2(AB + DE + GH)x_1 x_2$ und es folgt $AB + DE + GH = 0$. Entsprechend erhalten wir im 5. Fall die Gleichung $BC + EF + HI = 0$ und im 4. Fall die Gleichung $AC + DF + GI = 0$. Womit wir die Bedingung $M^T M = \mathrm{Id}$ gezeigt haben. □

Euler [Eul71, §5-§8] zeigte, daß aus der Bedingung $M^T M = \mathrm{Id}$ die Bedingung $MM^T = \mathrm{Id}$ folgt. Dies kann algebraisch (und auf ähnliche Weise wie Euler) mit Hilfe einer kurzen Rechnung (z. B. mit dem Computeralgebrasystem Magma [BCP97]) nachvollzogen

werden. Aus einer kurzen Rechnung mit Magma folgt aus der Bedingung $M^T M = \mathrm{Id}$, daß die Determinante $\det(M)$ von M entweder gleich $+1$ oder -1 ist. Wir betrachten im folgenden nur noch den Fall $\det(M) = +1$, d. h. der Gruppe der sogenannten eigentlichen Rotationen, die wir mit dem Symbol SO(3) (vgl. z. B. [Ros02, S. 30] oder [SW86, Abschnitt 1.2]) bezeichnen:

$$\mathrm{SO}(3) = \left\{ M \in \mathrm{M}_3(\mathbb{R}) |\, M^T M = \mathrm{Id} \text{ und } \det M = 1 \right\}.$$

Wir suchen nun nach einer allgemeinen Parametrisierung der Gruppe SO(3):

Theorem 2.2 ([Eul71, §9-§11])**.** Eine allgemeine Parametrisierung eines Elementes

$$M = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}$$

der SO(3) kann auf folgende Weise gewählt werden:

$$A = \cos\zeta, B = -\sin\zeta\cos\eta, C = -\sin\zeta\sin\eta,$$
$$D = \sin\zeta\cos\theta, E = \sin\eta\sin\theta + \cos\zeta\cos\eta\cos\theta, F = -\cos\eta\sin\theta + \cos\zeta\sin\eta\cos\theta,$$
$$G = \sin\zeta\sin\theta, H = -\sin\eta\cos\theta + \cos\zeta\cos\eta\sin\theta \text{ und } I = \cos\eta\cos\theta + \cos\zeta\sin\eta\sin\theta.$$

Bemerkung. Im Gegensatz zu Referenz [Eul71] wählen wir eine Parametrisierung mit $\det(M) = 1$. Der Beweis benutzt Ideen aus [Eul71].

Beweis. Wir wählen $A = \cos\zeta$. Aus den Gleichungen $A^2 + D^2 + G^2 = 1$ und $A^2 + B^2 + C^2 = 1$ folgt $D^2 + G^2 = B^2 + C^2 = (\sin\zeta)^2$. Deshalb können wir die folgenden Parametrisierungen benutzen: $B = -\sin\zeta\cos\eta$, $C = -\sin\zeta\sin\eta$, $D = \sin\zeta\cos\theta$ und $G = \sin\zeta\sin\theta$. Wir können nun die Gleichungen $\cos(\alpha) = (1-t^2)/(1+t^2)$ und $\sin(\alpha) = 2t/(1+t^2)$ mit $t = \tan(\alpha/2)$ benutzen (vgl. z. B. [Kun01]) und die Kosinusse und Sinusse entsprechend ersetzen. Wir berechnen mit Magma für das von den Gleichungen für A,B,C,D und G sowie von den zu $M^T M = \mathrm{Id}$ gehörenden Gleichungen erzeugte Ideal die zugehörige Gröbnerbasis (siehe z. B. [BW93]). Danach berechnen wir für die Unbekannten E, F, H und I die Normalformen. Mit Hilfe des Computeralgebrasystems Maple [Map05] und der Gleichung $\tan(\alpha/2) = \sin\alpha/(1+\cos\alpha)$ erhalten wir aus den Normalformen die Parametrisierungen für die Unbekannten E, F, H und I. □

Die Gruppe SO(3) enthält insbesondere die Rotationen, die entgegen dem Uhrzeigersinn um die reellen Winkel α, β bzw. γ um die Koordinatenachsen eines dreidimensionalen reellen Vektorraums drehen (vgl. [Eul45, Anhang, Kapitel IV], Theorem 2.2 und [SW86, S. 7]):

$$\mathrm{R}_1(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix},$$
$$\mathrm{R}_2(\beta) = \begin{pmatrix} \cos\beta & 0 & \sin\beta \\ 0 & 1 & 0 \\ -\sin\beta & 0 & \cos\beta \end{pmatrix} \text{ und}$$
$$\mathrm{R}_3(\gamma) = \begin{pmatrix} \cos\gamma & -\sin\gamma & 0 \\ \sin\gamma & \cos\gamma & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ähnlich wie in [Eul45, Anhang, Kapitel IV] bilden wir das Produkt $\mathrm{R}_1(\theta)\mathrm{R}_3(\zeta)\mathrm{R}_1(-\eta)$ und wir erhalten die Matrix aus Theorem 2.2. Damit ist gezeigt, daß eine allgemeines Element aus SO(3) mit einer Rotation um die x-Achse, einer Rotation um die y-Achse und einer weiteren Rotation um die x-Achse darstellbar ist. Diese Art von Schlußfolgerung ist implizit in Referenz [Eul71] enthalten (vgl. z. B. [Rob68]). Aber ähnliche Parametrisierungen waren schon früher üblich (siehe z. B. [Eul45, Anhang, Kapitel IV]). Die Referenzen [CG89; Shu93; PHG01; Ver03] verweisen bezüglich dieser Art von Zerlegungen auf Referenz [Eul62]. Allgemein erhalten wir:

Theorem 2.3 (Euler-Winkel, siehe z. B. [Shu93, S. 454-455])**.** Die Gruppe SO(3) kann mit Hilfe von drei Rotationen $\mathrm{R}_{n_i}(\alpha_i)$ um drei orthogonale Rotationsachsen $n_i \in \mathbb{R}^3$ parametrisiert werden, d. h.

$$\mathrm{SO}(3) = \mathrm{R}_{n_1}(\alpha_1)\mathrm{R}_{n_2}(\alpha_2)\mathrm{R}_{n_3}(\alpha_3),$$

falls $n_1 \neq n_2$ und $n_2 \neq n_3$ gilt.

Mit Hilfe von geometrischen Argumenten zeigte Euler:

Faktum 2.4 (siehe z. B. [Eul76a, §24-§26])**.** Jede Rotation läßt eine Achse fix, so daß der Abstand eines Punktes zu der Achse vor und nach der Rotation gleich ist. Diese Achse wird als Rotationsachse bezeichnet.

In der Arbeit [Eul76b] entwickelte Euler die allgemeine Transformationsformel für eine Rotation, die durch Rotationsachse und Rotationswinkel festgelegt ist. Dabei benutzte er sphärische Trigometrie (siehe z. B. [Zei96, S. 769–775]).

Faktum 2.5 ([Eul76b, §4-§14])**.** Sei ϕ der Rotationswinkel und sei die Rotationsachse durch den Nullpunkt und die Koordinaten

$$r = (r_1, r_2, r_3)^T \in \mathbb{R}^3 \text{ mit } r_1 = \cos\alpha,\ r_2 = \cos\beta \text{ und } r_3 = \cos\gamma$$

festgelegt. Dann wird ein Punkt

$$x = (x_1, x_2, x_3)^T \in \mathbb{R}^3 \text{ mit } x_1 = \cos\zeta,\ x_2 = \cos\eta \text{ und } x_3 = \cos\theta$$

durch die Rotation auf den Punkt

$$y = (y_1, y_2, y_3)^T \in \mathbb{R}^3 \text{ mit } y_1 = \cos\zeta',\ y_2 = \cos\eta' \text{ und } y_3 = \cos\theta'$$

abgebildet, d. h. $y = Mx$ mit

$$M = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix},$$

wobei die Einträge der Matrix durch die Gleichungen

$$A = (\cos\alpha)^2 + (\sin\alpha)^2\cos\phi,\ B = \cos\alpha\cos\beta(1-\cos\phi) - \cos\gamma\sin\phi,$$
$$C = \cos\alpha\cos\gamma(1-\cos\phi) + \cos\beta\sin\phi,\ D = \cos\alpha\cos\beta(1-\cos\phi) + \cos\gamma\sin\phi,$$
$$E = (\cos\beta)^2 + (\sin\beta)^2\cos\phi,\ F = \cos\beta\cos\gamma(1-\cos\phi) - \cos\alpha\sin\phi,$$
$$G = \cos\alpha\cos\gamma(1-\cos\phi) - \cos\beta\sin\phi,\ H = \cos\beta\cos\gamma(1-\cos\phi) + \cos\alpha\sin\phi$$
$$\text{und } I = (\cos\gamma)^2 + (\sin\gamma)^2\cos\phi$$

gegeben sind.

Diese Formel wird heute oft in der folgenden Form dargestellt (vgl. [Rao96, S. 288-289] oder [Alt05, S. 74-75]):

$$M = \exp(\phi S) = \mathrm{Id} + (\sin\phi)S + (1 - \cos\phi)S^2,$$

wobei

$$S = \begin{pmatrix} 0 & -r_3 & r_2 \\ r_3 & 0 & -r_1 \\ -r_2 & r_1 & 0 \end{pmatrix}.$$

2.1.2. Die Gruppen SU(2) und SO(3)

Wir können die Menge der Ein-Qubit-Operationen als die speziell unitäre Gruppe der Dimension zwei (siehe z. B. [SW86, S. 12]) wählen (vgl. Abschnitt 1.1):

$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \middle| \, a, b \in \mathbb{C} \text{ mit } |a|^2 + |b|^2 = 1 \right\}. \tag{2.1}$$

Nach Euler [Eul71, §33] (vgl. [Jac84a, S. 606], [DK00, S. 12] und [Alt05, S. 133]) erhalten wir eine Abbildung von der Gruppe SU(2) in die Gruppe SO(3). Wir verwenden die Konvention aus Referenz [DK00, S. 12] und geben das Bild der Abbildung an:

$$\begin{aligned} N &= \begin{pmatrix} |a|^2 - |b|^2 & 2\Im(ab^*) & 2\Re(ab^*) \\ 2\Im(ab) & \Re(a^2 + b^2) & -\Im(a^2 - b^2) \\ -2\Re(ab) & \Im(a^2 + b^2) & \Re(a^2 - b^2) \end{pmatrix} \\ &= \begin{pmatrix} a_1^2 + a_2^2 - b_1^2 - b_2^2 & 2(-a_1b_2 + a_2b_1) & 2(a_1b_1 + a_2b_2) \\ 2(a_1b_2 + a_2b_1) & a_1^2 - a_2^2 + b_1^2 - b_2^2 & 2(-a_1a_2 + b_1b_2) \\ 2(-a_1b_1 + a_2b_2) & 2(a_1a_2 + b_1b_2) & a_1^2 - a_2^2 - b_1^2 + b_2^2 \end{pmatrix}, \end{aligned}$$

wobei wir die Notation aus Gleichung (2.1) sowie die Gleichungen $a = a_1 + a_2 i$ und $b = b_1 + b_2 i$ verwenden. (Dabei bezeichnet $\Re$ (bzw. $\Im$) den Realteil (bzw. den Imaginärteil) des Arguments.) Heute werden die komplexen Parameter a und b oft als Cayley-Klein-Parameter bezeichnet (siehe z. B. [Shu93, S. 470], [Rao96, S. 31] oder [Alt05, S. 131]). In der Orginalkonvention von Referenz [Eul71, §33] wurde anstatt N die Matrix N^T und in Referenz [Alt05, S. 133] wurde die Matrix PNP mit

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

verwendet. Es ist leicht zu überprüfen, daß die Matrix N reell und orthogonal ist. Weiter gilt $\det(N) = 1$ und es folgt, daß $N \in \mathrm{SO}(3)$. Zusätzlich gilt genau dann $N = \mathrm{Id}$, wenn das Urbild aus der Menge $\{\mathrm{Id}, -\mathrm{Id}\} \subset \mathrm{SU}(2)$ ist. Allgemein berechnen wir nun das Urbild der Abbildung bezüglich der Parametrisierung der Gruppe SO(3) aus Theorem 2.2. Wir benutzen die Notation $t_1 = \tan(\zeta/2) = \sin\zeta/(1+\cos\zeta)$, $t_2 = \tan(\eta/2) = \sin\eta/(1+\cos\eta)$ und $t_3 = \tan(\theta/2) = \sin\theta/(1+\cos\theta)$. Und wir erhalten mit Hilfe einer kurzen Rechnung

in Magma die beiden folgenden Lösungen für die Urbilder:

$$a_1 = \mp\frac{t_2t_3+1}{\sqrt{d}}, \tag{2.2a}$$

$$a_2 = \pm\frac{t_2-t_3}{\sqrt{d}}, \tag{2.2b}$$

$$b_1 = \pm\frac{t_1(t_2+t_3)}{\sqrt{d}}, \tag{2.2c}$$

$$b_2 = \pm\frac{t_1(t_2t_3-1)}{\sqrt{d}}, \tag{2.2d}$$

wobei $d = (t_1^2+1)(t_2^2+1)(t_3^2+1)$. Damit haben wir auf rein algebraische Weise folgendes Theorem gezeigt:

Theorem 2.6 (siehe z. B. [OV93, S. 25])**.** Es existiert ein 2-1-Abbildung von der Gruppe SU(2) auf die Gruppe SO(3).

Aufgrund von Gleichung (2.1) erhalten wir $a_1^2 + a_2^2 + b_1^2 + b_2^2 = 1$, und wir können sowohl die Gruppe SU(2) als auch die Gruppe SO(3) als Elemente der Einheitssphäre in einem vierdimensionalen reellen Vektorraum auffassen. Dabei werden für die Gruppe SO(3) gegenüberliegende Punkte der Einheitssphäre identifiziert (vgl. Gleichung (2.2), siehe auch [DK00, S. 8]).

2.1.3. Rodrigues' Formel

Unter Benutzung von sphärischer Trigometrie zeigte Rodrigues:

Faktum 2.7 ([Rod40, S. 408])**.** Seien zwei Rotationen R bzw. R' durch die Rotationsachsen

$$r = (r_1, r_2, r_3)^T \in \mathbb{R}^3 \text{ mit } r_1 = \cos\alpha,\ r_2 = \cos\beta \text{ und } r_3 = \cos\gamma$$

bzw.

$$r' = (r'_1, r'_2, r'_3)^T \in \mathbb{R}^3 \text{ mit } r'_1 = \cos\alpha',\ r'_2 = \cos\beta' \text{ und } r_3 = \cos\gamma'$$

sowie den Rotationswinkel ϕ bzw. ϕ' spezifiziert. Die Rotation $R'' = RR'$ wird nun durch ihre Rotationsachse

$$r'' = (r''_1, r''_2, r''_3)^T \in \mathbb{R}^3 \text{ mit } r''_1 = \cos\alpha'',\ r_2 = \cos\beta'' \text{ und } r_3 = \cos\gamma''$$

und ihren Rotationswinkel ϕ'' spezifiziert. Wir erhalten:

$$\begin{aligned}
\cos\frac{\phi''}{2} &= \cos\frac{\phi}{2}\cos\frac{\phi'}{2} - \sin\frac{\phi}{2}\sin\frac{\phi'}{2}(r_1r'_1 + r_2r'_2 + r_3r'_3)\\
\sin\frac{\phi''}{2}r''_1 &= \sin\frac{\phi}{2}\cos\frac{\phi'}{2}r_1 + \sin\frac{\phi'}{2}\cos\frac{\phi}{2}r'_1 + \sin\frac{\phi}{2}\sin\frac{\phi'}{2}(r_2r'_3 - r_3r'_2)\\
\sin\frac{\phi''}{2}r''_2 &= \sin\frac{\phi}{2}\cos\frac{\phi'}{2}r_2 + \sin\frac{\phi'}{2}\cos\frac{\phi}{2}r'_2 + \sin\frac{\phi}{2}\sin\frac{\phi'}{2}(r_3r'_1 - r_1r'_3)\\
\sin\frac{\phi''}{2}r''_3 &= \sin\frac{\phi}{2}\cos\frac{\phi'}{2}r_3 + \sin\frac{\phi'}{2}\cos\frac{\phi}{2}r'_3 + \sin\frac{\phi}{2}\sin\frac{\phi'}{2}(r_1r'_2 - r_2r'_1)
\end{aligned}$$

Wir bezeichnen die Parameter $\cos\frac{\phi}{2}$ und $\sin\frac{\phi''}{2}r = (\sin\frac{\phi''}{2}r_1, \sin\frac{\phi''}{2}r_2, \sin\frac{\phi''}{2}r_3)^T$ nach [Alt05, S. 160] als Euler-Rodrigues-Parameter. Ferner merken wir an, daß diese Parameter sich als Hamiltonsche Quaternionen [Ham44] auffassen lassen können (siehe [Cay45] oder [Alt05, Kap. 12]). Wir verweisen weiter darauf, daß die Formeln aus Theorem 2.7 auch schon Gauß bekannt waren, siehe [Gau00b].

2.2. Diskussion ausgewählter Ansätze

In diesem Abschnitt diskutieren wir exemplarisch Ansätze aus der Literatur zur Erzeugung von unitären Transformationen auf Ein-Qubit-Systemen.

In der Kernresonanz [EBW97] wird üblicherweise davon ausgegangen, daß (mindestens) die Grundoperationen $\exp(-it_1\sigma_x)$ und $\exp(-it_2\sigma_y)$ $(t_1, t_2 > 0)$ zur Verfügung stehen, d. h., daß es zwei Kontrollfunktionen im zugehörigen Kontrollsystem (siehe Abschnitt 1.3) gibt. In Anlehnung an Theorem 2.3 kann damit jede Ein-Qubit-Operation ausgeführt werden (vgl. [GC97, S. 353], [LKC+02, S. 234] oder [VC04, S. 1044]). Weiterhin wird die Rodrigues' Formel (Abschnitt 2.1.3) zur Analyse von Kernresonanz-Techniken in sogenannten zusammengesetzten Pulsen verwendet (siehe [CLE85], vgl. auch [Lev86, S. 76–77], [EBW97, S. 135] und [Lev96, S. 1405]). Für einen Überblick zu Kernresonanz-Techniken für zusammengesetzte Pulse verweisen wir auf [Lev86; Lev96].

Die Arbeiten [SWS93; WMS94] diskutieren Kontrollsysteme auf der Lie-Gruppe SO(3) mit zwei Kontrollfunktionen und finden in einem Kontrollsystem, daß einem Kontrollsystem auf der Lie-Gruppe SU(2) sehr ähnlich ist, die optimalen Kontrollen bzgl. eines speziell gewählten Optimalitätsmaß. Dabei verwenden die Autoren eine in diesem Fall anwendbare Technik, den Driftterm mit Hilfe einer Transformation des Kontrollsystems zu entfernen.

Vergleichbar zu den Arbeiten [SWS93; WMS94] wird in den Referenzen [DD00; DD01; D'A01] ein Kontrollsystem auf der Lie-Gruppe SU(2) mit zwei Kontrollfunktionen betrachtet. Dabei wird ein Optimalitätsmaß verwendet, das ähnlich zu einem Energiemaß ist. In den Referenzen [DD00; DD01; D'A01] wird dieses optimale Kontrollproblem gelöst: Die Autoren erhalten aus der Kernresonanz bekannte Lösungen als Lösungen dieses Kontrollproblems. (Ein ähnliches Kontrollproblem wird in Referenz [AD04] betrachtet.) Das Optimalitätsmaß Zeit wird in den Referenzen [BM06; BC05; BM05] im Fall von zwei Kontrollfunktionen behandelt, wobei die zwei Kontrollfunktionen Drehungen konstanter Geschwindigkeit um zwei nicht-orthogonalen Rotationsachsen steuern. Die Autoren ermitteln die zeitoptimalen Lösungen des Kontrollproblems und zeigen, daß alle zeitoptimalen Lösungen nur eine endliche Anzahl von Schritten (siehe z. B. Abschnitt 1.4) benötigen. Wir weisen auch noch auf die Arbeit [CHKO06] hin, in der ein spezielles Kontrollproblem analysiert wird, das auf einem Ein-Qubit-System die zeitoptimale Überführung von Zuständen behandelt.

In Referenz [ZW06] werden Kontrollsysteme mit einer Kontrollfunktion auf einem Ein-Qubit-System untersucht. Im Kontext von Zwei-Qubit-Systemen mit fester Wechselwirkung zwischen den Qubits wurden in Referenz [ZW06] Kontrollmethoden entwickelt, um beliebige Transformationen auf den zugehörigen Ein-Qubit-Systemen zeiteffizient durchzuführen.

Ramakrishna et. al. [ROS+00; RFRO00; Ram01a; Ram01b; ROFR01] zerlegen in Ver-

allgemeinerung von Theorem 2.3 Ein-Qubit-Operationen in Produkte von Exponentialfunktionen

$$\exp\left(i(\alpha(t)\sigma_x + \beta(t)\sigma_y + \delta(t)\sigma_z)\right) = \cos(\sqrt{\lambda(t)}) \cdot \mathrm{Id}_2 + \frac{i}{\sqrt{\lambda(t)}} \sin(\sqrt{\lambda(t)}) \cdot (\alpha(t)\sigma_x + \beta(t)\sigma_y + \delta(t)\sigma_z), \quad (2.3)$$

wobei $\lambda(t) = (\alpha(t))^2 + (\beta(t))^2 + (\delta(t))^2$ und $t \in \mathbb{R}$. Dabei betrachten sie insbesondere den Fall $\exp(i \cdot d\sigma_z)\exp(i \cdot e\sigma_x)\exp(i \cdot f\sigma_z)$ $(d, e, f \in \mathbb{R})$ und

$$\prod_{k=1}^{3} \exp(i(-\Im(\gamma_k)\sigma_y + \Re(\gamma_k)\sigma_x)) = \prod_{k=1}^{3} \begin{pmatrix} 0 & i\gamma_k \\ i\gamma_k^* & 0 \end{pmatrix} \qquad (\gamma_k \in \mathbb{C}).$$

2.3. Zerlegen in Einparameter-Gruppen auf Ein-Qubit-Systemen

In diesem Abschnitt betrachten wir ausgehend von Abschnitt 1.4 Einparameter-Gruppen auf Ein-Qubit-Systemen. Dabei basiert dieser Abschnitt teilweise auf den Abschnitten 4 aus den Referenzen [BGJ+03; BGJ+05]. Zur Erzeugung von unitären Transformationen seien m Einparameter-Gruppen

$$\{t \mapsto \exp(-i\mathrm{H}_1 t), t \mapsto \exp(-i\mathrm{H}_2 t), \ldots, t \mapsto \exp(-i\mathrm{H}_m t)\}$$

gegeben, die durch die unterschiedlichen Hamilton-Operatoren H_j induziert werden. Dabei ist es unser Ziel, jede unitäre Transformation U als ein Produkt von Elementen der gegebenen Einparameter-Gruppen darzustellen:

$$\mathrm{U} = \prod_{j=1}^{f} \exp(-i\mathrm{H}_{p_j} t_{p_j}), \quad \text{wobei } \mathrm{H}_{p_j} \in \{\mathrm{H}_1, \mathrm{H}_2, \ldots, \mathrm{H}_m\} \text{ und } t_{p_j} \in \mathbb{R}.$$

Wir betrachten die Anzahl der Zerlegungsschritte $\xi_{\mathrm{U}_{\mathrm{zul}}} = f$ (vgl. Seite 6) als Komplexitätsmaß. Dieses Komplexitätsmaß wurde in Referenz [Low71] als „order of generation“ bezeichnet. In einem physikalischem System entspricht $f - 1$ der Anzahl der Umschaltvorgänge zwischen unterschiedlichen Hamilton-Operatoren.

Wir diskutieren kurz die Bedingungen, damit die gegebene Menge von Hamilton-Operatoren jede unitäre Transformation erzeugen kann. Falls die Menge der Hamilton-Operatoren eine Unteralgebra der Lie-Algebra der unitären Transformationen erzeugt, deren Dimension gleich der Dimensionen der Lie-Algebra der unitären Transformationen ist, so folgt aufgrund der Lie-Algebra-Rang-Bedingung (siehe Faktum 1.12), daß jede unitäre Transformation erzeugt werden kann. Theorem 1.13 zeigt zusätzlich, daß die Anzahl der Zerlegungsschritte endlich ist. Da wir hier den Fall einer kompakten und zusammenhängenden Lie-Gruppe betrachten, wird nach Faktum 1.14 die Menge der unitären Transformationen gleichmäßig endlich erzeugt (vgl. Abschnitt 1.4).

Die Anzahl der Zerlegungsschritte hängt stark von den gegebenen Einparameter-Gruppen ab. Wir bestimmen nun Schranken für die Anzahl der Zerlegungsschritte im

Fall von bis zu drei Hamilton-Operatoren aus der Lie-Algebra su(2) der unitären Transformationen auf Ein-Qubit-Systemen. Wir beschreiben die Hamilton-Operatoren als infinitesimale Rotationen der Bloch-Sphäre. Die Bloch-Sphäre (vgl. z. B. [NC00, S. 15]) ist dabei eine geometrische Beschreibung von (normierten) Zuständen eines Qubits in der Einheitssphäre im dreidimensionalen reellen Raum. Der Nordpol der Bloch-Sphäre entspricht dem Zustand $|0\rangle$ und der Südpol dem Zustand $|1\rangle$. Ein allgemeiner Zustand $|\Psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$ (normiert und ohne globale Phase) wird durch einen (normierten) Vektor in der Bloch-Sphäre dargestellt, der mit der z-Achse den Winkel θ einschließt und dessen Projektion in die x-y Ebene mit der x-Achse den Winkel ϕ einschließt. Wir verwenden dabei ein linkshändiges Koordinatensystem, bei dem die z-Achse vom Mittelpunkt der Bloch-Sphäre auf den Nordpol der Bloch-Sphäre zeigt. Dabei können wir die Anwendung der Hamilton-Operatoren durch die stereographische Projektion (siehe z. B. [Ber87a, 4.3.8]) der Bloch-Sphäre auf die komplexe Zahlenebene abbilden. Das Bild der Bloch-Sphäre entspricht dabei der Einpunktkompaktifizierung $\bar{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ der komplexen Zahlen. Es ist bekannt, daß die Rotationen der Sphäre im dreidimensionalen reellen Raum den Möbius-Transformationen (vgl. Referenz [Gau00a], Referenz [For51, Kapitel 1], Referenz [Sch79], Referenz [Ber87b, Abschnitt 18.10.2], Referenz [Cox98, Abschnitt 14.6] und Referenz [SW86, Abschnitt 1.3]) der folgenden Form entsprechen ([Sch79, Abschnitt 12.b]):

$$z \mapsto \frac{az - c^*}{cz - a^*}, \quad \text{wobei } aa^* + cc^* = 1.$$

Der Orbit einer solchen Möbius-Transformation bildet in der komplexen Zahlenebene einen apollonischen Kreis (vgl. Referenz [Cox89, Abschnitt 6.6] oder Referenz [Ogi90, Kapitel 2]).

Wir betrachten nun den Fall von zwei Hamilton-Operatoren und folgen Ideen von Referenz [Low71]. Da die Hamilton-Operatoren mit infinitesimalen Rotationen in der Bloch-Sphäre identifiziert werden, nehmen wir ohne Beschränkung der Allgemeinheit an, daß eine Rotationsachse in der z-Achse liegt und daß die andere Rotationsachse in der x-z-Ebene liegt. Die Orbits der beiden Hamilton-Operatoren entsprechen in der komplexen Zahlenebene Systemen von apollonischen Kreisen. Wir verfolgen die abwechselnde Anwendung der beiden Hamilton-Operatoren auf dem Zustandsraum. Dabei starten wir im Nullpunkt der komplexen Zahlenebene, wobei dies dem Südpol der Bloch-Sphäre und damit dem Zustand $|1\rangle$ entspricht. Beim Übergang von einem Kreis zum nächsten tangentialen Kreis verwenden wir einen Raffke-artigen Algorithmus (vgl. [CLR90, Kap. 17]), um die ganze komplexe Zahlenebene abzudecken. Die tangentialen Kreise werden auf folgende Weise berechnet ([Sch79, S. 5–8]): Die Kreise $\mathcal{C}_i$ ($i \in \{1, 2\}$) werden mit der Gleichung

$$\mathcal{C}_i = A_i z z^* + B_i z + C_i z^* + D_i = 0$$

beschrieben, wobei $A_i, D_i \in \mathbb{R}$, $B_i, C_i \in \mathbb{C}$ und $B_i = C_i^*$. Ferner sei $\Delta_i = |\mathcal{C}_i| = A_i D_i - B_i C_i$. Im System $\mathcal{C} = \lambda_1 \mathcal{C}_1 + \lambda_2 \mathcal{C}_2$ von Kreisen, wobei λ_1, λ_2 reell und nicht beide null sind, sind zwei Kreise tangential, falls

$$(A_1 D_2 + A_2 D_1 - B_1 C_2 - B_2 C_1)/2 = \sqrt{\Delta_1 \Delta_2}$$

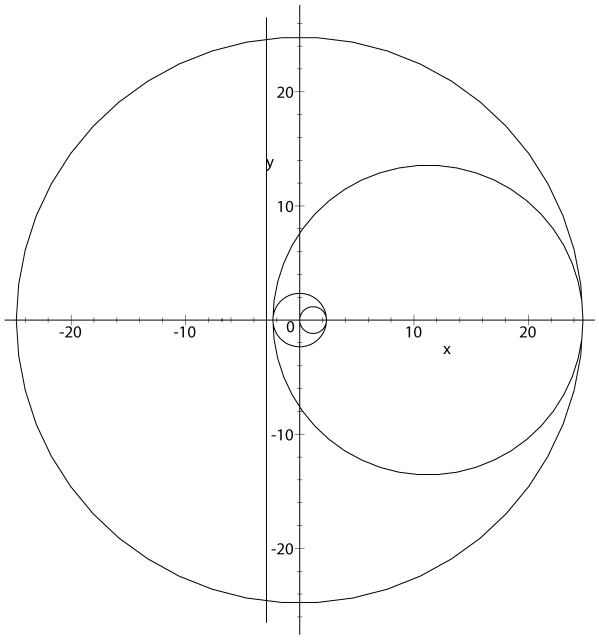


Abbildung 2.1.: Wie im Text beschrieben, zeigt die Abbildung tangentiale Kreise, die zur abwechselnden Anwendung von zwei Hamilton-Operatoren gehören. Dabei ist ein weiterer Schritt notwendig und hinreichend, um die ganze komplexe Zahlenebene abzudecken. Zur besseren Orientierung haben wir einen apollonischen Kreis mit unendlichem Radius als Linie eingezeichnet. Der Winkel zwischen den Rotationsachsen beträgt $(2 \cdot \pi/4 + \pi/5)/3$. In diesem Fall erhalten wir, daß die Anzahl der Zerlegungsschritte kleiner gleich 6 ist.

gilt.

Abbildung 2.1 zeigt tangentiale Kreise in der komplexen Zahlenebene, die der abwechselnden Anwendung der Hamilton-Operatoren entspricht. Dabei ist ein weiterer Schritt des Raffke-artigen Algorithmus notwendig und hinreichend, die ganze komplexe Zahlenebene abzudecken. Mit einer Analyse von ähnlichen Abbildungen wie Abbildung 2.1 ist es möglich, die minimale Anzahl von Schritten zu bestimmen, die jeden Punkt der Bloch-Sphäre in den Südpol der Bloch-Sphäre transformiert, d. h. jeden Punkt der komplexen Zahlenebene in den Ursprung der komplexen Zahlenebene abbildet. Wir erhalten eine Schranke für die Anzahl der Zerlegungsschritten für eine unitäre Transformation in einem Ein-Qubit-System, wenn wir die vorherige Zahl um eins erhöhen. Dies gilt, da jeder Punkt der Bloch-Sphäre (und jeder Punkt der komplexen Zahlenebene) als Rechts-Nebenklasse von Rotationen der Bloch-Sphäre aufgefaßt werden kann. Um die Rotationen in einer Nebenklasse zu unterscheiden, ist dieser zusätzliche Schritt im allgemeinem notwendig.

In der Referenz [Low71] (und in den Referenzen [Sil91a; Sil91b; D'A00; D'A03; D'A04; ZW05]) wurden ähnliche Abbildung wie Abbildung 2.1 analysiert. Für den Fall der Euler-Zerlegung (ähnlich der Euler-Winkel, siehe Theorem 2.3) verweisen wir auch auf die Referenz [Dav73].

Faktum 2.8 ([Low71])**.** Sei α der Winkel zwischen zwei Rotationen der Bloch-Sphäre und f die Anzahl der Zerlegungsschritte.

1. $\alpha = \pi/2 \implies f = 3$ (Euler-Zerlegung),
2. $\forall\ k \geq 2: \quad \pi/(k+1) \leq \alpha < \pi/k \implies f = k+2.$

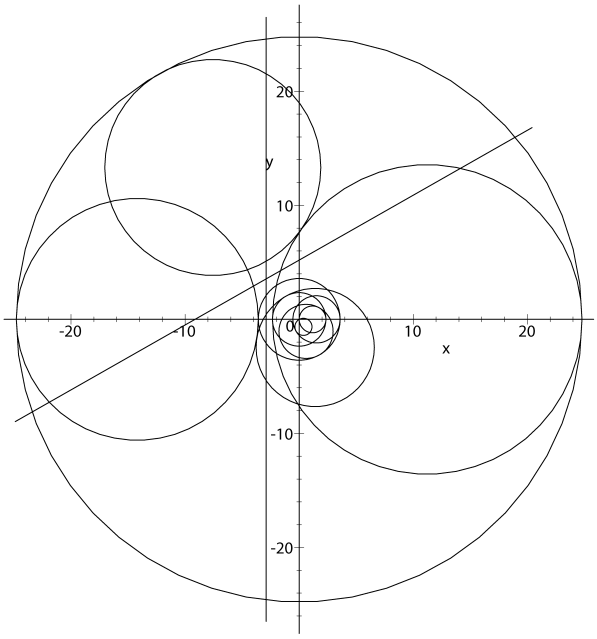


Abbildung 2.2.: Ähnlich zu Abbildung 2.1 entsprechen tangentiale Kreise der Anwendung von drei Hamilton-Operatoren. Der Zustandsraum wird mittels der stereographischen Projektion in der komplexen Zahlenebene dargestellt. Dabei ist kein weiterer Schritt notwendig um, die ganze komplexe Zahlenebene abzudecken. Zur besseren Orientierung haben wir zwei apollonische Kreise mit unendlichen Radien als zwei Linien eingezeichnet. Die Winkel zwischen den Rotationsachsen betragen $(2{\cdot}\pi/4{+}\pi/5)/3$, $\pi/5$, und $\pi/6$. Obwohl alle Winkel kleiner oder gleich den Winkeln aus Abbildung 2.1 sind, erhalten wir eine kleinere Schranke von 5 Zerlegungsschritten.

Wir erweitern unsere Analyse von zwei auf drei Hamilton-Operatoren. Da wir nun einen dritten Hamilton-Operator haben, müssen wir auch die zusätzliche Rotation der Bloch-Sphäre und das zugehörige System von apollonischen Kreisen mit einbeziehen. Die drei Rotationsachsen können mittels der eingeschloßenen Winkel α_1, α_2 und α_3 charakterisiert werden. Wir erhalten ein gültiges Tripel von Winkel, falls

$$\alpha_3 \in [\min\{\pi - (\alpha_1 + \alpha_2), |\alpha_1 - \alpha_2|\}, \pi/2].$$

Wie im Fall von zwei Hamilton-Operatoren ist es wichtig, die minimale Anzahl von Schritten zu bestimmen, um jeden Punkt der komplexen Zahlenebene in den Ursprung

der komplexen Zahlenebene abzubilden. Abbildung 2.2 zeigt tangentialen Kreise, die der abwechselnden Anwendung von drei Hamilton-Operatoren entspricht. Wie in Abbildung 2.2 angemerkt wurde, erhalten wir mit dieser Analyse eine bessere Schranke für die Anzahl der Zerlegungsschritte, obwohl die eingeschloßenen Winkel nicht größer als in Abbildung 2.1 sind.

3. Approximation von Quantenschaltkreisen

3.1. Einführung

Deutsch [Deu89] führte den Begriff der approximativen Universalität ein. Verallgemeinerungen, die die Benutzung von Hilfssystemen erlauben, sind in [Shi03; Aha03; Jea04; Jea05] zu finden.

Definition 3.1 (approximative Universalität)**.** Eine Menge von speziell unitären Grundoperationen ist approximativ universell, falls sie dicht (vgl. [Bou89a, S. 25]) in der speziell unitären Gruppe ist.

Bemerkung. Hierbei weichen wir (unwesentlich) von unserer Notation für Quantenschaltkreise (siehe Def. 1.7) ab: In Def. 3.1 erzeugen wir (approximativ) alle speziell unitäre Transformationen. Im Gegensatz dazu werden unitäre Transformationen durch Quantenschaltkreise nur bis auf einen skalaren Faktor erzeugt.

Wenn wir eine Halbgruppe S betrachten, die dicht in einer Lie-Gruppe G ist und ein nicht leeres Inneres $\mathrm{int}(S)$ (vgl. [Bou89a, S. 23]) besitzt, sind wir in einer besonderen Situation:

Faktum 3.2 ([HHL89, Lemma V.4.29] oder [HN93, Lemma 3.7])**.** Sei $S \subset \mathrm{G}$ eine Halbgruppe in einer Lie-Gruppe G. Ist S dicht in G und gilt $\mathrm{int}(S) \neq \emptyset$, so folgt $S = \mathrm{G}$.

Verschiedene Spezialfälle von Faktum 3.2 sind in den Arbeiten [JS72, Lemma 6.3], [Wea00b] und [BB02b, Lemma 4.1] zu finden. In diesem Kapitel betrachten wir (im folgenden) nur noch diskrete Mengen von Grundoperationen, insbesondere besitzen diese Mengen ein leeres Inneres. Diese Mengen können aber nicht universell, sondern nur approximativ universell sein, da die Menge der unitären Operatoren überabzählbar ist.

Faktum 3.3 (Kroneckers Approximationstheorem (siehe [Apo90, S. 149] oder [HW60, S. 375–376]))**.** Sei $\beta \in \mathbb{R}$, γ irrational und $\epsilon > 0$ beliebig, so existieren $h \in \mathbb{Z}$ und $k \in \mathbb{N}$ mit $k > 0$, so daß $|k\gamma - h - \beta| < \epsilon$.

Unter Verwendung von Faktum 3.3 zeigte [Deu89], daß das (auf drei Qubits operierende) Quantengatter $\Lambda_2(U_\alpha)$ (α irrational) mit

$$U_\alpha = \begin{pmatrix} i\cos(\alpha\pi/2) & \sin(\alpha\pi/2) \\ \sin(\alpha\pi/2) & i\cos(\alpha\pi/2) \end{pmatrix}$$

approximativ universell (für Qubitsysteme) ist. Die gleiche Technik wurde in [SW95b; Bar95] verwendet, um (für Qubitsysteme) die approximative Universalität einiger auf zwei Qubits operierenden Quantengatter zu zeigen. Daraus folgt, daß die Menge der auf zwei Qubits operierenden Quantengatter (für Qubitsysteme) approximativ universell ist. Aufbauend auf [Deu89] zeigte auch DiVincenzo [DiV95], daß die Menge der

auf zwei Qubits operierenden Quantengatter (für Qubitsysteme) approximativ universell ist. Entsprechend bewiesen [DBE95; Llo95] (vgl. auch [Wea00b]), daß die Menge der (für Qubitsysteme) nicht approximativ universellen und auf mehr als zwei Qubits operierenden Quantengatter vom Maß null ist.

Ausgehend von der Arbeit von Shor [Sho96] erlebte die Idee, eine diskrete Menge von Quantengattern als Grundoperationen zu benutzen (wie es von Deutsch [Deu89] ursprünglich vorgeschlagen wurde), eine neues und verstärktes Interesse. Dabei ist dieses Interesse hauptsächlich auf die Erfindung des fehlertoleranten Quantenrechnens (siehe z. B. [Zei00] oder [NC00, Kap. 10]) zurückzuführen: Für das fehlertolerante Quantenrechnen ist es wichtig, von einer diskreten Menge von Grundoperationen auszugehen. Eine große Anzahl von approximativ universellen Mengen von Quantengattern wurde vorgeschlagen [Sho96; KLZ96; Kit97; BMP+99]. In einigen Fällen wurde die diskrete Menge von Quantengattern durch die Möglichkeit ergänzt, ein Quantensystem in einem ausgezeichneten Zustand zu präparieren [KLZ98a; KLZ98b; BK05]. Wir verwenden die Quantengatter

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ und } {\sigma_z}^{\beta} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi\beta) \end{pmatrix}$$

und geben drei (für Qubitsysteme) approximativ universelle Mengen von Grundoperationen an:

$$\mathrm{G}_1 = \left\{H, {\sigma_z}^{\frac{1}{2}}, \Lambda_2(\sigma_x)\right\} \quad ([\text{Sho96}], \text{ vgl. auch } [\text{Kit97; BMP}^+99]),$$
$$\mathrm{G}_2 = \left\{H, \Lambda_1({\sigma_z}^{\frac{1}{2}})\right\} \quad ([\text{Kit97}]),$$
$$\mathrm{G}_3 = \left\{H, {\sigma_z}^{\frac{1}{4}}, \Lambda_1(\sigma_x)\right\} \quad ([\text{BMP}^+99]).$$

3.2. Analyse der approximativen Universalität

Es bezeichne τ eine (komplex) lineare Darstellung einer Untergruppe R einer Lie-Gruppe G und $\operatorname{env}\tau(R)$ die von der Darstellung τ erzeugte (assoziative) Algebra zu R. Wir identifizieren die Gruppe R mit ihrer von G induzierten (linearen) Standarddarstellung und $\operatorname{env} R$ mit der von der Standarddarstellung erzeugten Algebra zu R. Die Standarddarstellung induziert eine Abbildung in die Algebra $\mathrm{M}_n(\mathbb{C})$ der Matrizen der entsprechenden Dimension. Die Operation conj der Gruppe R auf der Algebra $\mathrm{M}_n(\mathbb{C})$ per Konjugation ist folgendermaßen definiert ($g \in R$, $M \in \mathrm{M}_n(\mathbb{C})$): $\operatorname{conj}(g)M := gMg^{-1}$. Die Operation conj der Gruppe R ist isomorph zu der Darstellung $\phi : g \mapsto g \otimes (g^{-1})^T$ für $g \in R$ (vgl. [Neu69, S. 954] oder [Gra81, S. 25]). Falls R eine Untergruppe einer unitären Gruppe ist, gilt insbesondere, daß ϕ isomorph zu der Darstellung $g \mapsto g \otimes g^*$ ($g \in G$) ist.

Für eine halbeinfache Lie-Gruppe G führen wir die Abbildungen Φ_i von G in die Nebenklassen G/G_i bzgl. der normalen Lie-Untergruppen G_i ein. Wir bezeichnen mit $\bar{R}$ den topologischen Abschluß von R in G ([Bou89a, Kap. I, §1.6, Def. 11]). Nach diesen Vorbereitungen sind wir nun in der Lage, eine Methode zur algorithmischen Analyse der approximativen Universalität einer endlich erzeugten Untergruppe einer halbeinfachen und kompakten Lie-Gruppe anzugeben. Diese Methode ist von einem Ergebnis [Jea05, Thm. 2.11] (vgl. auch [Jea04]) für algebraische Gruppen (vgl. z. B. [TY05]) motiviert.

Theorem 3.4 (vgl. [Jea05, Thm. 2.11])**.** Sei G eine endlichdimensionale reelle Lie-Gruppe, die halbeinfach und kompakt ist. Ferner bezeichne Γ eine endlich erzeugte Untergruppe von G. Die Gruppe Γ ist genau dann dicht in G, wenn $\Phi_i(\Gamma)$ für alle zusammenhängenden echten normalen Lie-Untergruppen G_i ($G_i \neq G$) eine unendliche Gruppe ist und $\operatorname{env}\phi(\Gamma) = \operatorname{env}\phi(G)$ gilt.

Beweis. Zuerst zeigen wir, daß $\operatorname{env}\phi(\Gamma) = \operatorname{env}\phi(\bar{\Gamma})$ gilt: Da $\operatorname{env}\phi(\Gamma)$ ein endlicher Vektorraum über den reellen oder komplexen Zahlen ist, ist $\operatorname{env}\phi(\Gamma)$ abgeschlossen ([Bou87, Kap. I, §2.3, Kor. 1 zu Prop. 2]). Damit folgt $\phi(\bar{\Gamma}) \subseteq \operatorname{env}\phi(\Gamma)$ und $\operatorname{env}\phi(\bar{\Gamma}) \subseteq \operatorname{env}\phi(\Gamma)$. Ferner gilt $\Gamma \subseteq \bar{\Gamma}$ und $\operatorname{env}\phi(\Gamma) \subseteq \operatorname{env}\phi(\bar{\Gamma})$.

Sei nun Γ dicht in G. Nehmen wir an, daß $\Phi_i(\Gamma)$ für ein i eine endliche Gruppe ist, so ist Γ/G_i nicht dicht in der Gruppe G/G_i und somit ist Γ nicht dicht in G. Es folgt, daß $\Phi_i(\Gamma)$ für alle i unendlich ist. Da $\bar{\Gamma} = G$, gilt auch $\operatorname{env}\phi(G) = \operatorname{env}\phi(\bar{\Gamma}) = \operatorname{env}\phi(\Gamma)$.

Seien nun alle $\Phi_i(\Gamma)$ unendliche Gruppen und es gelte $\operatorname{env}\phi(\Gamma) = \operatorname{env}\phi(G)$. Aus der Abgeschlossenheit von $\bar{\Gamma}$ folgt, daß $\bar{\Gamma}$ eine Lie-Untergruppe von G ist ([Bou89b, Kap. III, §8.2, Thm. 2]). Da die Zusammenhangskomponente $(\bar{\Gamma})_\circ$ der Identität von $\bar{\Gamma}$ abgeschlossen ist ([Bou89a, Kap. III, §2.2, Prop. 7]), ist sie eine zusammenhängende Lie-Untergruppe von $\bar{\Gamma}$ ([Bou89b, Kap. III, §8.2, Thm. 2]) und damit auch eine zusammenhängende Lie-Untergruppe von G ([Bou89b, Kap. III, §1.4]). Da $(\bar{\Gamma})_\circ$ eine zusammenhängende Lie-Untergruppe von G ist, ist $(\bar{\Gamma})_\circ$ eine virtuelle Lie-Untergruppe (siehe z. B. Seite 11) von G ([Bou89b, Kap. III, §6.2, Beispiel 1]).

Die Lie-Algebra von $\bar{\Gamma}$ ist invariant unter der adjungierten Darstellung $\operatorname{Ad}(\bar{\Gamma})$ von $\bar{\Gamma}$ ([Bou89b, Kap. III, §3.12, Def. 8]). Mit Hilfe von $\operatorname{env}\phi(\bar{\Gamma}) = \operatorname{env}\phi(G) \supseteq \phi(G)$ erhalten wir, daß die Lie-Algebra von $\bar{\Gamma}$ invariant unter Ad(G) ist. Nach dem drittem Fundamentaltheorem von Lie (siehe z. B. [Var84, §2.8]) sind die Lie-Algebren von $\bar{\Gamma}$ und $(\bar{\Gamma})_\circ$ gleich, und wir erhalten, daß auch die Lie-Algebra von $(\bar{\Gamma})_\circ$ invariant unter Ad(G) ist. Da $(\bar{\Gamma})_\circ$ eine virtuelle Lie-Untergruppe von G ist, folgt, daß $(\bar{\Gamma})_\circ$ normal in G ist ([Bou89b, Kap. III, §6.6, Prop. 14]). Damit folgt, daß $(\bar{\Gamma})_\circ$ eine der Untergruppen G_i oder gleich G ist.

Nehmen wir nun an, daß $(\bar{\Gamma})_\circ$ eine der Untergruppen G_i ist. Dann erhalten wir, daß $\bar{\Gamma}$ unendlich viele Zusammenhangskomponenten besitzt ($\Phi_i(\Gamma)$ ist unendlich). Aber $\bar{\Gamma}$ ist eine abgeschlossene Untergruppe der kompakten Lie-Gruppe G und somit auch eine kompakte Gruppe ([Bou89a, Kap. I, §9.3, Prop. 3]) und insbesondere eine (kompakte) Lie-Gruppe (siehe z. B. [Che99, Kap. IV, §XV, Kor. zu Prop. 2]). Kompakte Lie-Gruppen besitzen eine treue lineare Darstellung (siehe [Che99, Kap. VI, §XII, Thm. 2] oder [OV90, Kap. 5, §2.4, Thm. 10]). Lie-Gruppen mit treuen linearen Darstellungen werden als lineare Lie-Gruppen bezeichnet. Kompakte lineare Lie-Gruppen sind algebraische Gruppen (siehe [Che55, Kap. VI, §5.2, Prop. 2] oder [OV90, Kap. 3, §4.4, Thm. 5]) und besitzen damit aber nur endlich viele Zusammenhangskomponenten. Ein Beweis für die letzte Aussage kann in [Mos57, Anhang] gefunden werden. In der Referenz [BT65, §14] wird auf [Whi57] verwiesen. Zusammenfassend erhalten wir, daß $(\bar{\Gamma})_\circ$ keine der Untergruppen G_i ist und damit gleich G ist. Insbesondere gilt $\bar{\Gamma} = G$. □

Bemerkung. In der Referenz [Jea05] fehlte beim entsprechenden Beweis für algebraische Gruppen ([TY05]) die Argumentation über die Anzahl der Zusammenhangskomponenten und insbesondere wurde dort auch nicht darauf verwiesen, daß algebraische Gruppen

nur endliche viele Zusammenhangkomponenten besitzen. In [Jea05, S. 13] wurde darauf hingewiesen, daß Theorem 3.4 auch durch die Benutzung der Ergebnisse von [Jea05, Thm. 2.11] für algebraische Gruppen ([TY05]) folgt: Für Untergruppen kompakter Lie-Gruppen ist der in [Jea05] verwendete Zariski-Abschluß ([TY05, Kap. 11, §2]) äquivalent (siehe Lemma 3.5) zu dem hier verwendeten Abschluß in der Operatornorm-Topologie (vgl. Seite 91).

Lemma 3.5. Sei G eine kompakte Lie-Gruppe und Γ eine Untergruppe von G. Der Zariski-Anschluß $\bar{\Gamma}^{\mathrm{z}}$ von Γ ist gleich dem Abschluß $\bar{\Gamma}$ von Γ in der Operatornorm-Topologie.

Beweis. Wir merken an, daß $\bar{\Gamma} \subseteq \bar{\Gamma}^{\mathrm{z}}$ gilt (vgl. [Eis95, S. 32–33, S. 54–55]). Da $\bar{\Gamma}$ eine abgeschlossene Untergruppe ([Bou89a, Kap. III, §2.1, Prop. 1]) einer kompakten Lie-Gruppe ist, ist $\bar{\Gamma}$ kompakt und damit eine algebraische Gruppe (siehe Beweis von Theorem 3.4). Insbesondere ist $\bar{\Gamma}$ Zariski-abgeschlossen. Da aber $\bar{\Gamma}^{\mathrm{z}}$ die minimale Menge ist, die Zariski-abgeschlossen ist und Γ enthält, erhalten wir $\bar{\Gamma} = \bar{\Gamma}^{\mathrm{z}}$. □

Theorem 3.4 kann dazu verwendet werden, die approximative Universalität einer endlich erzeugten Untergruppe der speziell unitären Gruppe $\mathrm{SU}(n)$ ($n \in \mathbb{N}$) zu entscheiden (vgl. [Jea04, Thm. 8] und [Jea05, Thm. 2.4]). In diesem Fall ist $\mathrm{SU}(n)$ einfach, und die Identität und $\mathrm{SU}(n)$ selbst sind die einzigen zusammenhängenden normalen Untergruppen von $\mathrm{SU}(n)$. Das Testen der Endlichkeit von Matrixgruppen in Theorem 3.4 kann ausgehend von [BBR93] effizient (für Matrixgruppen über Zahlkörpern) getestet werden (siehe auch [Bab92; Bea97; RTB99; Iva01]). Eine Implementierung steht z. B. in Magma [BCP97] zur Verfügung. Das Testen der Bedingung $\mathrm{env}\,\phi(\Gamma) = \mathrm{env}\,\phi(\mathrm{G})$ von Theorem 3.4 kann zu Effizienzproblemen führen, da durch die Verwendung der Abbildung ϕ die Dimension der verwendeten linearen Darstellung quadriert wird.

In der Arbeit [FKL03] wurde ein hinreichendes Kriterium dafür angegeben, ob für eine abgeschlossene Untergruppe H einer zusammenhängenden und kompakten Lie-Gruppe G die Bedingung H = G gilt. Dieses Kriterium basiert auf einer Schranke für einen sogenannten Durchmesser für den homogenen Raum G/H (siehe [FKL03]). Der Durchmesser kann in konkreten Fällen berechnet werden, und falls die Schranke unterschritten wird, gilt H = G. Ein weiteres hinreichendes Kriterium, ob eine Untergruppe in einer unitären Gruppe dicht ist, wurde in [Kit97] angegeben und in [Aha99, Lemma 20] (siehe auch [ABO99]) und [KSV02, S. 75, Problem 8.11] bewiesen:

Faktum 3.6 ([Kit97])**.** Sei H die Untergruppe der unitären Gruppe $\mathrm{U}(n)$ ($n \geq 3$), die einen gegebenen Vektor fix läßt. Ferner sei $G \in \mathrm{U}(n)$ nicht aus der Untergruppe H. Die von H und G erzeugte Untergruppe ist dicht in $\mathrm{U}(n)$.

3.3. Nicht-Konstruktive Approximation

3.3.1. Der allgemeine Fall

Sei G eine endlichdimensionale, zusammenhängende und kompakte reelle Lie-Gruppe. Ferner sei $S \subset \mathrm{G}$ eine endliche Teilmenge von G. Wir bezeichnen mit $\Gamma = \langle S \cup S^{-1} \rangle$ die von S und S^{-1} endlich erzeugte Untergruppe von G und mit $\mathrm{W}_n(S \cup S^{-1})$ die Worte der

Länge $n \in \mathbb{N} \cup \{0\}$ in der Erzeugermenge $S \cup S^{-1}$. Ohne Beschränkung der Allgemeinheit wählen wir S so, daß $S \cap S^{-1} = \{s \in S \mid s^2 = \mathrm{Id}\}$ gilt. In [HRC02] (siehe auch [Har01]) wurde der Begriff der effizienten Universalität eingeführt:

Definition 3.7 ([HRC02, Theorem 1])**.** Sei S eine endliche Teilmenge einer endlichdimensionalen, zusammenhängenden und kompakten Lie-Gruppe G und gelte $\Gamma = \langle S \cup S^{-1} \rangle$. Die Menge S wird als effizient universell in G bezeichnet, falls eine Konstante $C > 0$ existiert, so daß für alle Elemente $G \in \mathrm{G}$ und für alle $\epsilon > 0$ eine Konstante $n > C \log(1/\epsilon)$ $(n \in \mathbb{N})$ sowie ein Wort $w \in \mathrm{W}_n(S \cup S^{-1})$ der Länge n existieren, die die Bedingung $|w - G| < \epsilon$ erfüllen.

Es ist klar, daß die approximative Universalität (Def. 3.1) von $\Gamma = \langle S \cup S^{-1} \rangle$ eine notwendige Bedingung für die effiziente Universalität (Def. 3.7) einer Menge S ist. Wir folgen nun [HRC02] und führen einige Begriffe ein, um später eine hinreichende Bedingung für die effiziente Universalität anzugeben. In [HRC02] wurde der Fall der speziell unitären Gruppe betrachtet. Im Gegensatz dazu präsentieren wir die Begriffe gleich allgemein für Lie-Gruppen, die endlichdimensional, zusammenhängend und kompakt sind.

Wir führen nun das Haarsche Maß (siehe z. B. [DK00, S. 182], [BD85, S. 40], [Kna02, S. 531], [Gaa73, Abschnitt V.2], [HN91, Abschnitt III.4], [Ros02, Kapitel 5], [Che99, Abschnitt VII]) zur Integration auf einer Lie-Gruppe ein.

Definition 3.8 ([Gaa73, S. 241])**.** Ein links invariantes Maß μ auf einer lokal kompakten topologischen Gruppe G besitzt folgende Eigenschaften:

1. $\mu(GE) = \mu(E)$ für jede meßbare Teilmenge $E \subseteq \mathrm{G}$ und jedes Element $G \in \mathrm{G}$,
2. $0 \leq \mu(K) < \infty$ für jede kompakte Teilmenge $K \subseteq \mathrm{G}$,
3. $0 < \mu(K)$ für jede kompakte Teilmenge $K \subseteq \mathrm{G}$ mit $\mathrm{int}(K) \neq \emptyset$.

Wir bezeichnen ein solches Maß als Haarsches Maß.

Jede endlichdimensionale Lie-Gruppe, die komplex oder reell ist, ist lokal kompakt ([Bou89b, Kap. III, §1.1, Prop. 2(iii)]) und eine topologische Gruppe ([Bou89b, Kap. III, §1.1, Prop. 1]). Somit existiert ein links invariantes Maß insbesondere auf einer endlichdimensionalen, zusammenhängenden und kompakten rellen Lie-Gruppe G. Im Fall, daß G kompakt ist, gilt insbesondere, daß $\mu(\mathrm{G})$ endlich ist ([Gaa73, S. 247]) und wir normieren μ so, daß $\mu(\mathrm{G}) = 1$ gilt ([Gaa73, S. 243]). Für das Haarsche Maß benutzen wir zusätzlich die Integralnotation $\mu(E) = \int_E dG$ mit $E \subseteq \mathrm{G}$.

Nun sind wir in der Lage, den Raum $L^2(\mathrm{G})$ der quadrat-integrierbaren Funktion auf einer endlichdimensionalen komplexen oder reellen Lie-Gruppe G einzuführen. Wir verweisen auf [Gaa73, S. 272] (siehe auch [Wal90, S. 337] und [Jau68, S. 16–17 und S. 24]).

Definition 3.9. Sei G eine endlichdimensionale komplexe oder reelle Lie-Gruppe. Der Raum $L^2(\mathrm{G})$ ist definiert als

$$L^2(\mathrm{G}) := \{f : \mathrm{G} \to B \mid f \text{ meßbar bzgl. dem Haarschen Maß und } \|f\|_2 < \infty\},$$

wobei $B = \mathbb{R} \cup \{\infty\}$ oder $B = \mathbb{C}$. Weiter gilt, daß $L^2(\mathrm{G})$ zusammen mit dem Skalarprodukt

$$\langle f, g \rangle = \int_{\mathrm{G}} f^* g \, dG \quad \text{mit } f, g \in L^2(\mathrm{G})$$

und der Norm

$$\|f\|_2 = \sqrt{\int_{\mathrm{G}} |f|^2 \, dG} = \sqrt{\int_{\mathrm{G}} f^* f \, dG} = \sqrt{\langle f, f \rangle} \quad \text{mit } f \in L^2(\mathrm{G})$$

ein Hilbertraum ist.

Ausgehend von der Norm $\| \ \|_2$ auf $L^2(\mathrm{G})$ definieren wir für Operatoren M auf $L^2(\mathrm{G})$ eine Operatornorm ([Gaa73, S. 58]):

$$\|M\|_{\mathrm{op}} = \sup_{0 \neq f \in L^2(\mathrm{G})} \frac{\|Mf\|_2}{\|f\|_2} = \sup_{f \in L^2(\mathrm{G}), \|f\|_2 = 1} \|Mf\|_2.$$

Die Lie-Gruppe G operiert auf $L^2(\mathrm{G})$ mittels der links regulären Darstellung

$$G_1 \cdot f(G_2) = f((G_1)^{-1} G_2) \quad \text{mit } G_1, G_2 \in \mathrm{G} \text{ und } f \in L^2(\mathrm{G})$$

(siehe z. B. [Gaa73, S. 191], [Vin89, S. 10] oder [Kna02, S. 556–557]). Die links reguläre Darstellung induziert einen Operator auf $L^2(\mathrm{G})$, den wir mit $\mathring{G} : L^2(\mathrm{G}) \to L^2(\mathrm{G})$ bezeichnen:

$$\mathring{G} f(G_1) = G \cdot f(G_1) \text{ mit } G, G_1 \in \mathrm{G} \text{ und } f \in L^2(\mathrm{G}). \tag{3.1}$$

Für eine endliche Teilmenge $\mathcal{A} \subset \mathrm{G}$ führen wir den Hecke-Operator $\mathcal{T}(\mathcal{A})$ (siehe z. B. [LPS86, S. S153], [Col89, S. 83], [Sar90, S. 51], [Lub94, S. 119] oder [HRC02, S. 4447]) ein:

$$\mathcal{T}(\mathcal{A}) = \frac{1}{|\mathcal{A}|} \sum_{A \in \mathcal{A}} \mathring{A}.$$

Insbesondere definieren wir die Operatoren

$$T_n = T_n(S \cup S^{-1}) = \mathcal{T}(\mathrm{W}_n(S \cup S^{-1})),$$

mit $n \in \mathbb{N}$ (vgl. [LPS86, S. S156] oder [HRC02, S. 4447]). Ferner sei $T = T_1$. Wir erhalten $T_n = T^n$. Zusätzlich benötigen wir den Operator P (vgl. [Lub94, S. 119] oder [HRC02, S. 4447]):

$$Pf(H) = \int_{\mathrm{G}} f(GH) \, dG = \int_{\mathrm{G}} f(G) \, dG \quad \text{mit } f \in L^2(\mathrm{G}) \text{ und } H, G \in \mathrm{G}.$$

Der Operator P projiziert auf die konstanten Funktionen aus $L^2(\mathrm{G})$, und es folgt, daß $\mathrm{Bild}(1 - P) = L_0^2(\mathrm{G}) = \{f \in L^2(\mathrm{G}) \mid \int_{\mathrm{G}} f \, dG = 0\}$. Weiterhin gilt $TP = P = PT$, und für $f_0 \in L_0^2(\mathrm{G})$ erhalten wir

$$Tf_0 = T \mid_{L_0^2(\mathrm{G})} f_0 = T(1 - P) f_0 = (T - P) f_0.$$

Lemma 3.10. Der Operator T ist selbstadjungiert, und es gilt $\|T^n\|_{\mathrm{op}} = (\|T\|_{\mathrm{op}})^n$ für $n \in \mathbb{N}$.

Beweis. Sei $\mathcal{A} = S \cup S^{-1}$ die zu dem Operator T gehörende Erzeugermenge. Wir verwenden die Notationen $f_1, f_2 \in L^2(\mathrm{G})$ und $G \in \mathrm{G}$:

$$\begin{aligned}\langle Tf_1, f_2\rangle &= \int_{\mathrm{G}} (Tf_1)^* f_2 \, dG = \frac{1}{|\mathcal{A}|} \sum_{A\in\mathcal{A}} \int_{\mathrm{G}} f_1^*(A^{-1}G) f_2(G) \, dG \\ &= \frac{1}{|\mathcal{A}|} \sum_{A\in\mathcal{A}} \int_{\mathrm{G}} f_1^*(G) f_2(A\,G) \, dG = \frac{1}{|\mathcal{A}|} \sum_{A\in\mathcal{A}} \int_{\mathrm{G}} f_1^*(G) f_2(A^{-1}G) \, dG \\ &= \int_{\mathrm{G}} f_1^*(Tf_2) \, dG = \langle f_1, Tf_2\rangle.\end{aligned}$$

Die dritte Gleichung folgt, da dG invariant unter der Lie-Gruppe G ist, und die vierte Gleichung folgt, da $\mathcal{A} = \mathcal{A}^{-1}$ gilt. Wir erhalten, daß der Operator T selbstadjungiert ist, weil er beschränkt ist. Die Gleichung $\|T^n\|_{\mathrm{op}} = (\|T\|_{\mathrm{op}})^n$ folgt nun mit Hilfe von [Gaa73, Lemma 5, S. 46] und der Tatsache, daß $L^2(\mathrm{G})$ ein Hilbertraum ist. □

Definition 3.11 (siehe z. B. [Col89, S. 84] oder [Lub94, S. 119])**.** Wir definieren das Maß $\Lambda := \Lambda(S \cup S^{-1}) = \|T(S \cup S^{-1}) \mid_{L_0^2(\mathrm{G})}\|_{\mathrm{op}}$.

Damit sind wir nun in der Lage, den Unterschied zwischen den Operatoren T und P zu quantifizieren:

Lemma 3.12 (vgl. [Lub94, S. 119–120])**.** Es gilt: $\Lambda(S \cup S^{-1}) = \|T(S \cup S^{-1}) - P\|_{\mathrm{op}}$.

Beweis. Da $(1 - P)$ die Identität auf $L_0^2(\mathrm{G})$ ist, erhalten wir

$$\|T \mid_{L_0^2(\mathrm{G})}\|_{\mathrm{op}} = \|(T - P) \mid_{L_0^2(\mathrm{G})}\|_{\mathrm{op}} \leq \|(T - P)\|_{\mathrm{op}}.$$

Ferner gilt $\|f\|_2 \geq \|(1 - P)f\|_2$ und es folgt

$$\begin{aligned}\|(T - P)\|_{\mathrm{op}} &= \sup_{0\neq f\in L^2(\mathrm{G})} \frac{\|(T - P)f\|_2}{\|f\|_2} = \sup_{0\neq f\in L^2(\mathrm{G})} \frac{\|T(1 - P)f\|_2}{\|f\|_2} \\ &\leq \sup_{0\neq f\in L^2(\mathrm{G})} \frac{\|T(1 - P)f\|_2}{\|(1 - P)f\|_2} = \sup_{0\neq f'\in L_0^2(\mathrm{G})} \frac{\|Tf'\|_2}{\|f'\|_2}.\end{aligned}$$

□

Unter Benutzung von Lemma 3.10 und Lemma 3.12 erhalten wir:

Lemma 3.13. Für $n \in \mathbb{N}$ gilt: $\Lambda^n = \|T^n - P\|_{\mathrm{op}}$.

Die Aussage von Lemma 3.13 motiviert unseren bisher gewählten Ansatz: Das Maß Λ quantifiziert den Unterschied zwischen dem Operator T^n und dem Integraloperator P. Dabei kann T^n als Entsprechung für die Verteilung der Worte W_n der Länge n aufgefaßt werden. Damit beschreibt Λ^n die Konvergenzgeschwindigkeit der Gruppe $\Gamma = \langle S \cup S^{-1}\rangle$ an die Gleichverteilung in der Lie-Gruppe G.

Theorem 3.14. Sei G eine endlichdimensionale, zusammenhängende und kompakte reelle Lie-Gruppe. Ferner sei $S \subset \mathrm{G}$ eine endliche Teilmenge von G. Für jede endlich erzeugte Untergruppe $\Gamma = \langle S \cup S^{-1}\rangle$ gilt: Aus $\Lambda(S \cup S^{-1}) < 1$ folgt, daß die Untergruppe Γ effizient universell in G ist.

Bemerkung. In [HRC02, Thm. 1] wurde der Spezialfall der speziell unitären Gruppe betrachtet. Der Beweis von Theorem 3.14 folgt im wesentlichen der Arbeit [HRC02].

Beweis. Seien $G, G_0 \in \mathrm{G}$. Wir führen die Funktion $\eta \in L^2(\mathrm{G})$ ein:

$$\eta(G) := \begin{cases} 1 & \text{für } |G - \mathrm{Id}| < \epsilon/2, \\ 0 & \text{sonst.} \end{cases}$$

Es gilt $\eta^2(G) = \eta(G)$ und wir erhalten

$$\begin{aligned}(\|\eta\|_2)^2 &= \int_{\mathrm{G}} \eta^2(G)\, dG = \int_{\mathrm{G}} \eta(G)\, dG = (P\eta)(G_0) \\ &= \sqrt{((P\eta)(G_0))^2 \int_{\mathrm{G}} dG} = \sqrt{\int_{\mathrm{G}} (P\eta)^2\, dG} = \|P\eta\|_2.\end{aligned}$$

Im folgenden benötigen wir das Maß $V = V(\epsilon/2) = \|P\eta\|_2 = (\|\eta\|_2)^2$ einer offenen Kugel vom Radius $\frac{\epsilon}{2}$ um die Identität Id. Es gilt die Abschätzung $V > k(\epsilon/2)^d$ für V, wobei k eine von ϵ unabhängige Konstante ist und d die Dimension von G ist. Sei $U \in \mathrm{G}$ ein beliebiges Element aus G, das approximiert werden soll. Aus der Cauchy-Schwarz-Ungleichung und der Ungleichung $\|Xf\|_2 \leq \|X\|_{\mathrm{op}}\, \|f\|_2$ für einen Operator X auf $L^2(\mathrm{G})$ und $f \in L^2(\mathrm{G})$ folgt

$$\begin{aligned}|\langle \eta, T^n \mathring{U} \eta\rangle - V^2| &= |\langle \eta, T^n \mathring{U}\eta\rangle - \langle \eta, P\mathring{U}\eta\rangle| = |\langle \eta, (T^n - P)\mathring{U}\eta\rangle| \\ &\leq \|\eta\|_2\, \|(T^n - P)\mathring{U}\eta\|_2 \leq (\|\eta\|_2)^2\, \|(T^n - P)\mathring{U}\|_{\mathrm{op}} = V \cdot \Lambda^n.\end{aligned}$$

Der Operator $\mathring{U}$ wurde in Gleichung (3.1) definiert. Wir wählen nun ein $n \in \mathbb{N}$, so daß die Bedingung

$$n > \frac{d \log(\epsilon/2)}{\log(1/\Lambda)} + \frac{\log(2^d/k)}{\log(1/\Lambda)}$$

erfüllt ist, d. h., es existiert eine Konstante C mit $n > C \log(\epsilon/2)$. Nach Voraussetzung gilt $\Lambda < 1$ und es folgen die Gleichungen $\log(1/\Lambda) > 0$ und $\Lambda^n < k(\epsilon/2)^d < V$. Damit ergibt sich: $|\langle \eta, T^n \mathring{U}\eta\rangle - V^2| < V^2$. Wir erhalten

$$\int_{\mathrm{G}} \eta(G) \frac{1}{|W_n(S \cup S^{-1})|} \left(\sum_{w \in W_n(S \cup S^{-1})} \eta(wU^{-1}G) \right) dG = \langle \eta, T^n \mathring{U}\eta\rangle > 0,$$

d. h., es existieren ein $G \in \mathrm{G}$ und ein Wort $w \in W_n(S \cup S^{-1})$, so daß die Bedingungen $\eta(G) > 0$ und $\eta(wU^{-1}G) > 0$ gelten. Damit folgt, daß die Gleichungen $|G - \mathrm{Id}| < \epsilon/2$ und $|wU^{-1}G - \mathrm{Id}| < \epsilon/2$ erfüllt sind. Mit Hilfe der Dreiecksungleichung erhalten wir $|w - U| < \epsilon$. □

3.3.2. Der halbeinfache Fall

Wir schränken uns nun auf kompakte reelle Lie-Gruppen G ein, die endlichdimensional, zusammenhängend und halbeinfach sind. In [HRC02, Lemma 2] wurde unter Verwendung von Ergebnissen aus [LPS86; LPS87] (siehe auch [Col89; Sar90; Lub94; GJS99])

eine dreielementige Teilmenge $S \in \mathrm{SU}(2)$ mit $\Lambda(S \cup S^{-1}) < 1$ angegeben. Nach Theorem 3.14 ist diese Menge effizient universell in SU(2). In [HRC02, Prop. 5] wurden auch Teilmengen $S \in \mathrm{SU}(n)$ für $n > 2$ angegeben, die die Bedingung $\Lambda(S \cup S^{-1}) < 1$ erfüllen. Weiterhin wurde in [HRC02, S. 4451] (siehe auch [FLW02, S. 195–196]) die Vermutung geäußert, daß, falls $\Gamma = \langle S \cup S^{-1} \rangle$ dicht in der Lie-Gruppe G ist, die Teilmenge S effizient universell in G ist. In [NC00, Abschnitt. 4.5.4] wurde unter Benutzung eines Zählarguments gezeigt, daß alle Quantenzustände auf n Quantenbits durch unitäre Operationen nur mit $\Omega(2^n \log(1/\epsilon)/\log(n))$ Operationen bis auf eine Genauigkeit von ϵ approximiert werden können. Andere Argumente wurden in [KR01, Thm. 1] benutzt, um auf der Gruppe SO(3) eine untere Schranke von $\Omega(\sqrt{\log(1/\epsilon)})$ Operationen zur Approximation eines beliebigen Gruppenelements aus SO(3) mit der Genauigkeit ϵ zu beweisen.

3.4. Konstruktive Approximation

Wir diskutieren nun konstruktive Ergebnisse zur Approximation von unitären Transformationen. Kitaev [Kit97] und Solovay schlugen unabhängig voneinander einen effizienten Algorithmus vor:

Faktum 3.15 (siehe z. B. [DN06])**.** Sei S eine endliche Teilmenge der $\mathrm{SU}(n)$ und $\Gamma = \langle S \cup S^{-1} \rangle$ eine endlich erzeugte dichte Untergruppe der $\mathrm{SU}(n)$. Es existieren Konstanten $c_1, c_2 > 0$ und ein Algorithmus, der in Abhängigkeit von der Genauigkeit ϵ für jedes zu approximierende Element $U \in \mathrm{SU}(n)$ ein Wort $w \in \mathrm{W}_n(S \cup S^{-1})$ der Länge $n \in O(\log^{c_1}(1/\epsilon))$ in der Laufzeit $O(\log^{c_2}(1/\epsilon))$ findet, so daß $|w - U| < \epsilon$ gilt.

Bemerkung. In [DN06] werden die Konstanten als $c_1 \approx 3.97$ sowie $c_2 \approx 2.71$ angegeben. Unter gewissen Annahmen (siehe [KSV02, S. 78]), können die Konstanten als $c_1 > 3$ und $c_2 = 3$ gewählt werden. Es ist unbekannt, ob eine Wahl $c_1 = c_2 = 1$ möglich ist.

Der Algorithmus von Faktum 3.15 wird auch in den Referenzen [NC00; Har01; KSV02; DN06] behandelt, und ein weiterer Algorithmus zur konstruktiven Approximation, der aber nur für eine spezielle dichte Teilmenge der $\mathrm{SU}(n)$ geeignet ist, wird in [KSV02, Abschnitt 13.7] vorgestellt. Dabei gibt [DN06] einen Überblick über den Algorithmus von Faktum 3.15 und beschreibt seine Entstehungsgeschichte. In einem ersten Schritt des Algorithmus von Faktum 3.15 muß eine Startapproximation gefunden werden, die einer festen Genauigkeit genügt. Diese Startapproximation wird später sukzessiv verfeinert. Harrow [Har01, Abschnitt 2.5] implementierte den Teilalgorithmus zur Bestimmung einer Startapproximation mit Hilfe von Heuristiken. In [KSV02, S. 76] wird darauf hingewiesen, daß der Schritt zur Bestimmung der Startapproximation nicht konstruktiv ist und potentiell beliebig lange dauern könnte, womit der vorgeschlagene Algorithmus von Faktum 3.15 kein Algorithmus im engeren Sinne wäre. In Referenz [DN06, S. 85] wird vorgeschlagen, Startapproximationen zu allen Elementen der $\mathrm{SU}(n)$ vorzuberechnen, d. h., ein sogenanntes Startnetz vorzuberechnen.

4. Simulation von unitären Operationen

In diesem Kapitel folgen wir [ZGB04].

4.1. Das Modell

Wir betrachten ein System von n Qubits, wobei $n \in \mathbb{N}$ endlich ist. Dieses System wird mit einem n-fachen Tensorprodukt $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ von n zwei-dimensionalen komplexen Vektorräumen modelliert. Die einzelnen Tensorkomponenten entsprechen dabei einzelnen Qubits. Die Zeitentwicklung ist durch die Schrödinger-Gleichung für den Zeitentwicklungsoperator gegeben, vgl. Gleichung (1.2):

$$\frac{d}{dt}U(t) = (-iH)U(t),$$

wobei t die Zeit, $U(t)$ die Zeitentwicklung, und H den zeitunabhängigen Hamilton-Operator bezeichnen. Aufgrund der Irrelevanz der globalen Phase in der Quantenmechanik beschränken wir uns für Zeitentwicklungsoperatoren auf die speziell unitäre Gruppe $\mathrm{SU}(2^n)$.

Zusätzlich zur Möglichkeit, das System unter dem Zeitentwicklungsoperator $U(t) = \exp(-iHt)$ evolvieren zu lassen, ist in unserem Modell die Anwendung von lokalen unitären Transformationen vorgesehen. Eine unitäre Transformation wird als lokal betrachtet, falls sie keine Interaktion zwischen verschiedenen Qubits zur Folge hat, d. h., falls sich die unitäre Transformation als n-faches Tensorprodukt $U_1 \otimes \cdots \otimes U_n$ von unitären Transformationen $U_i \in \mathrm{SU}(2)$ mit $i \in \{1, \ldots, n\}$ schreiben läßt. Die Zeit zur Ausführung von lokalen unitären Transformationen ist vernachlässigbar und wird als null angenommen. Damit haben wir die vorhandenen Ressourcen des Kontrollsystems angegeben.

Aus mathematischen Gründen beschränken wir uns auf Systeme, deren Hamilton-Operator ohne Verwendung von lokalen Termen dargestellt werden kann. Aus diesem Grund folgt im Fall der Simulation von Hamilton-Operatoren aus der Simulierbarkeit, daß der Hamilton-Operator ohne lokale Terme dargestellt werden kann. Um einen Hamilton-Operator von lokalen Termen zu befreien, werden oft Approximationsmethoden verwendet, siehe z. B. [BCL$^+$02, S. 3] oder [MVL02, S. 288]. Wir benutzen keine Approximationsmethoden. Zusätzlich scheinen lokale Terme in Hamilton-Operatoren verantwortlich für Probleme mit unendlichen Programmen, d. h. mit unendlich vielen Schritten $m = \infty$ (siehe z. B. Definition 4.1), zu sein. In [HNO03] (siehe auch [DHK04]) werden im Fall von Hamilton-Operatoren mit lokalen Termen die Voraussetzungen analysiert, unter denen unendliche Programme notwendig für die zeit-optimale Kontrolle sind. Unabhängig davon erlauben wir aus technischen Gründen alle Arten von Programmen, auch unendliche. Wir verwenden die verfügbaren Ressourcen auf drei verschiedene Arten:

Zuerst betrachten wir die Simulation einer unitären Transformation mit Hilfe der Zeitentwicklung und lokalen unitären Transformationen (siehe Definition 4.1). Der englische Begriff „gate simulation“ wurde in [BCL+02, S. 3] eingeführt. Die folgende Definition ist eine Spezialisierung der Definitionen 1.2 und 1.3.

Definition 4.1 (Simulation von unitären Transformationen)**.** Ein n-Qubit-System mit einem Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U in der Zeit $0 \leq t \in \mathbb{R}$, falls lokale unitäre Transformationen U_0 und U_j sowie Zeiten $0 \leq t_j \in \mathbb{R}$ mit $t = \sum_{j=1}^{m} t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, und $m \in \mathbb{N} \cup \{0, \infty\}$ existieren, so daß

$$U = \left[\prod_{j=1}^{m} U_j \exp(-iHt_j) \right] U_0.$$

Bemerkung. Da die unitäre Gruppe nicht kommutativ ist, ist die Bedeutung des Symbols $\prod$ für Elemente der unitären Gruppe folgendermaßen definiert (vgl. Seite 6):

$$\prod_{j=e}^{f} V_j := \begin{cases} \left(\prod_{j=e+1}^{f} V_j \right) V_e & \text{für } f \geq e, \\ \mathrm{Id} & \text{für } f < e, \end{cases}$$

wobei $e, f \in \mathbb{Z}$ und mit Id wird die Identität der unitären Gruppe bezeichnet. Falls f unendlich ist, bezeichnet das Symbol $\prod$ ein Element aus dem Abschluß der konvergenten Produkte.

Als zweites führen wir ein Konzept von infinitesimaler Simulation von unitären Transformationen ein. Eine zu erzeugende unitäre Transformation U wird als Punkt auf einer Einparameter-Gruppe $\exp(-iH't')$ betrachtet. Bei einer infinitesimalen Simulation eines Hamilton-Operators H' wird davon ausgegangen, daß das Kontrollsystem die zugehörige Einparameter-Gruppe für infinitesimale Zeiten t' simuliert, d. h., daß die Ableitungen der Einparameter-Gruppe und der Simulation für infinitesimale Zeiten übereinstimmen. Wir betonen, daß die infinitesimale Simulation eines Hamilton-Operators in Definition 4.2 unabhängig von der unitären Transformation U definiert wird.

Definition 4.2 (Infinitesimale Simulation eines Hamilton-Operators)**.** Ein n-Qubit-System mit einem Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator H' infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, falls lokale unitäre Transformationen U_0 und U_j sowie Zeiten $0 \leq t_j \in \mathbb{R}$ mit $t = \sum_{j=1}^{m} t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, und $m \in \mathbb{N} \cup \{0, \infty\}$ existieren, so daß $\prod_{j=0}^{m} U_j$ gleich der Identität in der unitären Gruppe ist und die folgende Gleichung erfüllt ist ($t' \in \mathbb{R}$):

$$\lim_{\substack{t' \to 0 \\ t' > 0}} \left[\frac{d}{dt'} \exp(-it'H') \right] = \lim_{\substack{t' \to 0 \\ t' > 0}} \left(\frac{d}{dt'} \left\{ \left[\prod_{j=1}^{m} U_j \exp(-it'Ht_j) \right] U_0 \right\} \right). \tag{4.1}$$

Bemerkung. Die Bedingung $\prod_{j=0}^{m} U_j = \mathrm{Id}$ sorgt dafür, daß das von den unitären Transformationen U_0 und U_j sowie den Zeiten t_j spezifizierte Programm für $t' \to 0$ nahe der

Identität operiert. Weiter bezeichnet $t = \sum_{j=1}^{m} t_j$ den Faktor um den sich die Implementierungszeit der rechten Seite der Gleichung (4.1) von der Implementierungszeit der linken Seite der Gleichung (4.1) unterscheidet. Dabei werden nur sehr kleine Implementierungszeiten betrachtet ($t' \to 0$).

In den Referenzen [WJB02; JWB02; WRJB02b; WRJB02a; Woc03] wurde die infinitesimale Simulation eines Hamilton-Operators in erster Näherung auf eine globale Simulation aller unitärer Transformationen erweitert. Ähnliche Methoden wurden in [BCL+02] verwendet, um die Zeitentwicklung des zu kontrollierenden Systems exakt mit Simulation eines Hamilton-Operators nachzubilden. Nachfolgend wurde in [BCL+02] angemerkt, daß es nur infinitesimal möglich ist, die Zeitentwicklung des zu kontrollierenden Systems exakt nachzubilden, da die Kontrollmöglichkeiten nicht kontinuierlich sind. Wir betrachten in diesem Kapitel keine solchen Approximationen.

Obwohl Definition 4.2 die wesentliche Bedeutung der infinitesimalen Simulation eines Hamilton-Operators beschreibt, ist diese Beschreibung reichlich unpraktisch. Deshalb geben wir nun eine äquivalente Bedingung an, die üblicherweise als Definition verwendet wird [WJB02; JWB02; WRJB02b; WRJB02a; Che03].

Lemma 4.3. Ein n-Qubit-System mit einem Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator H' infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, falls lokale unitäre Transformationen U_0 und U_j sowie Zeiten $0 \leq t_j \in \mathbb{R}$ mit $t = \sum_{j=1}^{m} t_j$, $j \in \mathbb{N}$, $1 \leq j \leq m$, und $m \in \mathbb{N} \cup \{0, \infty\}$ existieren, so daß die folgende Gleichung erfüllt ist:

$$H' = \sum_{j=1}^{m} t_j ({V_j}^{-1} H V_j). \tag{4.2}$$

Beweis. Die notwendige Bedingung: Die linke Seite der Gleichung (4.1) ist gleich $-iH'$ und die rechte Seite der Gleichung (4.1) ist gleich

$$\lim_{\substack{t' \to 0 \\ t' > 0}} \left[\frac{d}{dt'} \left(\left\{ \prod_{j=1}^{m} \exp\left[-it' (W_j H {W_j}^{-1}) t_j \right] \right\} W_0 \right) \right], \tag{4.3}$$

wobei

$$W_j = \begin{cases} U_m & \text{für } j = m, \\ W_{j+1} U_j & \text{für } 0 \leq j < m. \end{cases}$$

Wir bilden die Ableitung, berechnen den Grenzwert und setzen das Ergebnis von Gleichung (4.3) mit $-iH'$ gleich. Dann benutzen wir die Gleichungen $V_j := {W_j}^{-1}$ und $W_0 = \prod_{j=0}^{m} U_j = \mathrm{Id}$ und erhalten die Gleichung (4.2).

Die hinreichende Bedingung: Wir setzen die Gleichung (4.2) in die Gleichung (4.1) ein und erhalten die hinreichende Bedingung. □

Als drittes führen wir eine Version von infinitesimaler Simulation unitärer Transformationen ein, die explizit von der unitären Transformation U abhängt.

Definition 4.4 (Infinitesimale Simulation unitärer Transformationen)**.** Ein n-Qubit-System mit einem Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U infinitesimal in der Zeit

$0 \leq t \in \mathbb{R}$, falls ein Hamilton-Operator H' und lokale Transformationen U_1 und U_2 existieren, so daß die Gleichung $U = U_1 \exp(-iH')U_2$ erfüllt ist und das System den Hamilton-Operator H' infinitesimal in der Zeit t simuliert.

Bemerkung. Tatsächlich benutzen wir Definition 4.4 nicht explizit. Aber wir geben diese Definition an, um zu betonen, daß die Definition 4.2 unabhängig von der unitären Transformation U ist und daß die Definition 4.2 nicht verschiedene Zerlegungen der unitären Transformation U berücksichtigt, die potenziell zu unterschiedlichen Hamilton-Operatoren H' führen können. Die Existenz verschiedener Hamilton-Opertoren H' wird in Abschnitt 4.4 betrachtet.

Bemerkung. Im Gegensatz zu unserer bisheriger Konvention in diesem Kapitel verwenden wir im folgenden die Exponentialfunktion $\exp(itH)$ ohne Minuszeichen. Wir nehmen an, daß H das Minuszeichen enthält und daß t weiterhin positiv ($t \geq 0$) ist.

Bevor wird fortfahren, diskutieren wir unser Modell. Verschränkung beschreibt wesentliche nicht-lokale Eigenschaften von Quantenzuständen und unitärer Transformationen. Da die Verschränkung invariant unter lokalen unitären Transformationen ist [NC00], scheint es plausibel, die Zeit zur Erzeugung von lokaler unitärer Transformationen zu vernachlässigen. Diese Vorgehensweise wird durch die allgemeine Annahme unterstützt, daß die Erzeugung von Zwei-Qubit-Transformationen als bedeutend schwerer betrachtet wird als die Erzeugung von Ein-Qubit-Transformationen [HH02]. Zusätzlich wird die Anwendung von lokalen unitären Transformationen in einer vernachlässigbaren Zeit in der Kernresonanz gewöhnlich als gute Approximation angesehen, da lokale und nicht-lokale Transformationen auf verschiedenen Zeitskalen operieren [HW68; EBW97; KBG01].

4.2. Lie-theoretische Grundlagen

In diesem Abschnitt führen wir Lie-theoretischen Begriffe und Methoden ein, die wir später verwenden werden. Dabei wird die besondere Bedeutung der Lie-Theorie für die betrachteten Problemstellungen hervorgehoben. Zusätzlich ist der Text dadurch einfacher zu lesen und ist in sich abgeschlossen. Dieser Abschnitt kann als Referenz betrachtet werden. Dieser Abschnitt wurde teilweise von der Darstellung in den Referenzen [KBG01; KG01; ZVSW03] inspiriert

4.2.1. Grundlegende Konzepte

In diesem Kapitel können wir Lie-Gruppen als lineare Matrix-Gruppen auffassen, d. h. als abgeschlossene Untergruppen der allgemeinen linearen Gruppe. Wir verweisen bzgl. der (elementaren) Lie-Theorie und der verwendeten Notation auf Anhang A. Im folgenden sei G eine Lie-Gruppe und $\mathfrak{g}$ die zugehörige Lie-Algebra.

Definition 4.5 (Orthogonale symmetrische Lie-Algebra, siehe Referenz [Hel01, S. 213] und Referenz [KN96, S. 225–226 und S. 246])**.** Ein Paar $(\mathfrak{g}, \theta)$ ist eine orthogonale symmetrische Lie-Algebra, falls gilt

(i) $\mathfrak{g}$ ist eine reelle Lie-Algebra,

(ii) θ ist ein involutiver Automorphismus von $\mathfrak{g}$

(iii) und die zusammenhängende Lie-Gruppe der von $\mathrm{ad}_{\mathfrak{g}}(\mathfrak{k})$ erzeugten linearen Transformationen von $\mathfrak{g}$ ist kompakt, wobei $\mathfrak{k}$ die Menge der Fixpunkte von θ in der Lie-Gruppe $\mathfrak{g}$ bezeichnet.

Bemerkung. Ein Automorphismus der Lie-Algebra $\mathfrak{g}$ respektiert die Lie-Klammer, d. h., für alle Elemente g und h von $\mathfrak{g}$ gilt $\theta([g,h]) = [\theta(g), \theta(h)]$. Ein involutiver Automorphismus ist zusätzlich selbstinvers. Seien $\mathfrak{k}$ und $\mathfrak{p}$ die Eigenräume zu den Eigenwerten $+1$ bzw. -1 von θ in der Lie-Algebra $\mathfrak{g}$. Wir führen die kanonische Zerlegung $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ der Lie-Algebra $\mathfrak{g}$ ein. Die Bedingung (ii) der Definition 4.5 ist äquivalent zu

$$[\mathfrak{k},\mathfrak{k}] \subset \mathfrak{k},\ [\mathfrak{k},\mathfrak{p}] \subset \mathfrak{p},\ [\mathfrak{p},\mathfrak{p}] \subset \mathfrak{k} \text{ (siehe [KN96, S. 226–227]).} \tag{4.4}$$

In der Referenz [KBG01] wurde diese Zerlegung als Cartan-Zerlegung bezeichnet. Falls Gleichung (4.4) gilt, können wir θ auf folgende Weise definieren

$$\theta(k) = k \text{ für alle } k \in \mathfrak{k} \text{ und } \theta(p) = -p \text{ für alle } p \in \mathfrak{p}. \tag{4.5}$$

Falls $\mathfrak{g}$ eine Lie-Algebra einer kompakten Lie-Gruppe G ist, dann gilt zusätzlich, daß die Bedingung (iii) der Definition 4.5 immer gültig ist.

Im folgenden nehmen wir an, daß $\mathfrak{g}$ halbeinfach ist und daß $(\mathfrak{g}, \theta)$ eine orthogonale symmetrische Lie-Algebra ist. Dabei ist $\mathfrak{g}$ halbeinfach, falls die Killing-Form von $\mathfrak{g}$ ist nicht entartet ist. Als Beispiel für eine halbeinfache Lie-Algebra geben wir die Lie-Algebra $\mathfrak{su}(2^n)$ zur Lie-Gruppe $\mathrm{SU}(2^n)$ an. Wir wählen eine kanonische Zerlegung $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$, die die Gleichung (4.4) erfüllt, sowie eine abelsche Unteralgebra $\mathfrak{a}$ von $\mathfrak{p}$ aus. Wir bezeichnen die von $\mathfrak{k}$ bzw. $\mathfrak{a}$ erzeugten Untergruppen von G mit $\mathrm{K} = \exp(\mathfrak{k})$ bzw. $\mathrm{A} = \exp(\mathfrak{a})$. Wir erhalten eine Zerlegung $\mathrm{G} = \mathrm{K\,A\,K}$ der Lie-Gruppe G:

Faktum 4.6 (K A K-Zerlegung der Lie-Gruppe G [Hel01, Ch. V, Thm. 6.7])**.** Mit der oben eingeführten Notation können wir die Lie-Gruppe G zur Lie-Algebra $\mathfrak{g}$ wie folgt zerlegen:

$$\mathrm{G} = \mathrm{K\,A\,K}.$$

Ähnlich wie die adjungierte Darstellung $\mathrm{ad}_{\mathfrak{g}}$ der Lie-Algebra $\mathfrak{g}$ auf sich selbst können wir die adjungierte Darstellung $\mathrm{Ad}_{\mathfrak{g}}$ der Lie-Gruppe G auf der Lie-Algebra $\mathfrak{g}$ definieren. Für jedes Element $G \in \mathrm{G}$ führen wir die Abbildung $\phi_{\mathrm{G}}(G) : H \mapsto G^{-1}HG$ mit der Signatur $\mathrm{G} \to \mathrm{G}$ ein. Die Abbildung $\mathrm{Ad}_{\mathfrak{g}}(G)$ hat die Signatur $\mathfrak{g} \to \mathfrak{g}$ und ist als die Ableitung von $\phi_{\mathrm{G}}(G)$ definiert. Für Matrix-Darstellungen können wir $\mathrm{Ad}_{\mathfrak{g}}(G)$ als die Abbildung $g \mapsto G^{-1}gG$ angeben. Wir benutzen die Abkürzung $\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}) := \bigcup_{K \in \mathrm{K}} \mathrm{Ad}_{\mathfrak{g}}(K)$ und erhalten folgende Verbindung zwischen dem Unterraum $\mathfrak{p}$ und seiner abelschen Unteralgebra $\mathfrak{a}$:

Faktum 4.7 ([Hel01, Ch. V, Lemma 6.3 (iii)])**.** Die folgende Gleichung gilt:

$$\mathfrak{p} = (\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(\mathfrak{a}).$$

4.2.2. Die Weyl-Gruppe und die infinitesimale Konvexität

Wir führen die Notationen

$$C_{\mathrm{K}}(\mathfrak{a}) := \{K \in \mathrm{K} |\, (\mathrm{Ad}_{\mathfrak{g}}(K))(a) = a \text{ für alle } a \in \mathfrak{a}\}$$

bzw.

$$N_{\mathrm{K}}(\mathfrak{a}) := \{K \in \mathrm{K} |\, (\mathrm{Ad}_{\mathfrak{g}}(K))(\mathfrak{a}) \subset \mathfrak{a}\}$$

für den Zentralisator $C_{\mathrm{K}}(\mathfrak{a})$ bzw. für den Normalisator $N_{\mathrm{K}}(\mathfrak{a})$ von $\mathfrak{a}$ in K ein.

Definition 4.8 (Weyl-Gruppe, siehe [Hel01, S. 284] oder [Kna02, S. 381])**.** Die Weyl-Gruppe bezüglich der abelschen Unteralgebra $\mathfrak{a}$ ist die Faktorgruppe $N_{\mathrm{K}}(\mathfrak{a})/C_{\mathrm{K}}(\mathfrak{a})$. Wir bezeichnen diese Gruppe mit $\mathcal{W}(\mathrm{G}, \mathrm{A})$, wobei $\mathrm{A} = \exp(\mathfrak{a})$.

Die Weyl-Gruppe $\mathcal{W}(\mathrm{G}, \mathrm{A})$ ist endlich (siehe Faktum 4.10). Um die Weyl-Gruppe explizit zu bestimmen, führen wir das Konzept der eingeschränkten Wurzeln ein.

Definition 4.9 (Eingeschränkte Wurzeln, siehe z. B. [Kna02, S. 370])**.** Sei λ ein lineares Funktional auf $\mathfrak{a}$. Der lineare Unterraum $\mathfrak{g}^{\lambda}$ ist definiert durch die Gleichung

$$\mathfrak{g}^{\lambda} = \{g \in \mathfrak{g} |\, [a, g] = \lambda(a)g \text{ für alle } a \in \mathfrak{a}\}.$$

Ein lineares Funktional λ wird als eingeschränkte Wurzel von $\mathfrak{g}$ bezüglich $\mathfrak{a}$ bezeichnet, falls $\mathfrak{g}^{\lambda} \neq \{0\}$ gilt und falls λ nicht identisch gleich null auf $\mathfrak{a}$ ist. Wir bezeichnen mit $\Delta_{\mathfrak{a}}$ die Menge der eingeschränkten Wurzeln von $\mathfrak{g}$ bezüglich $\mathfrak{a}$.

Bemerkung. In Referenz [Kna02, S. 370] sind die eingeschränkten Wurzeln bezüglich $i\mathfrak{a}$ definiert. Aber wir können die eingeschränkten Wurzeln auch bezüglich $\mathfrak{a}$ definieren.

Da $\mathfrak{g}$ halbeinfach ist, wissen wir, daß die Killing-Form $B_{\mathfrak{g}}$ eingeschränkt auf $\mathfrak{a} \times \mathfrak{a}$ nicht entartet ist. Deshalb sind eingeschränkte Wurzeln λ identisch mit der Abbildung $a \mapsto B_{\mathfrak{g}}(a_\lambda, a)$, wobei $a_\lambda \in \mathfrak{a}$ eindeutig definiert ist. Wir definieren die Killing-Form auch für eingeschränkte Wurzeln: $B_{\mathfrak{g}}(\lambda, \mu) := B_{\mathfrak{g}}(a_\lambda, a_\mu)$. Für $\lambda \in \Delta_{\mathfrak{a}}$ ist die Spiegelung $s_\lambda(\mu)$ einer eingeschränkten Wurzel $\mu \in \Delta_{\mathfrak{a}}$ an der Hyperebene $\{a \in \mathfrak{a} |\, \lambda(a) = 0\}$ durch die Gleichung

$$s_\lambda(\mu) := \mu - 2\frac{B_{\mathfrak{g}}(\mu, \lambda)}{B_{\mathfrak{g}}(\lambda, \lambda)}\lambda.$$

gegeben. Wir folgen Referenz [Hel01, S. 286] und definieren die Spiegelung s_λ auch für Elemente von $\mathfrak{a}$. Die Spiegelung $s_\lambda(a)$ von $a \in \mathfrak{a}$ an der Hyperebene $\{a \in \mathfrak{a} |\, \lambda(a) = 0\}$ ist durch die Gleichung

$$s_\lambda(a) = a - 2\frac{B_{\mathfrak{g}}(a, a_\lambda)}{B_{\mathfrak{g}}(a_\lambda, a_\lambda)}a_\lambda. \tag{4.6}$$

definiert.

Mit dieser Vorbereitung können wir die Weyl-Gruppe bezüglich $\mathfrak{a}$ auf folgende Weise berechnen:

Faktum 4.10 ([Kna02, S. 383])**.** Die Weyl-Gruppe bezüglich $\mathfrak{a}$ ist endlich und wird von den Spiegelungen s_λ mit $\lambda \in \Delta_{\mathfrak{a}}$ erzeugt.

Wir erinnern daran, daß $\mathcal{W}(\mathrm{G},\mathrm{A})$ eine Teilmenge von K ist und daß $\mathcal{W}(\mathrm{G},\mathrm{A})$ mittels der adjungierten Darstellung $\mathrm{Ad}_{\mathfrak{g}}(K)$ ($K \in \mathrm{K}$) auf $\mathfrak{a}$ operiert.

Definition 4.11 (Weyl-Orbit, siehe z. B. [Kos73, S. 422])**.** Der Weyl-Orbit $\mathcal{W}(a)$ von $a \in \mathfrak{a}$ ist als die Menge $\{(\mathrm{Ad}_{\mathfrak{g}}(W))(a) |\, W \in \mathcal{W}(\mathrm{G},\mathrm{A})\}$ definiert. Unter Benutzung von Faktum 4.7 erhalten wir, daß der Weyl-Orbit $\mathcal{W}(p)$ von $p \in \mathfrak{p}$ gleich $\mathcal{W}(p) := \mathcal{W}(a)$ ist. Dabei bezeichnet a ein Element aus $(\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(p) \cap \mathfrak{a}$.

Um zu verstehen, daß die Definition von $\mathcal{W}(p)$ für $p \in \mathfrak{p}$ unabhängig von a ist und damit wohldefiniert ist, charakterisieren wir Weyl-Orbits etwas genauer.

Faktum 4.12 ([Kna02, Lemma 7.38])**.** Für $a, a' \in \mathfrak{a}$ und $K \in \mathrm{K}$ gelte die Gleichung $(\mathrm{Ad}_{\mathfrak{g}}(K))(a) = a'$. Dann existiert ein Element $K' \in N_{\mathrm{K}}(\mathfrak{a})$, so daß $(\mathrm{Ad}_{\mathfrak{g}}(K'))(a) = a'$ gilt.

Nun erhalten wir aus Faktum 4.12, daß zwei Elemente a und a' des Weyl-Orbits $\mathcal{W}(p)$ von $p \in \mathfrak{p}$ konjugiert bezüglich eines Elementes der Weyl-Gruppe sind. Dies beweist, daß die Definition 4.11 von $\mathcal{W}(p)$ unabhängig von a ist. Zusätzlich erhalten wir, daß der Weyl-Orbit $\mathcal{W}(p)$ identisch mit der Menge $\mathfrak{a} \cap (\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(p)$ ist. Wir bezeichnen die konvexe Hülle des Weyl-Orbits $\mathcal{W}(p)$ mit $\mathfrak{c}(p)$. Wir geben nun die infinitesimale Version von Kostants Konvexitätstheorem an.

Faktum 4.13 (Kostants Konvexitätstheorem (infinitesimale Version), siehe [Kos73, Thm. 8.2] oder [Hec80, Thm. 1])**.** Sei Γ die orthogonale Projektion von $\mathfrak{p}$ auf $\mathfrak{a}$ bezüglich der Killing-Form. Für jedes Element $p \in \mathfrak{p}$ erhalten wir

$$\Gamma\Big((\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(p)\Big) = \mathfrak{c}(p).$$

Bemerkung. Die wesentliche Bedeutung der infinitesimalen Version von Kostants Konvexitätstheorem (Faktum 4.13) ist, daß die Projektion von $(\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(p)$ auf $\mathfrak{a}$ bezüglich der Killing-Form eine konvexe Menge ist und daß deren Extremalpunkte durch den Weyl-Orbit $\mathcal{W}(p)$ gegeben sind.

Um Weyl-Orbits näher zu charakterisieren, führen wir weitere Konzepte ein. Der Unterraum $\mathfrak{a}$ kann in zusammenhängende Komponenten, die sogenannten Weyl-Kammern, aufgeteilt werden.

Definition 4.14 (Weyl-Kammern [Hel01, S. 287])**.** Sei λ eine eingeschränkte Wurzel von $\mathfrak{g}$ bezüglich $\mathfrak{a}$. Die Hyperebenen $\{a \in \mathfrak{a} |\, \lambda(a) = 0\}$ teilen $\mathfrak{a}$ in endlich viele und zusammenhängende Komponenten ein. Dabei werden die Komponenten ohne ihre Trennhyperebenen als Weyl-Kammern bezeichnet. Der Abschluß einer Weyl-Kammer enthält die Trennhyperebenen und wird als abgeschlossene Weyl-Kammer bezeichnet.

Die Weyl-Gruppe operiert auf den Weyl-Kammern:

Faktum 4.15 ([Hel01, Thm. 2.12, Ch. VII])**.** Die Weyl-Gruppe permutiert die Weyl-Kammern.

Wir wählen eine beliebige, aber unveränderliche Ordnung auf den eingeschränkten Wurzeln von $\mathfrak{g}$ bezüglich $\mathfrak{a}$. Aus diesem Grund können wir die eingeschränkten Wurzeln in positive und negative (eingeschränkte) Wurzeln einteilen, wobei positiv und negativ bezüglich der gewählten Ordnung definiert ist. Eine eingeschränkte Wurzel wird als (eingeschränkte) Fundamentalwurzel bezeichnet, falls sie positiv ist und nicht als eine Summe von zwei positiven (eingeschränkten) Wurzeln geschrieben werden kann [Sam99, S. 59]. Sei $\{\alpha_k\} \subset \Delta_\mathfrak{a}$ die Menge der eingeschränkten Fundamentalwurzeln. Da die Killing-Form eingeschränkt auf $\mathfrak{a}\times\mathfrak{a}$ nicht entartet ist, können wir für jede eingeschränkte Wurzel λ ein Element $a_\lambda \in \mathfrak{a}$ definieren, so daß $B_\mathfrak{g}(a_\lambda, a) = \lambda(a)$ für alle $a \in \mathfrak{a}$ gilt. Die Menge $\{a \in \mathfrak{a} |\, B_\mathfrak{g}(a_{\alpha_k}, a) > 0 \text{ für alle } \alpha_k\}$ ist eine Weyl-Kammer und wird als fundamentale Weyl-Kammer bezeichnet [Sam99, S. 61].

Faktum 4.16 (angepaßt von [Sam99, Prop. I, Sec. 2.11])**.** Seien λ bzw. μ eingeschränkte Wurzeln bezüglich der Elemente a_λ bzw. a_μ der abgeschlossenen fundamentalen Weyl-Kammer. Das Element a_μ liegt genau dann in der konvexen Hülle der Weyl-Kammer $\mathcal{W}(a_\lambda)$ von a_λ, wenn $\lambda(a) \geq \mu(a)$ für alle Elemente a der fundamentalen Weyl-Kammer gilt. Die Bedingung $\lambda(a) \geq \mu(a)$ ist äquivalent zu $B_\mathfrak{g}(a_\lambda, a) \geq B_\mathfrak{g}(a_\mu, a)$.

4.2.3. Der Zwei-Qubit-Fall

Wir betrachten nun den Fall G = SU(4). Für die explizite Rechnung verwenden wir eine Matrix-Darstellung für die reelle halbeinfache Lie-Algebra $\mathfrak{su}(4)$ der Lie-Gruppe G. Seien

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ und } \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

die Pauli-Matrizen und sei

$$\sigma_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

die Identitätsmatrix. Wir benutzen die Notation $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, und $\sigma_3 = \sigma_z$ und definieren

$$\begin{aligned}
X_1 &:= \frac{i}{2}\sigma_0 \otimes \sigma_1, X_2 := \frac{i}{2}\sigma_0 \otimes \sigma_2, X_3 := \frac{i}{2}\sigma_0 \otimes \sigma_3, \\
X_4 &:= \frac{i}{2}\sigma_1 \otimes \sigma_0, X_5 := \frac{i}{2}\sigma_2 \otimes \sigma_0, X_6 := \frac{i}{2}\sigma_3 \otimes \sigma_0, \\
X_7 &:= \frac{i}{2}\sigma_1 \otimes \sigma_1, X_8 := \frac{i}{2}\sigma_2 \otimes \sigma_2, X_9 := \frac{i}{2}\sigma_3 \otimes \sigma_3, \\
X_{10} &:= \frac{i}{2}\sigma_1 \otimes \sigma_2, X_{11} := \frac{i}{2}\sigma_1 \otimes \sigma_3, X_{12} := \frac{i}{2}\sigma_2 \otimes \sigma_1, \\
X_{13} &:= \frac{i}{2}\sigma_2 \otimes \sigma_3, X_{14} := \frac{i}{2}\sigma_3 \otimes \sigma_1, X_{15} := \frac{i}{2}\sigma_3 \otimes \sigma_2.
\end{aligned}$$

Die Standarddarstellung (oder definierende Darstellung) der Lie-Algebra $\mathfrak{su}(4)$ ist auf folgende Weise gegeben:

$$\mathfrak{g} := \mathfrak{su}(4) = \mathrm{span}_\mathbb{R}\{X_1, \ldots, X_{15}\}.$$

Dabei bezeichnet $\mathrm{span}_{\mathbb{R}}$ den reellen Aufspann. Wir definieren die Vektorräume

$$\mathfrak{k} := \mathrm{span}_{\mathbb{R}}\{X_1, \ldots, X_6\},\ \mathfrak{p} := \mathrm{span}_{\mathbb{R}}\{X_7, \ldots, X_{15}\} \text{ und } \mathfrak{a} := \mathrm{span}_{\mathbb{R}}\{X_7, \ldots, X_9\}.$$

Nun können wir einfach überprüfen, daß $\mathfrak{k}$ und $\mathfrak{p}$ die Kommutatorrealationen in Gleichung (4.4) erfüllen. Da die Lie-Gruppe SU(4) kompakt ist, erhalten wir, daß das Paar $(\mathfrak{g}, \theta)$ eine orthogonale symmetrische Lie-Algebra ist, wobei θ durch Gleichung (4.5) gegeben ist. Der Unterraum $\mathfrak{a}$ ist eine abelsche Unteralgebra von $\mathfrak{p}$. Die Menge der eingeschränkten Wurzeln bezüglich $\mathfrak{a}$ kann als die Eigenwerte von $\mathrm{ad}_{\mathfrak{g}}(c_1X_7 + c_2X_8 + c_3X_9)$ bestimmt werden:

$$\{\pm i(c_2 - c_3), \pm i(c_2 + c_3), \pm i(c_1 - c_3), \pm i(c_1 + c_3), \pm i(c_1 + c_2), \pm i(c_1 - c_2)\}. \quad (4.7)$$

Wir verwenden Gleichung (4.6) zur Bestimmung einer Erzeugermenge der Weyl-Gruppe (bezüglich $\mathfrak{a}$) als eine Menge von Matrizen

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad (4.8)$$

die auf den Vektoren

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \triangleq X_7,\ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \triangleq X_8,\ \text{und}\ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \triangleq X_9 \quad (4.9)$$

operieren.

Mit der Notation aus Gleichung (4.9) geben wir die Killing-Form eingeschränkt auf $\mathfrak{a} \times \mathfrak{a}$ auf folgende Weise an:

$$B_{\mathfrak{g}}(a, b)\big|_{\mathfrak{a}\times\mathfrak{a}} := a^T \begin{pmatrix} -8 & 0 & 0 \\ 0 & -8 & 0 \\ 0 & 0 & -8 \end{pmatrix} b.$$

Die Elemente $a_\lambda \in \mathfrak{a}$ bezüglich der eingeschränkten Wurzeln λ in Gleichung (4.7) können wir nun als Elemente $a_\lambda \in \mathfrak{a}$ angeben, so daß $B_{\mathfrak{g}}(a_\lambda, a) = \lambda(a)$ für alle $a \in \mathfrak{a}$ gilt:

$$\left\{ \frac{\pm i}{-8} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \frac{\pm i}{-8} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \frac{\pm i}{-8} \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \frac{\pm i}{-8} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \frac{\pm i}{-8} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{\pm i}{-8} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right\}.$$

Wir haben die Basis aus Gleichung (4.9) für die Darstellung der Elemente a_λ verwendet. Um unsere Ergebnisse im Kontext von Referenz [BCL$^+$02] zu präsentieren, wählen wir die Ordnung auf den eingeschränkten Wurzeln so, daß die Wurzeln aus der Gleichung (4.7) mit positivem Vorzeichen als positiv gelten. Damit erhalten wir für ein

Element $d = d_1X_7 + d_2X_8 + d_3X_9$ der fundamentalen Weyl-Kammer die folgenden Gleichungen:

$$\{d_2 - d_3 > 0, d_2 + d_3 > 0, d_1 - d_3 > 0, d_1 + d_3 > 0, d_1 + d_2 > 0, d_1 - d_2 > 0\}. \quad (4.10)$$

Dabei setzen wir $(\mathbb{R}, >)$ mit $(i\mathbb{R}, >)$ gleich, indem wir für alle Elemente $r_1, r_2 \in \mathbb{R}$ folgende Notation verwenden: $ir_1 > ir_2 \Leftrightarrow r_1 > r_2$.

4.3. Simulation von Hamilton-Operatoren auf Zwei-Qubit-Systemen

4.3.1. Lie-theoretischer Zugang

Ausgehend von Definition 4.2 betrachten wir nun die infinitesimale Simulation von Hamilton-Operatoren in Zwei-Qubit-Systemen. Wir betonen, daß im Zwei-Qubit-Fall die lokalen unitären Transformationen durch die Elemente aus $\mathrm{K} = \exp(\mathfrak{k})$ gegeben sind. Wir verwenden nun die Notation aus Abschnitt 4.2, insbesondere aus Abschnitt 4.2.3. Da wir nur Hamilton-Operatoren ohne lokale Terme betrachten (siehe Abschnitt 4.1), können wir für alle nicht-lokale Hamilton-Operatoren H und H' annehmen, daß $iH \in \mathfrak{p}$ und $iH' \in \mathfrak{p}$ gilt. Dabei bezeichnet $\mathfrak{p}$ den Untervektorraum der Lie-Algebra $\mathfrak{g}$, der in Abschnitt 4.2 eingeführt wurde. Deshalb können wir mit Hilfe von Faktum 4.7 alle nicht-lokale Hamilton-Operatoren H' unter Verwendung eines Elements $a' \in \mathfrak{a}$ und einer lokalen unitären Transformation L' auf folgende Weise darstellen: $H' = (\mathrm{Ad}_{\mathfrak{g}}((L')^{-1}))(a')$.

Theorem 4.17. Wir nehmen an, daß H und H' nicht-lokale Hamilton-Operatoren auf einem Zwei-Qubit-System sind. Sei a' ein Element von $\mathfrak{a}$ mit der Eigenschaft, daß $a' = (\mathrm{Ad}_{\mathfrak{g}}(L'))(H')$ für eine lokale unitäre Transformation L' gilt.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator genau dann infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, wenn der Hamilton-Operator (a'/t) im konvexen Abschluß des Weyl-Orbits $\mathcal{W}(H)$ von H liegt. Die Bedingung ist unabhängig von der Wahl des Elementes a'.

Bemerkung. Tatsächlich ist Theorem 4.17 eine infinitesimale Variante von Faktum 4.25 (siehe unten und in Referenz [KBG01]). Um die Verbindung zwischen Theorem 4.18 und den Ergebnissen aus Referenz [KBG01] zu verdeutlichen, geben wir hier nun einen Beweis der infinitesimalen Version an. Dabei verwenden wir Argumente aus den Referenzen [KBG01; BCL$^+$02].

Beweis. Wir nehmen an, daß

$$t \sum_{i=1}^{m_3} q_i'' (\mathrm{Ad}_{\mathfrak{g}}(K_i''))(H) \quad (4.11)$$

eine infinitesimale Simulation von H' in der Zeit t ist. Dabei ist K_i'' eine lokale unitäre Transformation, $H, H' \in \mathfrak{p}$, $q_i'' \geq 0$ und $\sum_{i=1}^{m_3} q_i'' = 1$.

Aufgrund von Faktum 4.7 existieren Elemente a und a' in $\mathfrak{a}$, so daß für geeignet gewählte lokale unitäre Transformationen L und L' die Gleichungen $a = (\mathrm{Ad}_{\mathfrak{g}}(L))(H)$ und $a' = (\mathrm{Ad}_{\mathfrak{g}}(L'))(H')$ gelten. Wir betonen, daß lokale unitäre Transformationen keine Zeit benötigen. Deshalb ist die Existenz der Simulation aus Gleichung (4.11) äquivalent zur Existenz der Simulation $t\sum_{i=1}^{m_2} q_i'(\mathrm{Ad}_{\mathfrak{g}}(K_i'))(a)$ von a' durch a in der Zeit t, wobei K_i' eine lokale unitäre Transformation bezeichnet, $q_i' \geq 0$ und $\sum_{i=1}^{m_2} q_i' = 1$. Wir bezeichnen mit Γ bzw. Γ' die orthogonalen Projektionen (bezüglich der Killing-Form) von $\mathfrak{p}$ auf $\mathfrak{a}$ bzw. $\mathfrak{a}^{\perp}$. Wir können nun die Simulation auf folgende Weise angeben:

$$t\sum_{i=1}^{m_2} q_i' \left[\Gamma\Big((\mathrm{Ad}_{\mathfrak{g}}(K_i'))(a)\Big) + \Gamma'\Big((\mathrm{Ad}_{\mathfrak{g}}(K_i'))(a)\Big)\right] = a'.$$

Dies ist äquivalent zu

$$t\sum_{i=1}^{m} q_i \Gamma\Big((\mathrm{Ad}_{\mathfrak{g}}(K_i))(a)\Big) = a', \tag{4.12}$$

wobei K_i geeignet gewählte lokale unitäre Transformationen sind, $q_i \geq 0$ und $\sum_{i=1}^{m} q_i = 1$. Die letzte Äquivalenz ist notwendig, da wir die Projektion Γ mit Hilfe von Faktum 4.13 als konvexe Kombination schreiben können. Und die Äquivalenz ist hinreichend, da der Term $\sum_{i=1}^{m_2} q_i'\Gamma'\big((\mathrm{Ad}_{\mathfrak{g}}(K_i'))(a)\big)$ gleich null sein muß.

Aus der Bemerkung nach Faktum 4.13 wissen wir, daß die Projektion von $(\mathrm{Ad}_{\mathfrak{g}}(\mathrm{K}))(p)$ auf $\mathfrak{a}$ bezüglich der Killing-Form eine konvexe Menge ist. Folglich können wir Gleichung (4.12) in die Gleichung

$$\Gamma\Big((\mathrm{Ad}_{\mathfrak{g}}(K'))(a)\Big) = (a'/t)$$

umformen, wobei wir eine geeignet gewählte lokale unitäre Transformation K' benötigen. Mit Faktum 4.13 erhalten wir, daß (a'/t) im konvexen Abschluß des Weyl-Orbits $\mathcal{W}(a)$ von a liegt. Da $a = (\mathrm{Ad}_{\mathfrak{g}}(L))(H)$, können wir a im letzten Satz durch H ersetzen. Damit haben wir das Theorem bis auf die Unabhängigkeit von der Wahl von a' bewiesen.

Nehmen wir an, wir würden a' durch ein Element $a'' \in \mathfrak{a}$ ersetzen, so daß $a'' = (\mathrm{Ad}_{\mathfrak{g}}(L''))(H')$ für eine geeignet gewählte lokale unitäre Transformation L'' gilt. Aufgrund von Faktum 4.12 existiert ein Element $W \in \mathcal{W}(\mathrm{G},\mathrm{A})$ mit $a'' = (\mathrm{Ad}_{\mathfrak{g}}(W^{-1}))(a')$. Da die Operation eines Elementes der Weyl-Gruppe den Weyl-Orbit $\mathcal{W}(H)$ invariant läßt, gilt $\mathcal{W}(H) = (\mathrm{Ad}_{\mathfrak{g}}(W))(\mathcal{W}(H))$. Es ist offensichtlich, daß der konvexe Abschluß des Weyl-Orbits $\mathcal{W}(H)$ auch unverändert bleibt. Deshalb ist das Element a' genau dann in dem konvexen Abschluß des Weyl-Orbits $\mathcal{W}(H)$, wenn dies für a'' gilt. □

Für $a' \in \mathfrak{a}$ wurde in Referenz [BCL$^+$02] bewiesen, daß die Menge der Hamilton-Operatoren (a'/t), die in der Zeit eins simuliert werden können, konvex ist. Wir betonen, daß die Extremalpunkte dieser Menge durch den Weyl-Orbit $\mathcal{W}(H)$ gegeben sind. Und dieser Weyl-Orbit kann unter Benutzung von Gleichung (4.8) berechnet werden. In Referenz [BCL$^+$02] wurden die Extremalpunkte angegeben und ihre Extremalität wurde auf andere Weise bewiesen. Ausgehend von Referenz [BCL$^+$02] geben wir nun eine Version von Theorem 4.17 an, die eine einfacher zu überprüfende Bedingung für die infinitesimale Simulation von Hamilton-Operatoren im Zwei-Qubit-Fall ist.

Theorem 4.18 ([BCL+02, S. 11])**.** Seien H und H' nicht-lokale Hamilton-Operatoren auf einem Zwei-Qubit-System. Seien a und a' Elemente der abgeschlossenen fundamentalen Weyl-Kammer, so daß für geeignet gewählte lokale unitäre Transformationen L und L' die Gleichungen $a = a_1X_7 + a_2X_8 + a_3X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L))(H)$ und $a' = a'_1X_7 + a'_2X_8 + a'_3X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L'))(H')$ gelten.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator genau dann infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, wenn die folgenden Gleichungen gelten:

$$a_1 \geq a'_1/t, \tag{4.13a}$$
$$a_1 + a_2 + a_3 \geq (a'_1 + a'_2 + a'_3)/t, \tag{4.13b}$$
$$a_1 + a_2 - a_3 \geq (a'_1 + a'_2 - a'_3)/t. \tag{4.13c}$$

Bemerkung. Da wir die Elemente a und a' als Elemente der abgeschlossenen fundamentalen Weyl-Kammer wählen, sind sie (fast) eindeutige Elemente aus $\mathfrak{a}$. Falls a oder a' auf dem Rand der fundamentalen Weyl-Kammer liegen, sind sie Elemente der abgeschlossenen fundamentalen Weyl-Kammer, aber keine Elemente der fundamentalen Weyl-Kammmer. Einzig in diesem Fall sind die Elemente a oder a' möglicherweise nicht eindeutig und können als Elemente auf verschiedenen Trennhyperebenen der fundamentalen Weyl-Kammer gewählt werden.

Beweis. Da die Weyl-Gruppe die Weyl-Kammern (Faktum 4.15) permutiert, können wir a und a' als Elemente der abgeschlossenen fundamentalen Weyl-Kammer wählen. Aus Gleichung (4.10) folgt, daß ein Element $d = d_1X_7+d_2X_8+d_3X_9$ genau dann in der fundamentalen Weyl-Kammer liegt, wenn die Ungleichungen $d_2-d_3 > 0$, $d_2+d_3 > 0$, $d_1-d_3 > 0$, $d_1 + d_3 > 0$, $d_1 + d_2 > 0$ und $d_1 - d_2 > 0$ erfüllt sind. Durch Anwendung von Theorem 4.17 und Faktum 4.16 erhalten wir, daß $a_1d_1+a_2d_2+a_3d_3 \geq (a'_1d_1+a'_2d_2+a'_3d_3)/t$ für alle Elemente $d = d_1X_7 + d_2X_8 + d_3X_9$ der fundamentalen Weyl-Kammer gilt. Mit Hilfe des Computeralgebrasystems QEPCAD [CH91; QEP03] eliminieren wir die Quantoren aus der letzten Bedingung und wir erhalten die Bedingungen aus Gleichung (4.13). □

4.3.2. Majorisierung

In diesem Abschnitt führen wir zur späteren Verwendung Konzepte aus der Theorie der Majorisierung ein. Die Darstellung ist knapp, und wir verweisen für eine ausführlichere Behandlung auf die Referenzen [NV01; MO79; AU82; And89a; And89b; Bha97].

Wir bezeichnen eine Permutation eines Elementes $x = (x_1, \ldots, x_k)^T \in \mathbb{R}^k$ mit $x^\downarrow = (x_1^\downarrow, \ldots, x_k^\downarrow)^T$, falls $x_i^\downarrow \geq x_j^\downarrow$ für $i < j$ und $1 \leq i, j \leq k$.

Definition 4.19 (Majorisierung [Bha97, S. 28])**.** Ein Vektor $x \in \mathbb{R}^k$ wird von dem Vektor $y \in \mathbb{R}^k$ majorisiert, falls

$$\sum_{i=1}^{l} x_i^\downarrow \leq \sum_{i=1}^{l} y_i^\downarrow \text{ für alle } 1 \leq l \leq k$$

und

$$\sum_{i=1}^{k} x_i^{\downarrow} = \sum_{i=1}^{k} y_i^{\downarrow}$$

gilt. Die Notation $x \prec y$ besagt, daß x von y majorisiert wird.

Wir verwenden im folgenden das Konzept der s-Majorisierung aus Referenz [BCL$^+$02]. Für ein Element $x = (x_1, x_2, x_3)^T \in \mathbb{R}^3$ führen wir die Notation $\hat{x} = (|x_1|, |x_2|, |x_3|)^T$ ein, und wir definieren die s-geordnete Version $x^{\downarrow_s}$ von x, indem wir die Komponenten festlegen: $x_1^{\downarrow_s} := \hat{x}_1^{\downarrow}$, $x_2^{\downarrow_s} := \hat{x}_2^{\downarrow}$ und $x_3^{\downarrow_s} := \mathrm{sgn}(x_1x_2x_3)\hat{x}_3^{\downarrow}$. Das Vorzeichen von $x_1x_2x_3$ wird mit $\mathrm{sgn}(x_1x_2x_3)$ bezeichnet.

Definition 4.20 ([BCL$^+$02, S. 11])**.** Ein Vektor $x \in \mathbb{R}^3$ wird von $y \in \mathbb{R}^3$ s-majorisiert, falls

$$\begin{aligned} x_1^{\downarrow_s} &\leq y_1^{\downarrow_s}, \\ x_1^{\downarrow_s} + x_2^{\downarrow_s} + x_3^{\downarrow_s} &\leq y_1^{\downarrow_s} + y_2^{\downarrow_s} + y_3^{\downarrow_s} \end{aligned}$$

und

$$x_1^{\downarrow_s} + x_2^{\downarrow_s} - x_3^{\downarrow_s} \leq y_1^{\downarrow_s} + y_2^{\downarrow_s} - y_3^{\downarrow_s}$$

gilt. Die Notation $x \prec_s y$ besagt, daß x von y s-majorisiert wird.

Wir betonen, daß ein Element einer Lie-Unteralgebra $\mathfrak{a}$ genau dann s-geordnet ist, wenn dieses Element in der abgeschlossenen fundamentalen Weyl-Kammer liegt. Die Bedingungen dafür sind in Gleichung (4.10) angegeben, außer daß die Relation $<$ durch die Relation $\leq$ ersetzt werden muß. Damit erhalten wir eine geometrische Motivation für den Begriff der s-geordneten Vektoren. Zusätzlich sind die notwendigen und hinreichenden Bedingungen für die infinitesimale Simulation von Hamilton-Operatoren in Gleichung (4.13) äquivalent zur Definition der s-Majorisierung.

Korollar 4.21 ([BCL$^+$02, S. 11])**.** Wir nehmen an, daß H und H' nicht-lokale Hamilton-Operatoren auf einem Zwei-Qubit-System sind. Seien a und a' Elemente der abgeschlossenen fundamentalen Weyl-Kammer, so daß für geeignet gewählte lokale unitäre Transformationen L und L' die Gleichungen $a = a_1X_7 + a_2X_8 + a_3X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L))(H)$ und $a' = a_1'X_7 + a_2'X_8 + a_3'X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L'))(H')$ gelten. Wir verwenden die Notation $\vec{a} = (a_1, a_2, a_3)^T$ und $\vec{a}' = (a_1', a_2', a_3')^T$.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator genau dann infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, wenn die folgenden Gleichungen gelten:

$$\vec{a}' \prec_s t\vec{a}.$$

4.3.3. Spektraler Ansatz zur infinitesimalen Simulation von Hamilton-Operatoren

In diesem Abschnitt beweisen wir eine ähnliche Bedingung wie in Korollar 4.21 basierend auf einer spektralen Bedingung für die Hamilton-Operatoren. Dabei basiert diese spektrale Bedingung auf Referenz [VC02b, S. 9–10]. Es ist interessant, die spektrale Bedingung mit der s-Majorisierungsbedingung zu vergleichen.

Wir verwenden die Notation zur Majorisierung aus Abschnitt 4.3.2 zur Charakterisierung des Spektrums der Hamilton-Operatoren. Wir bezeichnen den Vektor der Eigenwerte einer $k \times k$-dimensionalen hermiteschen Matrix A mit

$$\operatorname{spec}(A) = (\operatorname{spec}(A)_1, \ldots, \operatorname{spec}(A)_k)^T,$$

wobei die Eigenwerte mit der entsprechenden Vielfachheit vorkommen. Zusätzlich nehmen wir an, daß $\operatorname{spec}(A)_i \geq \operatorname{spec}(A)_j$ für $i < j$ und $1 \leq i, j \leq k$ gilt. Aufgrund eines Theorems von Uhlmann [Uhl71] steht die Majorisierung der Spektren zweier Matrizen in Verbindung mit der konvexen Kombination unitärer Orbits.

Faktum 4.22 (Uhlmann (siehe z. B. [Uhl71, Satz 3] oder [AU82, Thm. 2-2.]))**.** Für hermitesche Matrizen A und B ist die Bedingung $\operatorname{spec}(A) \prec \operatorname{spec}(B)$ äquivalent dazu, daß unitäre Matrizen U_i und Zahlen $q_i \geq 0$ mit $\sum_i q_i = 1$ existieren, so daß die Gleichung

$$A = \sum_i q_i U_i^{-1} B U_i$$

gilt.

Wir zitieren ein weiteres Faktum, das das Konzept der Majorisierung mit der konvexen Hülle von permutierten Versionen eines Vektors verbindet.

Faktum 4.23 (Rado (siehe z. B. [Rad52] oder [MO79, Prop. 4.C.1.]))**.** Ein Vektor x wird von einem Vektor y genau dann majorisiert, wenn x in der konvexen Hülle aller Permutationen (der Komponenten) von y liegt.

Die spektrale Version von Theorem 4.18 lautet:

Theorem 4.24 ([VC02b, S. 9–10])**.** Seien H und H' nicht-lokale Hamilton-Operatoren, die auf einem Zwei-Qubit-System operieren. Ferner seien a und a' Elemente aus $\mathfrak{a}$, wobei für geeignet gewählte lokale unitäre Transformationen L und L' die Gleichungen $a = a_1 X_7 + a_2 X_8 + a_3 X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L))(H)$ und $a' = a'_1 X_7 + a'_2 X_8 + a'_3 X_9 = (\mathrm{Ad}_{\mathfrak{g}}(L'))(H')$ gelten.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert einen Hamilton-Operator genau dann infinitesimal in der Zeit $0 \leq t \in \mathbb{R}$, wenn

$$\operatorname{spec}(a') \prec t \operatorname{spec}(a).$$

Bemerkung. Die Notwendigkeit der Bedingung wurde in [WJB02] bewiesen. Im Beweis folgen wir [VC02b].

Beweis. Aufgrund von Faktum 4.7 können wir die Elemente a und a' wie angegeben wählen. Die Notwendigkeit folgt aus Faktum 4.22. Wir beweisen nun, daß die Bedingung hinreichend ist. Mit Faktum 4.23 erhalten wir

$$\mathrm{spec}(a'/t) = \sum_k q_k P_k \mathrm{spec}(a),$$

wobei P_k eine Permutation, $q_k \geq 0$, und $\sum_k q_k = 1$ ist. Da a und a' Elemente aus $\mathfrak{a}$ sind, kommutieren sie. Es folgt, daß eine Basis existiert, so daß die Elemente a und a' gemeinsam diagonal sind. In dieser Basis entsprechen die Permutationen P_k Permutationen der Diagonalemente von a. Deshalb gilt

$$(a'/t) = \sum_k q_k U_k^{-1} a U_k$$

für geeignet gewählte unitäre Transformationen U_k, die das Spektrum von a permutieren. Wir betonen, daß die Transformationen U_k nicht notwendigerweise lokal sind. Aber wir beweisen nun, daß sich alle Permutationen des Spektrums von a durch lokale unitäre Transformationen durchführen lassen. Durch Konjugation mit den lokalen unitären Transformationen $((\sigma_0 - i\sigma_1)/\sqrt{2}) \otimes ((\sigma_0 - i\sigma_1)/\sqrt{2})$, $((\sigma_0 + i\sigma_3)/\sqrt{2}) \otimes ((\sigma_0 + i\sigma_3)/\sqrt{2})$ bzw. $((\sigma_0 + i\sigma_1)/\sqrt{2}) \otimes ((\sigma_0 - i\sigma_1)/\sqrt{2})$ werden die Eigenwerte auf folgende Weise permutiert: $(1,2,3,4) \mapsto (2,1,3,4)$, $(1,2,3,4) \mapsto (1,3,2,4)$ bzw. $(1,2,3,4) \mapsto (1,2,4,3)$. Da sich alle Permutationen auf vierelementigen Vektoren aus diesen Permutationen erzeugen lassen, folgt, daß die Bedingung hinreichend ist. □

Wir merken an, daß die lokalen unitären Transformationen zur Permutation des Spektrums von Elementen aus $\mathfrak{a}$ in [VC02b] angegeben wurden. Dabei wurde die zweite Transformation falsch angegeben.

4.4. Simulation von unitären Transformationen auf Zwei-Qubit-Systemen

Ausgehend von Definition 4.1 betrachten wir nun die Simulation von unitären Transformationen. Diese Simulation betrachten wir als eine globale Version der infinitesimalen Simulation von Hamilton-Operatoren. Wir geben ein Theorem von Khaneja et al. [KBG01] an. Wir verweisen auch auf die Referenzen [YK05; Swo06].

Faktum 4.25 ([KBG01, Thm. 10])**.** Sei H ein nicht-lokaler Hamilton-Operator, der auf einem Zwei-Qubit-System operiert.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U genau dann in der Zeit $0 \leq t \in \mathbb{R}$, wenn die unitäre Transformation U wie folgt zerlegt werden kann

$$U = L_1 \exp(tW) L_2, \tag{4.14}$$

wobei L_1 und L_2 lokale unitäre Transformationen sind und W ein Element aus der konvexen Hülle des Weyl-Orbits $\mathcal{W}(H)$ von H ist.

Bemerkung. Gleichung (4.14) entspricht der Gleichung

$$L_1^{-1} U L_2^{-1} = \exp(tW). \tag{4.15}$$

Dies bedeutet, daß die unitäre Transformation U genau dann in der Zeit t simuliert werden kann, wenn es eine unitäre Transformation U' gibt, die lokal äquivalent zu U ist und die als $U' = \exp(tW)$ dargestellt werden kann. Aber die Wahl der Elemente L_1 und L_2 unterliegt gewissen Einschränkungen. Da $\exp(tW)$ ein Element von $\mathrm{A} = \exp(\mathfrak{a})$ ist, erhalten wir, daß auch $L_1^{-1} U L_2^{-1}$ ein Element von A seien muß. Es gibt verschiedene unitäre Transformationen U', die die Bedingungen erfüllen. Das Auftreten verschiedener unitärer Transformationen U' ist eine Konsequenz der Nicht-Eindeutigkeit der K A K-Zerlegung aus Faktum 4.6. Diese Nicht-Eindeutigkeit wird im folgenden untersucht. Wir betonen, daß die unitäre Transformation U möglicherweise nicht als $U = \exp(tW)$ bezüglich der gleichen (oder kürzeren) Zeit t aus Gleichung (4.15) dargestellt werden kann.

Wir präsentieren nun die Ergebnisse zur Simulation unitärer Transformationen auf eine vergleichbare Weise wie die infinitesimale Simulation von Hamilton-Operatoren in Abschnitt 4.3.2. Aufgrund der Bemerkung nach Faktum 4.25 können wir eine lokale unitäre Transformation U genau dann in der Zeit t simulieren, wenn eine lokale unitäre Transformation U', die lokal äquivalent zu U ist, als $U' = \exp(tW)$ bezüglich eines Elements W des Weyl-Orbits des System-Hamilton-Operators dargestellt werden kann. Wir bezeichnen im folgenden mit K_i für $i \in \{1, \ldots, 8\}$ geeignet gewählte Elemente der lokal unitären Transformationen $\mathrm{K} = \exp(\mathfrak{k})$. Zusätzlich seien A und A' passende Elemente aus $\mathrm{A} = \exp(\mathfrak{a})$. Nach Faktum 4.6 können wir eine unitäre Transformation U bzw. eine lokal äquivalente Transformation U' auf folgende Weise zerlegen: $U = K_1 A K_2$ bzw. $U' = K_3 A' K_4$. Um alle unitären Transformationen U' zu charakterisieren, die lokal äquivalent zu U sind, müssen wir alle Elemente A' charakterisieren, für die $K_5 A' K_6 = A$ gilt. Das heißt, wir bestimmen alle Elemente A' mit $A' = (K_7^{-1} A K_7) K_8$. Das folgende Lemma löst diese Aufgabe.

Lemma 4.26. Für ein festes Element $A \in \mathrm{A}$ und ein beliebiges Element der Form $A' = (K^{-1} A K) K' \in \mathrm{A}$ mit $K, K' \in \mathrm{K}$ können wir das Element K aus der Weyl-Gruppe und das Element K' aus der Menge $\mathrm{K} \cap \mathrm{A}$ wählen.

Entsprechend zu θ aus der Definition 4.5 der orthogonalen symmetrischen Lie-Algebra $(\mathfrak{g}, \theta)$, existiert eine globale Version Θ, die auf der Lie-Gruppe G operiert (siehe z. B. [Loo69a, Thm. 2.3 in Kap. IV] oder [Kna02, Thm. 6.31.]). Wir definieren Θ als $\Theta(K'') = K''$ für $K'' \in \mathrm{K}$ und $\Theta(P) = P^{-1}$ für $P \in \mathrm{P} = \exp(\mathfrak{p})$. Wir verwenden die Abbildung $()^\star$: $G \mapsto G^\star := \Theta(G^{-1})$ mit der Signatur $\mathrm{G} \to \mathrm{G}$. Das Symbol $()^\star$ wird hier verwendet, damit keine Verwechslung mit dem Symbol $()^*$ für die komplexe Konjugation möglich ist. Wir erhalten $(G_1 G_2)^\star = G_2^\star G_1^\star$ für $G_1, G_2 \in \mathrm{G}$, $P^\star = P$ für $P \in \mathrm{P}$ und $(K'')^\star = (K'')^{-1}$ für $K'' \in \mathrm{K}$ (siehe [Bor98, S. 81]). Die Abbildung ϕ: $\mathrm{G/K} \to \mathrm{P}$ wird als die Abbildung $GK \mapsto \phi(GK) := (GK)(GK)^\star = GG^\star$ definiert. Diese Abbildung wurde in [Bor98, S. 81-82] und in [Kna02, Beweis von Thm. 6.31.] untersucht. Referenz [Bor98] beweist, daß ϕ einen Isomorphismus von G/K auf P induziert.

Beweis von Lemma 4.26. Wir verwenden die Abbildung ϕ und erhalten die Gleichungen $\phi((K^{-1} A K) K') = K^{-1} A^2 K$ und $\phi(A') = (A')^2$. Da $A' = (K^{-1} A K) K'$ als Bedingung

in Lemma 4.26 angegeben wurde, folgt $K^{-1}A^2K = (A')^2$. Aufgrund von Faktum 4.12 können wir K als ein Element der Weyl-Gruppe wählen. Deshalb ist $K^{-1}AK \in \mathrm{A}$ und wir haben $K' \in \mathrm{K} \cap \mathrm{A}$ bewiesen. □

Wir charakterisieren nun die Elemente aus $\mathrm{K} \cap \mathrm{A}$.

Lemma 4.27. Die Menge K∩A besteht aus den Elementen $\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9)$, wobei $z_j \in \mathbb{Z}$ ($j \in \{1,2,3\}$), und die Symbole X_7, X_8, X_9 wurden auf Seite 44 definiert .

Beweis. Zuerst zeigen wir, daß die Elemente $\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9)$ eine Teilmenge von $\mathrm{K} \cap \mathrm{A}$ bilden. Da $\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9)$ für $z_j \in \mathbb{Z}$ Elemente von A sind und A eine abelsche Gruppe ist, erhalten wir, daß

$$\begin{aligned} &\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9) \\ =&\exp(z_1\pi X_7)\exp(z_2\pi X_8)\exp(z_3\pi X_9) \\ =&(i\sigma_1 \otimes \sigma_1)^{z_1}(i\sigma_2 \otimes \sigma_2)^{z_2}(i\sigma_3 \otimes \sigma_3)^{z_3}. \end{aligned}$$

Dies beweist, daß die Elemente $\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9)$ eine Teilmenge von $\mathrm{K} \cap \mathrm{A}$ bilden. Nun zeigen wir, daß $\mathrm{K} \cap \mathrm{A}$ eine Teilmenge von der Menge der Elemente $\exp(z_1\pi X_7 + z_2\pi X_8 + z_3\pi X_9)$ ist. Wir machen den Ansatz $\exp(a_7X_7 + a_8X_8 + a_9X_9) = \exp(a_1X_1 + a_2X_2 + a_3X_3 + a_4X_4 + a_5X_5 + a_6X_6)$, wobei $a_i \in \mathbb{R}$ und $i \in \{1,\ldots,9\}$. Wir erhalten für a_7, a_8 und a_9 die Bedingungen

$$\begin{aligned} &(a_7 - a_8 - a_9)/\pi \in \mathbb{Z}, (a_7 + a_8 - a_9)/\pi \in \mathbb{Z}, \\ &(a_7 + a_8 + a_9)/\pi \in \mathbb{Z}, (a_7 - a_8 + a_9)/\pi \in \mathbb{Z}. \end{aligned}$$

Damit folgt, daß $a_i/\pi \in \mathbb{Z}$ für $i \in \{7,8,9\}$. □

Nach dieser Vorarbeit geben wir eine zu Faktum 4.25 äquivalente Bedingung an, die die Form einer Majorisierung hat.

Korollar 4.28 (siehe [VHC02, Lemma] oder [HVC02, Result 1])**.** Sei H ein nicht-lokaler Hamilton-Operator, der auf einem Zwei-Qubit-System operiert. Wir wollen eine unitäre Transformation U simulieren. Seien a und a' Elemente aus $\mathfrak{a}$, wobei $a = a_1X_7 + a_2X_8 + a_3X_9 = (\mathrm{Ad}_{\mathfrak{g}}(K_1))(H)$, $a' = a'_1X_7 + a'_2X_8 + a'_3X_9$, und für geeignet gewählte lokale unitäre Transformationen $K_1, K_2, K_3 \in \mathrm{K}$ gilt $U = K_2\exp(a')K_3$. Wir verwenden die Notation $\vec{a} = (a_1,a_2,a_3)^T$ und $\vec{a}' = (a'_1,a'_2,a'_3)^T$.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U genau dann in der Zeit $0 \leq t \in \mathbb{R}$, wenn die folgende Gleichung mindestens für eine Wahl von $\vec{z} = (z_1,z_2,z_3)^T \in \mathbb{Z}^3$ erfüllt ist:

$$\vec{a}' + \pi\vec{z} \prec_s t\vec{a}.$$

Beweis. Nach Faktum 4.7 bzw. Faktum 4.6 können wir a bzw. a' wie angegeben wählen. Aufgrund der Faktum 4.25 folgenden Bemerkung ist es notwendig und hinreichend, alle unitäre Transformationen U' zu betrachten, die lokal äquivalent zu U sind. Mit Faktum 4.6 können wir die lokal äquivalenten Transformationen U' als eine Zerlegung $U' = K'_1A'K'_2$ darstellen, wobei $A' \in \mathrm{A}$ und K'_1, K'_2 lokale unitäre Transformationen

sind. Die verschiedenen Möglichkeiten für A' in dieser Zerlegung sind nach Lemma 4.26 durch $A' = \exp\left[(\mathrm{Ad}_{\mathfrak{g}}(K))(a')\right] K'$ gegeben, wobei K ein Element der Weyl-Gruppe ist, $K' \in \mathrm{K} \cap \mathrm{A}$, und $K' = \exp(k')$. Mit der Charakterisierung von $\mathrm{K} \cap \mathrm{A}$ nach Lemma 4.27 erhalten wir, daß $\mathrm{K} \cap \mathrm{A}$ links invariant unter der Operation der Weyl-Gruppe ist. Da A abelsch ist und $\mathrm{K} \cap \mathrm{A}$ links invariant unter der Operation der Weyl-Gruppe ist, können wir A' als $A' = \exp\left[(\mathrm{Ad}_{\mathfrak{g}}(K))(a') + k'\right] = \exp\left[(\mathrm{Ad}_{\mathfrak{g}}(K))(a' + k'')\right]$ angegeben, wobei für ein geeignet gewähltes Element $K'' \in \mathrm{K} \cap \mathrm{A}$ die Gleichung $K'' = \exp(k'')$ erfüllt ist. Mit Faktum 4.25 folgt, daß $A' = \exp\left[(\mathrm{Ad}_{\mathfrak{g}}(K))(a' + k'')\right] = \exp(tW)$. Dabei liegt W in der konvexen Hülle des Weyl-Orbits $\mathcal{W}(a)$ von a. Wenn wir die Gleichung $\exp\left[(\mathrm{Ad}_{\mathfrak{g}}(K))(a' + k'')\right] = \exp(tW)$ in einer Basis betrachten, in der $(\mathrm{Ad}_{\mathfrak{g}}(K))(a' + k'')$ und tW gleichzeitig diagonal sind, erhalten wir mit der Periodizität der Exponentialfunktion, daß $(\mathrm{Ad}_{\mathfrak{g}}(K))(a'+k'')+M = tW$, wobei $M = \mathrm{diag}(2\pi i\lambda_1, 2\pi i\lambda_2, 2\pi i\lambda_3, 2\pi i\lambda_4)$ und $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in \mathbb{Z}$. Da $(\mathrm{Ad}_{\mathfrak{g}}(K))(a' + k'')$ und tW Elemente von $\mathfrak{a}$ sind, folgt $M \in \mathfrak{a}$. Wir können M als $M = 2\pi z_1 X_7 + 2\pi z_2 X_8 + 2\pi z_3 X_9 = 2k_1$ mit $z_1 = (\lambda_1 + \lambda_2) \in \mathbb{Z}$, $z_2 = (\lambda_1+\lambda_3) \in \mathbb{Z}$, $z_3 = (\lambda_2+\lambda_3) \in \mathbb{Z}$, $K_1 = \exp(k_1)$ und $K_1 \in \mathrm{K}\cap\mathrm{A}$ darstellen. Deshalb erhalten wir $(\mathrm{Ad}_{\mathfrak{g}}(K))(a'+k'')+2k_1 = (\mathrm{Ad}_{\mathfrak{g}}(K))(a'+k''+2k_2) = (\mathrm{Ad}_{\mathfrak{g}}(K))(a'+k_3) = tW$, wobei $K_i = \exp(k_i)$, $K_i \in \mathrm{K} \cap \mathrm{A}$ und $i \in \{1, 2, 3\}$. Mit Korollar 4.21 können wir den Beweis beenden. □

Um Korollar 4.28 zu verbessern, geben wir Schranken für die Koeffizienten a_1, a_2 und a_3 eines Elementes $a_1X_7 + a_2X_8 + a_3X_9 \in \mathfrak{a}$ an. Unter Benutzung von Lemma 4.26 und Lemma 4.27 erhalten wir, daß die Koeffizienten a_i ($i \in \{1, 2, 3\}$) periodisch mit Periode π sind. (Diese Periodizität wurde auch in [KC01, Appendix B] und in [ZVSW03, S. 7] untersucht.) Aufgrund der π-Periodizität können wir die Koeffizienten a_i auf das Intervall $[-\frac{\pi}{2}, \frac{\pi}{2}]$ beschränken. Diese Wahl ist kompatibel mit den Konventionen aus Abschnitt 4.2.3. Wir schränken die Elemente auf Elemente der abgeschlossenen fundamentalen Weyl-Kammer ein, um die Symmetrie der Weyl-Gruppe zu brechen. Mit Gleichung (4.10) oder mit der s-Ordnung von Abschnitt 4.3.2 erhalten wir, daß $a_1 \geq 0$, $a_2 \geq 0$, $a_1 \geq a_2$ und $a_2 \geq a_3$. Diese Überlegungen führen zu folgendem Korollar:

Korollar 4.29 (siehe [VHC02, Thm. 1] oder [HVC02, Result 2])**.** Sei H ein nicht-lokaler Hamilton-Operator, der auf einem Zwei-Qubit-System operiert. Wir wollen eine unitäre Transformation U simulieren. Seien a und a' Elemente aus $\mathfrak{a}$, wobei $a = a_1X_7 + a_2X_8 + a_3X_9 = (\mathrm{Ad}_{\mathfrak{g}}(K_1))(H)$, $a' = a'_1X_7 + a'_2X_8 + a'_3X_9$, und für geeignet gewählte lokale unitäre Transformationen $K_1, K_2, K_3 \in \mathrm{K}$ gilt $U = K_2 \exp(a')K_3$. Wir verwenden die Notation $\vec{a} = (a_1, a_2, a_3)^T$ und $\vec{a}' = (a'_1, a'_2, a'_3)^T$. Zusätzlich wählen wir die Elemente a_1, a_2, a_3, a'_1, a'_2 und a'_3 so, daß sie in dem Intervall $[-\frac{\pi}{2}, \frac{\pi}{2}]$ liegen.

Ein Zwei-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokale unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U genau dann in der Zeit $0 \leq t \in \mathbb{R}$, wenn die folgende Gleichung mindestens für eine Wahl von $\vec{z} = (z_1, z_2, z_3)^T \in \{(0, 0, 0)^T, (-1, 0, 0)^T\}$ erfüllt ist:

$$\vec{a}' + \pi\vec{z} \prec_s t\vec{a}.$$

Bemerkung. Im Beweis folgen wir den Referenzen [VHC02; HVC02].

Beweis. Aufgrund von Korollar 4.28 ist es hinreichend, die folgende Gleichung für alle $\vec{z} \in \mathbb{Z}^3$ zu zeigen:

$$\vec{a}' + \pi(0,0,0)^T \prec_s \vec{a}' + \pi\vec{z}, \quad \vec{a}' + \pi(-1,0,0)^T \prec_s \vec{a}' + \pi\vec{z}.$$

Zuerst betrachten wir den Fall, daß $|z_i| > 1$ für ein $i \in \{1,2,3\}$. Da $a'_i \leq \pi/2$, ist die maximale Komponente $(\vec{a}' + \pi\vec{z})^{\downarrow_s}_1$ der s-geordneten Version von $\vec{a}' + \pi\vec{z}$ größer gleich $2\pi - \pi/2 = 3\pi/2$. Wir überprüfen die Bedingungen von Definition 4.20 und erhalten $\vec{a}' + \pi(0,0,0)^T \prec_s \vec{a}' + \pi\vec{z}$.

Als zweites betrachten wir den Fall, daß $|z_i| \leq 1$ für alle $i \in \{1,2,3\}$. Mit einfachen, aber aufwendigen Berechnungen kann überprüft werden, daß $\vec{a}' + \pi(0,0,0)^T \prec_s \vec{a}' + \pi\vec{z}$ für

$$\vec{z} \in \{(-1,-1,0)^T, (-1,0,-1)^T, (0,-1,-1)^T, (0,-1,1)^T, (0,0,0)^T, (-1,0,1)^T\}$$

und daß $\vec{a}' + \pi(-1,0,0)^T \prec_s \vec{a}' + \pi\vec{z}$ für

$$\vec{z} \in \{(-1,-1,-1)^T, (-1,-1,1)^T, (-1,0,0)^T, (0,-1,0)^T, (0,0,-1)^T, (0,0,1)^T\}$$

gilt. In allen anderen Fällen erhalten wir für $\vec{z} \in \{-1,0,1\}^3$, daß sowohl $\vec{a}' + \pi(0,0,0)^T \prec_s \vec{a}' + \pi\vec{z}$ als auch $\vec{a}' + \pi(-1,0,0)^T \prec_s \vec{a}' + \pi\vec{z}$ erfüllt ist. □

4.5. Untere Schranken für die Zeitkomplexität in n-Qubit-Systemen

In Zwei-Qubit-Systemen benutzten wir eine spezielle Zerlegung $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ der Lie-Algebra, die zu einer Zerlegung $\mathrm{G} = \mathrm{K}\,\mathrm{A}\,\mathrm{K}$ der Lie-Gruppe führt, wobei $\mathrm{K} = \exp(\mathfrak{k})$ die Menge der lokal unitären Transformationen ist. Mit diesem Ansatz kann auch die optimale Simulation von Faktum 4.25 bewiesen werden. Im allgemeinen n-Qubit-Fall können wir eine Zerlegung $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ der entsprechenden Lie-Algebra verwenden, wobei $\mathrm{K} = \exp(\mathfrak{k})$ alle lokal unitären Transformationen enthält. Obwohl K im allgemeinem nicht gleich der Menge der lokal unitären Transformationen ist, können wir trotzdem unseren Ansatz aus dem Zwei-Qubit-Fall verallgemeinern, um untere Schranken für die Zeitkomplexität zu beweisen. Untere Schranken wurden in Referenz [CHN03] betrachtet, und wir verfeinern und verallgemeinern nun den Ansatz von [CHN03]. Insbesondere betrachten wir den Ansatz von [CHN03] in einem erweiterten Kontext.

4.5.1. Magische Basis (für Zwei-Qubit-Systeme)

Wir beginnen, indem wir uns die Bell-Basis sowie die magische Basis ins Gedächtnis rufen. Die Bell-Basis (siehe [BMR92; BBC$^+$93]) ist eine Vektorraumbasis für reine Zwei-Qubit-Zustände:

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \quad |\Phi^-\rangle := \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right),$$
$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \quad |\Psi^-\rangle := \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right).$$

Wenn wir spezielle skalare Faktoren in die Bell-Basis einfügen, erhalten wir die magische Basis, die in Referenz [BDSW96] eingeführt wurde und von Hill und Wootters [HW97] ihren Namen hat:

$$|e_1\rangle := |\Phi^+\rangle, \quad |e_2\rangle := i|\Phi^-\rangle, \quad |e_3\rangle := i|\Psi^+\rangle, \quad |e_4\rangle := |\Psi^-\rangle.$$

Die magische Basis steht in enger Verbindung zur minimalen Ensembleverschränkung (engl. entanglement of formation) (siehe Referenz [BDSW96] und auch die verwandten Arbeiten in den Referenzen [BBPS96; PR97]). Wir vernachlässigen hier diese Verbindung, verweisen aber auf Abschnitt 4.7.

Die magische Basis hat zwei wichtige Eigenschaften. Erstens sind lokal unitäre Transformationen in der magischen Basis reell und orthogonal (siehe [HW97, S. 5023] und [Mak03, Thm. 1]). Zweitens sind die Elemente von $\mathrm{A} = \exp(\mathfrak{a})$ (für die Notation, siehe z. B. Abschnitt 4.2.3) diagonal in der magischen Basis (vgl. [KC01, S. 3] oder [HVC02, S. 2]). Der Basiswechsel von der Standardbasis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ in die magische Basis ist durch Q^{-1} gegeben, wobei

$$Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & i \\ 0 & i & 1 & 0 \\ 0 & i & -1 & 0 \\ 1 & 0 & 0 & -i \end{pmatrix}.$$

Für Elemente $U \in \mathrm{SU}(4)$ beschreibt die Abbildung $U \mapsto Q^{-1}UQ$ (siehe [Mak03]) den Isomorphismus zwischen $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$ und $\mathrm{SO}(4)$, siehe z. B. [Gil94, S. 52].

4.5.2. Darstellungstheorie

Es ist nicht offensichtlich, wie sich die magische Basis auf eine höhere Anzahl von Qubits verallgemeinert und welche Eigenschaften erhalten bleiben. Ausgehend von den Eigenschaften der magischen Basis für Zwei-Qubit-Systeme suchen wir Basiswechsel von den lokal unitären Transformationen $(\mathrm{SU}(2))^{\otimes n}$ in die orthogonale Gruppe, falls dies möglich ist. Für die Suche verwenden wir Darstellungstheorie.

Definition 4.30 (Darstellungen von Lie-Gruppen (siehe z. B. [DK00, S. 210]))**.** Eine komplexe Darstellung einer Lie-Gruppe G in einem endlichdimensionalen und komplexen Vektorraum $\mathrm{V}_{\mathbb{C}}$ ist ein kontinuierlicher Homomorphismus $\tau\colon \mathrm{G} \to \mathrm{GL}(\mathrm{V}_{\mathbb{C}})$ von der Gruppe G auf die Gruppe $\mathrm{GL}(\mathrm{V}_{\mathbb{C}})$ der invertierbaren und linearen Transformationen, die auf $\mathrm{V}_{\mathbb{C}}$ operieren.

Eine Darstellung τ in einem endlichdimensionalen und komplexen Vektorraum $\mathrm{V}_{\mathbb{C}}$ wird als irreduzibel bezeichnet, falls kein Unterraum $\mathrm{U}_{\mathbb{C}}$ mit $\mathrm{U}_{\mathbb{C}} \neq 0$ und $\mathrm{U}_{\mathbb{C}} \neq \mathrm{V}_{\mathbb{C}}$ existiert, so daß der Unterraum $\tau(\mathrm{G})$-invariant ist, d. h., die Gleichung $\tau(\mathrm{G})\mathrm{U}_{\mathbb{C}} \subset \mathrm{U}_{\mathbb{C}}$ gilt (siehe z. B. [DK00, S. 210]). Wir benötigen ein wichtiges Ergebnis über Tensorpodukte irreduzibler Darstellungen.

Faktum 4.31 ([BD85, Prop. 4.14 in Kap. II])**.** Ist τ_1 eine irreduzible komplexe Darstellung von G_1 in dem komplexen Vektorraum $\mathrm{V}_{\mathbb{C}}$ und τ_2 eine irreduzible komplexe Darstellung von G_2 in dem komplexen Vektorraum W, so ist $\tau_1 \otimes \tau_2$ eine irreduzible komplexe Darstellung von $\mathrm{G}_1 \times \mathrm{G}_2$ in dem komplexen Vektorraum $\mathrm{V}_{\mathbb{C}} \otimes \mathrm{W}_{\mathbb{C}}$. Ferner sind alle irreduziblen Darstellungen von $\mathrm{G}_1 \times \mathrm{G}_2$ ein Tensorprodukt dieser Form.

Im weiteren verwenden wir bilineare Formen $\mathcal{B}$: $\mathrm{V}_{\mathbb{C}} \times \mathrm{V}_{\mathbb{C}} \to \mathbb{C}$, die $\mathbb{C}$-linear in beiden Argumenten sind, um irreduzible komplexe Darstellungen zu charakterisieren. Seien v_1 und v_2 beliebige Vektoren aus $\mathrm{V}_{\mathbb{C}}$. Eine bilineare Form wird als symmetrisch bezeichnet, falls $\mathcal{B}(v_1, v_2) = \mathcal{B}(v_2, v_1)$, und als schiefsymmetrisch, falls $\mathcal{B}(v_1, v_2) = -\mathcal{B}(v_2, v_1)$ gilt. Eine bilineare Form ist $\tau(\mathrm{G})$-invariant, falls $\mathcal{B}(v_1, v_2) = \mathcal{B}(\tau(G)v_1, \tau(G)v_2)$ für alle $G \in \mathrm{G}$ gilt.

Definition 4.32 (vgl. [BD85; DK00])**.** Sei τ eine irreduzible komplexe Darstellung von G in dem Vektorraum $\mathrm{V}_{\mathbb{C}}$. Die Darstellung τ wird als

- reell bezeichnet, falls $\mathrm{V}_{\mathbb{C}}$ eine bilineare Form zuläßt, die nicht verschwindet, nicht entartet, $\tau(\mathrm{G})$-invariant und symmetrisch ist,
- komplex bezeichnet, falls $\mathrm{V}_{\mathbb{C}}$ keine bilineare Form zuläßt, die nicht verschwindet, nicht entartet und $\tau(\mathrm{G})$-invariant ist,
- quaternionisch bezeichnet, falls $\mathrm{V}_{\mathbb{C}}$ eine bilineare Form zuläßt, die nicht verschwindet, nicht entartet, $\tau(\mathrm{G})$-invariant und schiefsymmetrisch ist.

Wir führen die Abbildung χ_τ: $\mathrm{G} \to \mathbb{C}, G \mapsto \mathrm{Tr}(\tau(G))$ ein, wobei χ_τ den Charakter der Darstellung τ bezeichnet. Wir verwenden den Charakter, um eine irreduzible komplexe Darstellung als reell, komplex oder quaternionisch zu charakterisieren.

Faktum 4.33 ([DK00, Thm. 4.8.1])**.** Bezeichne τ eine irreduzible komplexe Darstellung von G in dem Vektorraum $\mathrm{V}_{\mathbb{C}}$. Der Charakter χ_τ ist genau dann reell-wertig, wenn eine komplexe bilineare Form $\mathcal{B}$ auf $\mathrm{V}_{\mathbb{C}}$ existiert, die nicht verschwindet und $\tau(\mathrm{G})$-invariant ist. Diese bilineare Form ist automatisch nicht entartet und bis auf einen nicht verschwindenden skalaren Faktor eindeutig bestimmt. Insbesondere gilt, daß die bilineare Form $\mathcal{B}$ entweder symmetrisch oder schiefsymmetrisch ist.

Mit Hilfe von Faktum 4.33 können wir nun entscheiden, ob eine Darstellung komplex ist. Um die Klassifikation (reell, komplex oder quaternionisch) der irreduziblen komplexen Darstellungen zu vervollständigen, geben wir ein weiteres Faktum an, welches uns ermöglicht, den Typ einer Darstellung anzugeben. Dafür muß nur ein normalisiertes Integral auf einer kompakten Lie-Gruppe G berechnet werden.

Faktum 4.34 (siehe [DK00, Prop. 4.8.7] und [BD85, Prop. 6.8 in Kap. II])**.** Sei τ eine irreduzible komplexe Darstellung einer kompakten Lie-Gruppe G in dem Vektorraum $\mathrm{V}_{\mathbb{C}}$ mit dem Charakter χ_τ. Wir erhalten

$$\int \chi_\tau(G^2) d\mathrm{G} = \begin{cases} 1 & \Leftrightarrow \ \tau \text{ ist reell,} \\ 0 & \Leftrightarrow \ \tau \text{ ist komplex,} \\ -1 & \Leftrightarrow \ \tau \text{ ist quaternionisch.} \end{cases}$$

Darstellungen können mit Untergruppen der Gruppe $\mathrm{GL}(\mathrm{V}_{\mathbb{C}})$ identifiziert werden, so können wir Definition 4.32 auf Untergruppen von $\mathrm{GL}(\mathrm{V}_{\mathbb{C}})$ erweitern. Wir bezeichnen die allgemeine lineare Gruppe auf einem komplexen Vektorraum der Dimension k mit $\mathrm{GL}(k, \mathbb{C})$. Nun können wir die Untergruppen von $\mathrm{GL}(k, \mathbb{C})$ charakterisieren, die konjugiert zu Untergruppen der orthogonalen Gruppe (wie aufgrund von Abschnitt 4.5.1 motiviert) oder der symplektischen Gruppe sind.

Faktum 4.35 (angepaßt von [Sam99, Thm. H in Kap. 3])**.** Eine kompakte Untergruppe der allgemeinen linearen Gruppe $\mathrm{GL}(k, \mathbb{C})$ ist genau dann zu einer Untergruppe der orthogonalen Gruppe konjugiert, wenn sie reell ist. Entsprechend ist eine kompakte Untergruppe der $\mathrm{GL}(2k, \mathbb{C})$ genau dann zu einer Untergruppe der (unitären) symplektischen Gruppe konjugiert, wenn sie quaternionisch ist.

Bemerkung. Tatsächlich gibt Referenz [Sam99] einen Algorithmus zur Berechnung des Basiswechsels für die bilineare Form aus Definition 4.32 an. Für die Notation $\mathrm{Sp}(k)$ verweisen wir auf Abschnitt 4.5.4 und Referenz [Che99].

Nach dieser Vorbereitung betrachten wir nun die lokal unitären Transformationen $(\mathrm{SU}(2))^{\otimes n}$. Wir verwenden die Standarddarstellung der $\mathrm{SU}(2)$:

$$G = \begin{pmatrix} a + i \cdot b & c + i \cdot d \\ -c + i \cdot d & a - i \cdot b \end{pmatrix},$$

wobei $a, b, c, d \in \mathbb{R}$ und $a^2 + b^2 + c^2 + d^2 = 1$. Um das Integral aus Faktum 4.34 zu berechnen, führen wir die reellen Parameter $0 \leq \phi < 2\pi$, $0 \leq \psi_1 \leq \pi$ und $0 \leq \psi_2 \leq \pi$ wie folgt ein:

$$\begin{aligned} a &= \cos(\phi)\sin(\psi_1)\sin(\psi_2), \\ b &= \sin(\phi)\sin(\psi_1)\sin(\psi_2), \\ c &= \cos(\psi_1)\sin(\psi_2), \\ d &= \cos(\psi_2). \end{aligned}$$

Wir erhalten

$$\begin{aligned} \int \chi_\tau(G^2) d(\mathrm{SU}(2))^{\otimes n} &= \left(\int \chi_\tau(G^2) d\mathrm{SU}(2) \right)^n \\ = \left(\int_0^{2\pi} \int_0^{\pi} \int_0^{\pi} \Xi(\phi, \psi_1, \psi_2) d\psi_2 d\psi_1 d\phi \right)^n &= (-1)^n, \end{aligned}$$

wobei

$$\begin{aligned} \Xi(\phi, \psi_1, \psi_2) = [4\cos(\phi)^2 (1 - \cos(\psi_1)^2 - \cos(\psi_2)^2 \\ + \cos(\psi_1)^2 \cos(\psi_2)^2) - 2] \sin(\psi_1)\sin(\psi_2)^2. \end{aligned}$$

Womit das folgende Theorem bewiesen ist.

Theorem 4.36. Die lokal unitären Transformationen auf einer geraden Anzahl von Qubits sind konjugiert zu einer Untergruppe der orthogonalen Gruppe. Die lokal unitären Transformationen auf einer ungeraden Anzahl von Qubits sind konjugiert zu einer Untergruppe der (unitär) symplektischen Gruppe.

Bemerkung. Ähnliche Ergebnisse wurden mit anderen Methoden in Referenz [BB04] gezeigt. Theorem 4.36 kann auch unter Zuhilfenahme von [BDNB04, Thm. 5] bewiesen werden.

4.5.3. Thompsons Theorem und die Majorisierung

Wir folgen Referenz [CHN03] und präsentieren ein Theorem von Thompson [Tho86] und eine Bedingung für die Majorisierung des Spektrums einer Summe von zwei hermiteschen Matrizen. Beide Ergebnisse werden im folgenden verwendet.

Faktum 4.37 ([Tho86])**.** Seien A und B hermitesche Matrizen. Dann existieren unitäre Matrizen U_1 und U_2, so daß

$$\exp(iA)\exp(iB) = \exp(iU_1^{-1}AU_1 + iU_2^{-1}BU_2).$$

Dieses Ergebnisses basiert teilweise auf einer Vermutung von Horn [Hor62]. Diese Vermutung wurde kürzlich bewiesen (vgl. [Lid82; DST98; Kly98; KT99; Knu00; Ful00]). Per Induktion erhalten wir das folgende Korollar.

Korollar 4.38. Seien A_j hermitesche Matrizen. Dann existieren unitäre Matrizen U_j, so daß

$$\prod_{j=1}^{m} \exp(iA_j) = \exp\left(i\sum_{j=1}^{m} U_j^{-1}A_jU_j\right).$$

Wir geben nun Schranken für das Spektrum einer Summe von zwei hermiteschen Matrizen an. Referenz [MO79] schreibt dieses Ergebnis Ky Fan [Fan49] zu. Wir bezeichnen den Vektor der Eigenwerte einer $k \times k$-dimensionalen hermiteschen Matrix A (einschließlich der Vielfachheiten) mit $\mathrm{spec}(A) = (\mathrm{spec}(A)_1, \ldots, \mathrm{spec}(A)_k)^T$. Zusätzlich nehmen wir an, daß $\mathrm{spec}(A)_i \geq \mathrm{spec}(A)_j$ falls $i < j$ $(1 \leq i, j \leq k)$.

Faktum 4.39 ([MO79, Thm. 9.G.1.])**.** Seien A und B hermitesche Matrizen. Dann erhalten wir die folgenden Gleichungen:

$$\mathrm{spec}(A+B) \prec \mathrm{spec}(A) + \mathrm{spec}(B).$$

4.5.4. Untere Schranken

In diesem Abschnitt leiten wir untere Schranken für die minimale Zeit zur Simulation unitärer Transformationen her (siehe Definition 4.1). Wir beginnen mit einer Diskussion der (unitär) symplektischen Gruppe. Wir folgen Referenz [Che99, S. 22] und führen die bilineare Form

$$\mathcal{B}_{\mathrm{Sp}}(\vec{x}, \vec{y}) := \sum_{j=1}^{k}(x_iy_{i+k} - x_{i+k}y_i) \tag{4.16}$$

ein. Dabei gilt $\vec{x} = (x_1, \ldots, x_{2k})^T \in \mathbb{C}^{2k}$ und $\vec{y} = (y_1, \ldots, y_{2k})^T \in \mathbb{C}^{2k}$. Es bezeichne J_k die Matrix

$$J_k = \begin{pmatrix} 0_k & I_k \\ -I_k & 0_k \end{pmatrix},$$

wobei I_k die $k \times k$-dimensionale Identitätsmatrix und 0_k die $k \times k$-dimensionale Nullmatrix ist.

Definition 4.40 (siehe z. B. [Che99, Prop. 1 auf S. 22])**.** Die Untergruppe der unitären Gruppe U($2k$) der Dimension $2k$, die aus Matrizen M besteht, die die bilineare Form aus Gleichung (4.16) invariant läßt, d. h., die die Gleichung

$$M^T J_k M = J_k \tag{4.17}$$

erfüllt, wird als (unitär) symplektische Gruppe Sp(k) bezeichnet.

Die Gruppe Sp(k) operiert auch auf einem k-dimensionalen Modul über den Quaternionen $\mathbb{H}$ und läßt das symplektische (Skalar-)Produkt invariant [Che99, S. 16–24]. Alle Elemente aus Sp(k) haben Determinante eins, siehe z. B. [Che99, S. 203]. Wenn wir Sp(k) als Mannigfaltigkeit auffassen, ist ihre reelle Dimension gleich $2k^2 + k$ [Che99, S. 23].

Nach Theorem 4.36 sind lokal unitäre Transformationen auf einer ungeraden Anzahl von Qubits konjugiert zu einer Untergruppe der (unitären) symplektischen Gruppe. Wir benutzen die Gleichung $(J_k)^{-1} = -J_k$ und zeigen, daß die Bedingung in Gleichung (4.17) äquivalent zu

$$M^{-1} = J_k M^T (J_k)^{-1} \tag{4.18}$$

ist. Wir wissen, daß die lokalen unitären Transformationen auf einer ungeraden Anzahl von Qubits die Bedingung aus Gleichung (4.18) in einer geeignet gewählten Basis erfüllen. Aber wir können diese Bedingung auch in der Standarddarstellung der $\mathrm{SU}(2)^{\otimes n}$ (n ungerade) angeben. Wir verwenden die Identifikation $2k = 2^n$. Bezeichne J'_n die Matrix

$$J'_n := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\otimes n} = (i\sigma_y)^{\otimes n}$$

und sei

$$G = \begin{pmatrix} a + ib & c + id \\ -c + id & a - ib \end{pmatrix},$$

mit $a, b, c, d \in \mathbb{R}$ die Standarddarstellung der SU(2). Wir benutzen die Abkürzung

$$G_j = \begin{pmatrix} a_j + ib_j & c_j + id_j \\ -c_j + id_j & a_j - ib_j \end{pmatrix},$$

wobei $a_j, b_j, c_j, d_j \in \mathbb{R}$. Es gilt

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} G^T \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1} = G^{-1}$$

und wir erhalten, daß

$$J'_n \left(\bigotimes_{j=1}^{n} G_j \right)^T (J'_n)^{-1} = \left(\bigotimes_{j=1}^{n} G_j \right)^{-1}. \tag{4.19}$$

Dabei gilt Gleichung (4.19) offensichtlich für ungerades und für gerades n. Deshalb schränken wir n nicht länger darauf ein, ungerade zu sein. Es gilt $(J'_n)^{-1} = (J'_n)^T = (-1)^n J'_n$ und wir erhalten

$$\left(\bigotimes_{j=1}^{n} G_j \right)^T J'_n \left(\bigotimes_{j=1}^{n} G_j \right) = J'_n. \tag{4.20}$$

Sei $\mathcal{H}$ ein 2^n-dimensionaler komplexer Vektorraum, auf dem die Gruppe $\mathrm{SU}(2^n)$ operiert. Wir führen die bilineare Form $\mathcal{B}_{\mathcal{H}}(x,y) := x^T J'_n y$ auf dem Hilbertraum $\mathcal{H}$ ein. Es gilt

$$\mathcal{B}_{\mathcal{H}}(y,x) = y^T J'_n x = (-1)^n x^T J'_n y = (-1)^n \mathcal{B}_{\mathcal{H}}(x,y).$$

Damit wurde bewiesen, daß $\mathcal{B}_{\mathcal{H}}(x,y)$ symmetrisch ist, falls n gerade ist, und schiefsymmetrisch ist, falls n ungerade ist. Aus Gleichung (4.20) folgt, daß $\mathcal{B}_{\mathcal{H}}(x,y)$ links invariant unter der Operation von $\mathrm{SU}(2)^{\otimes n}$ ist. Folglich haben wir die bilineare Form $\mathcal{B}_{\mathcal{H}}(x,y)$ als die bilineare Form aus Definition 4.32 identifiziert, wobei $\mathrm{V}_{\mathbb{C}} = \mathcal{H}$ ist.

Dies motiviert die folgende Definition der Tilde-Abbildung. Dabei bildet die Tilde-Abbildung lokal unitäre Transformationen auf deren Inverses ab.

Definition 4.41. Wir führen die Tilde-Abbildung Ψ ein:

$$\Psi : \begin{cases} \mathrm{SU}(2^n) \to \mathrm{SU}(2^n) \\ U \mapsto \tilde{U} := \Psi(U) = J'_n U^T (J'_n)^{-1} \end{cases}$$

Es ist ausgehend von $[J'_n U^T (J'_n)^{-1}][J'_n U^T (J'_n)^{-1}]^\dagger = I_{2^n}$ und $\det[(J'_n)^{-1} U^T J'_n] = \det(U)$ offensichtlich, daß die Tilde-Abbildung die Gruppe $\mathrm{SU}(2^n)$ in sich selbst abbildet.

Bemerkung. Die Tilde-Abbildung ist eine Verallgemeinerung der Abbildung

$$U \mapsto (\sigma_y)^{\otimes n} U^T (\sigma_y)^{\otimes n}$$

aus Referenz [CHN03, S. 5] für gerades n. Die beiden Abbildungen stimmen für gerades n überein. Wir verweisen auch auf die Diskussion in Abschnitt 4.7.

Wir geben nun ein wichtiges Lemma zur Charakterisierung der Tilde-Abbildung an.

Lemma 4.42. Bezeichnen V und W lokal unitäre Transformationen und bezeichne U eine beliebige unitäre Transformation. Die folgenden Gleichung gelten:

1. $\tilde{V} = V^{-1}$,
2. $\tilde{W} = W^{-1}$,
3. $VUW\Psi(VUW) = VU\tilde{U}V^{-1}$.

Beweis. Die erste und zweite Behauptung folgen aus Gleichung (4.19). Wir beweisen nun die dritte Behauptung: $VUW\Psi(VUW) = VUW\tilde{W}\tilde{U}\tilde{V} = VUWW^{-1}\tilde{U}V^{-1} = VU\tilde{U}V^{-1}$. □

Dies beweist, daß lokal unitäre Transformationen das Spektrum von $U\tilde{U}$ invariant lassen. Wir geben nun untere Schranken für die Simulationszeit unitärer Transformationen an. Wir verwenden die Notation arg, wobei $\arg[\exp(im)] = m$ und $\arg\left[(x_1,\ldots,x_l)^T\right] = (\arg[x_1],\ldots,\arg[x_l])^T$.

Theorem 4.43. Sei H ein nicht-lokaler Hamilton-Operator, der auf einem n-Qubit-System operiert. Wir wollen eine unitäre Transformation U simulieren.

Ein n-Qubit-System mit Hamilton-Operator H und der Möglichkeit, lokal unitäre Transformationen auszuführen, simuliert eine unitäre Transformation U nur dann in der Zeit $0 \leq t \in \mathbb{R}$, wenn die folgende Gleichung mindestens für eine Wahl von $\vec{z} \in \mathbb{Z}^{2^n}$ gilt:

$$\arg\left[\operatorname{spec}(U\tilde{U})\right] + 2\pi\vec{z} \prec 2t \operatorname{spec}(H)$$

Bemerkung. Dieses Theorem verallgemeinert Ergebnisse aus Referenz [CHN03, Thm. 5 und Cor. 7]. Im Beweis benutzen wir Ideen aus [CHN03].

Beweis. Wir nehmen an, daß $U = [\prod_{j=1}^{m} W_j \exp(it_j H)]W_0$ eine Simulation von U ist. Dabei bezeichnet W_j lokal unitäre Transformationen, $t_j \geq 0$ und $\sum_{j=1}^{m} t_j = t$. Seien

$$V_j = \begin{cases} W_m & \text{für } j = m, \\ V_{j+1} W_j & \text{für } 0 \leq j < m. \end{cases}$$

und $H_j = V_j H V_j^{-1}$ $(1 \leq j \leq m)$. Wir erhalten, daß die Simulation von U in der Form $U = [\prod_{j=1}^{m} \exp(it_j H_j)]V_0$ dargestellt werden kann, wobei $\operatorname{spec}(H_j) = \operatorname{spec}(H)$ für alle $1 \leq j \leq m$.

Wir verwenden Korollar 4.38, um geeignete Hamilton-Operatoren H'_j und H''_j mit $\operatorname{spec}(H'_j) = \operatorname{spec}(H''_j) = \operatorname{spec}(H)$ und $j \in \{1, \ldots, m\}$ anzugeben, so daß

$$\left[\prod_{j=1}^{m} \exp(it_j H_j)\right] \Psi\left(\prod_{j=1}^{m} \exp(it_j H_j)\right) = \exp\left[\sum_{j=1}^{m} it_j (H'_j + H''_j)\right]. \tag{4.21}$$

Aus der Gleichung $\tilde{V_0} = V_0^{-1}$ und der Gleichung (4.21) folgt

$$\operatorname{spec}(U\tilde{U}) = \operatorname{spec}\left\{\exp\left[i \sum_{j=1}^{m} t_j (H'_j + H''_j)\right]\right\}.$$

Faktum 4.39 vervollständigt den Beweis:

$$\arg\left[\operatorname{spec}(U\tilde{U})\right] + 2\pi\vec{z} = \operatorname{spec}\left[\sum_{j=1}^{m} t_j (H'_j + H''_j)\right] \prec 2t \operatorname{spec}(H).$$

□

4.5.5. Involutive Automorphismen

Wir heben nun eine Verbindung zwischen der Tilde-Abbildung aus Definition 4.41 und involutiven Automorphismen der Lie-Algebra $\mathfrak{su}(2^n)$ hervor.

Die Tilde-Abbildung ist ähnlich zur $()^\star$-Abbildung, die in dem Beweis von Lemma 4.26 in Abschnitt 4.4 verwendet wurde. Für n ungerade, ist K äquivalent zu $\mathrm{Sp}(2^{n-1})$, und für n gerade, ist K äquivalent zu $\mathrm{SO}(2^n)$. In beiden Fällen spielt die Abbildung $U \mapsto U\tilde{U}$ eine vergleichbare Rolle wie die Abbildung ϕ aus Abschnitt 4.4.

Basierend auf [Hel01, S. 451–452] geben wir alle symmetrische Räume $\mathrm{SU}(2^n)/K$ und die zugehörigen involutiven Automorphismen der Lie-Algebra $\mathfrak{su}(2^n)$ an. Wir müssen drei Fälle (AI, AII, und AIII) unterscheiden. Im Fall AI betrachten wir die Lie-Algebra $\mathfrak{g} = \mathfrak{su}(k)$ und den involutiven Automorphismus $\theta_{\mathrm{AI}}(g) = g^*$ und wir erhalten den Riemannschen symmetrischen Raum $\mathrm{SU}(k)/\mathrm{SO}(k)$.

Die Lie-Algebra $\mathfrak{g} = \mathfrak{su}(2k)$ und der involutive Automorphismus $\theta_{\mathrm{AII}}(g) = J_k g^*(J_k)^{-1}$ gehören zum Typ AII. Dieser Typ entspricht dem Riemannschen symmetrischen Raum $\mathrm{SU}(2k)/\mathrm{Sp}(k)$.

Obwohl wir den Typ AIII nicht verwenden, geben wir ihn der Vollständigkeit halber trotzdem an: Die Lie-Algebra ist $\mathfrak{g} = \mathfrak{su}(p+q)$, und der entsprechende involutive Automorphismus ist $\theta_{\mathrm{AII}}(g) = I_{p,q} g I_{p,q}$. Wir verwenden die Notation

$$I_{p,q} = \begin{pmatrix} -I_p & 0_{p,q} \\ 0_{q,p} & I_q \end{pmatrix},$$

wobei I_p die $p \times p$-dimensionale Identitätsmatrix und $0_{p,q}$ die $p \times q$-dimensionale Nullmatrix bezeichnet. Damit erhalten wir den Riemannschen symmetrischen Raum $\mathrm{SU}(p+q)/\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$. Die Gruppe $\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$ ist durch die Menge der Matrizen

$$\begin{pmatrix} g_1 & 0_{p,q} \\ 0_{q,p} & g_2 \end{pmatrix}$$

gegeben, wobei $g_1 \in \mathrm{U}(p)$, $g_2 \in \mathrm{U}(q)$ und $\det(g_1)\det(g_2) = 1$.

4.6. Verwandte Arbeiten

Wir dokumentieren nun Verbindungen zu den vielfältigen anderen Arbeiten. Verschiedene Aspekte der infinitesimalen Simulation von Hamilton-Operatoren (vgl. Abschnitt 4.3) wurden in den folgenden Referenzen untersucht: [VLK99; JK99; LCYY00; DVC+01; SM01; DNBT02; WJB02; JWB02; BCL+02; Leu02; VC02b; VC02a; WRJB02b; MVL02; NBD+02; WRJB02a; Woc03; Che03; CLV04; HNO03; Röt04; RW06; Woc06]. Einige Referenzen betrachten Modelle, die im Gegensatz zu unserem Modell zusätzliche Ressourcen erlauben: vorhandene Verschränkung [VC02a], zusätzliche klassische Kommunikation [VC02b], Messungen auf den Quantensysteme [BCL+02] oder Hilfssysteme [BCL+02; VC02b].

Für Zwei-Qubit-Systeme wurde die Simulation von unitären Transformationen (siehe Abschnitt 4.4) in den Referenzen [Kha00; D'A00; KBG01; VHC02; HVC02; BDD+02; ZVSW03; HNO03; YK05; MCB05; ZW05; DHH+06; Swo06] analysiert. In [KG01] wurden Lie-Gruppen-Zerlegungen für eine Theorie der Simulation von unitären Transformationen auf n-Qubit-Systemen verwendet. Im allgemeinem führen diese Zerlegungen nicht zu optimalen Simulationen. Im Fall von Drei-Qubit-Systemen gab es Fortschritte bei der Simulation von unitären Transformationen. Wir verweisen auf Referenz [KGB02]. Bezüglich unterer Schranken haben wir den Ansatz von Referenz [CHN03] verallgemeinert (siehe Abschnitt 4.5). Numerische Optimierungsmethoden wurden in [SHSKG05] verwendet, um effiziente Simulationen von unitären Transformationen zu finden.

Verbindungen zwischen der Zeitkomplexität von Simulationen im Sinne dieses Kapitels und der Komplexität von Quantenschaltkeisen (siehe Abschnitt 1.2) wurden in den Arbeiten [JB01; WJB02; Nie06; NDGD06b; NDGD06a] diskutiert.

4.7. Diskussion einer Verbindung zur Beschreibung der Verschränkung

In diesem Abschnitt diskutieren wir eine Verbindung zwischen dem Ansatz zu den unteren Schranken für die Zeitkomplexität der Simulation unitärer Transformationen und der Concurrence (engl. concurrence) [HW97; Woo98a; Woo98b; Woo01] sowie deren Verallgemeinerungen [CKW00; Uhl00; WC01; AF01; RBC+01; AVD01; BDH+02; JTFS+03; FMI03; LBŻW03; TFJ03; Ger03; VDD03; JSST03; BB04]. Die Concurrence C eines reinen Zwei-Qubit-Zustandes $|\psi\rangle \in \mathbb{C}^4$ wurde in Referenz [Woo98a] durch die Gleichung

$$C(|\psi\rangle) = |\langle\psi|\tilde{\psi}\rangle|$$

definiert, wobei $|\tilde{\psi}\rangle := (\sigma_y \otimes \sigma_y)(|\psi\rangle)^*$. Dabei bezeichnet $\langle\psi_1|\psi_2\rangle$ das Skalarprodukt zweier Vektoren $|\psi_1\rangle$ und $|\psi_2\rangle$ eines komplexen Hilbertraumes $\mathrm{V}_{\mathbb{C}}$. Für einen linearen Operator ρ auf $\mathrm{V}_{\mathbb{C}}$ definieren wir die (hermitesche) Adjungierte $\rho^\dagger$ mit Hilfe der Bedingung, daß $\langle\psi_1|\rho^\dagger\psi_2\rangle = \langle\psi_2|\rho\psi_1\rangle$ für alle $|\psi_1\rangle, |\psi_2\rangle \in \mathrm{V}_{\mathbb{C}}$ gilt (vgl. [Gaa73, S. 91]). Ein linearer Operator ρ auf $\mathrm{V}_{\mathbb{C}}$ gilt als positiv, falls er hermitesch ist, d. h. $\rho = \rho^\dagger$, und das Skalarprodukt $\langle\psi|\rho\psi\rangle$ der Vektoren $|\psi\rangle$ und $\rho|\psi\rangle$ für jeden Vektor $|\psi\rangle$ größer gleich null ist (vgl. [Gaa73, S. 129]). Ein Dichteoperator (oder eine Dichtematrix) ist ein positiver (linearer) Operator ρ, dessen Spur gleich eins ist ($\mathrm{Tr}\rho = 1$). Wir verweisen bzgl. dieser Definition auf [Mes61, S. 334]. Insbesondere bezeichnet $\rho_\psi = |\psi\rangle\langle\psi|$ den Dichteoperator, der dem Zustand $|\psi\rangle$ zugeordnet ist. Für jede Menge von Zuständen ψ_i und Wahrscheinlichkeiten p_i mit $0 \leq p_i \leq 1$ und $\sum_i p_i = 1$ ist $\sum_i p_i \rho_{\psi_i}$ ein Dichteoperator (siehe z. B. [Mes61, S. 331–332]).

Es bezeichnen λ_1, λ_2, λ_3 und λ_4 die (positiven) Quadratwurzeln der Eigenwerte der Matrix $\rho\tilde{\rho}$, wobei $\tilde{\rho} := (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$. Wir nehmen an, daß $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \lambda_4$. Die Referenzen [HW97; Woo98a] zeigen, daß die Concurrence C einer Zwei-Qubit-Dichtematrix ρ durch die folgende Gleichung gegeben ist:

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}. \tag{4.22}$$

Uhlmann [Uhl00] betrachtete Verallgemeinerungen der Concurrence. Wir folgen seiner Vorgehensweise und führen einige Notationen ein. Wir bezeichnen eine Abbildung ϑ auf einem komplexen Vektorraum $\mathrm{V}_{\mathbb{C}}$ als antilinear, falls die Gleichung $\vartheta(b_1|\psi_1\rangle + b_2|\psi_2\rangle) = (b_1)^*\vartheta(|\psi_1\rangle) + (b_2)^*\vartheta(|\psi_2\rangle)$ für alle $b_1, b_2 \in \mathbb{C}$ und alle $|\psi_1\rangle, |\psi_2\rangle \in \mathrm{V}_{\mathbb{C}}$ gilt. Für einen antilinearen Operator ϑ definieren wir die (hermitesche) Adjungierte $\vartheta^\dagger$ mit Hilfe der Bedingung, daß $\langle\psi_1|\vartheta^\dagger\psi_2\rangle = \langle\psi_2|\vartheta\psi_1\rangle$ für alle $|\psi_1\rangle, |\psi_2\rangle \in \mathrm{V}_{\mathbb{C}}$ gilt. Falls ein antilinearer Operator ϑ die Bedingung $\vartheta^\dagger = \vartheta^{-1}$ erfüllt, nennen wir ihn antiunitär. Ist die Abbildung ϑ antiunitär und gilt die Bedingung $\vartheta^{-1} = \vartheta$, dann erhalten wir, daß ϑ^2 identisch zur Identitätsabbildung ist, und wir nennen ϑ eine Konjugation. Eine Schief-Konjugation ist ein antiunitärer Operator ϑ, der die Bedingung $\vartheta^{-1} = -\vartheta$ erfüllt. Wir nehmen im folgenden an, daß ϑ eine Konjugation ist. Nun definierte Uhlmann eine verallgemeinerte Tilde-Abbildung mit Hilfe ihrer Operation auf reinen Zuständen $|\tilde{\psi}\rangle := \vartheta(|\psi\rangle)$ und ihrer Operation auf Dichtematrizen $\tilde{\rho} := \vartheta\rho\vartheta^{-1} = \vartheta\rho\vartheta$. Zusätzlich verallgemeinerte er das Konzept der Concurrence auf mehr als Zwei-Qubit-Systeme für reine Zustände

$$C_\vartheta(|\psi\rangle) := |\langle\psi|\tilde{\psi}\rangle|$$

und für gemischte Zustände

$$C_\vartheta(\rho) := \min \sum_j |\langle \phi_j | \tilde{\phi}_j \rangle|,$$

wobei das Minimum über alle Zerlegungen $\rho = \sum_j |\phi_j\rangle\langle\phi_j|$ von ρ in nicht normalisierte reine Zustände $|\phi_j\rangle$ betrachtet wird. Uhlmann [Uhl00] zeigte dies in Analogie zu Gleichung (4.22). Die verallgemeinerte Concurrence ist nun durch die Gleichung

$$C_\vartheta(\rho) = \max \left\{ 0, \lambda_1 - \sum_{j>1} \lambda_j \right\}$$

gegeben, wobei λ_i Quadratwurzeln von Eigenwerten der Matrix $\rho\tilde{\rho}$ bezeichnen und $\lambda_i \geq \lambda_j$ für $i < j$ gilt.

Die Referenzen [JTFS+03; TFJ03; JSST03] betrachten die Abbildung auf Dichtematrizen:

$$\rho \mapsto \tilde{\rho} := (\sigma_y)^{\otimes n} \rho^* (\sigma_y)^{\otimes n}. \tag{4.23}$$

Entsprechend wurde die Abbildung

$$iH \mapsto \widetilde{iH} := (-i\sigma_y)^{\otimes n} (iH)^* \left((-i\sigma_y)^{\otimes n} \right)^{-1} \tag{4.24}$$

in Referenz [BB04] für Elemente iH der Lie-Algebra $\mathfrak{su}(2^n)$ eingeführt. Die Abbildung aus Gleichung (4.24) kann auf Hamilton-Operatoren H angewendet werden:

$$\tilde{H} = (-i\sigma_y)^{\otimes n} (H)^* \left((-i\sigma_y)^{\otimes n} \right)^{-1} = (\sigma_y)^{\otimes n} (H)^* (\sigma_y)^{\otimes n}.$$

Dies beweist, daß sowohl die Gleichung (4.23) als auch die Gleichung (4.24) durch die Konjugation ϑ_1 mit

$$\vartheta_1(|\psi\rangle) = \sigma_y^{\otimes n} (|\psi\rangle)^*$$

induziert wird. In diesem Fall erhalten wir die Concurrence C_{ϑ_1}. Die zugehörige Tilde-Abbildung ist durch ihre Operation auf reinen Zuständen $|\tilde{\psi}\rangle = \vartheta_1 |\psi\rangle$ und ihrer Operation auf Dichtematrizen $\tilde{\rho} = \vartheta_1 \rho {\vartheta_1}^{-1} = \vartheta_1 \rho \vartheta_1$ definiert. Ein Ergebnis aus Referenz [VW00, Prop. 8] (siehe auch [RBC+01]) bezeichnet die Konjugation ϑ_1 als den (bis auf die Phase) eindeutigen Operator, der auf dem komplexen Vektorraum $(\mathbb{C}^2)^{\otimes n}$ operiert und der invariant unter einem Basiswechsel durch lokal unitäre Transformationen U ist, wobei ein Faktor, der gleich der Determinante $\det(U)$ ist, unberücksichtigt bleibt. Weiterhin gibt die Referenz [VW00] an, daß eine antilineare Abbildung nur für n-Qubit-Systeme existiert und nicht für allgemeine Systeme, die nicht aus Qubits bestehen.

Nach dieser Exkursion in die Theorie der Concurrence-artigen Verschränkungsmaße geben wir nun eine Verbindung zwischen diesen Verschränkungsmaßen und unteren Schranken für die Zeitkomplexität der Simulation unitärer Transformationen an. Die Tilde-Abbildung aus Definition 4.41 kann nun im Kontext von Concurrence-artigen Verschränkungsmaßen betrachtet werden. Da $H^T = H^*$ für alle hermitesche Operatoren gilt, folgt

$$\Psi(U) = J'_n (\exp(iH))^T (J'_n)^{-1} = \exp(i J'_n H^* (J'_n)^{-1}),$$

wobei $iJ'_n H^*(J'_n)^{-1}$ bis auf ein Minuszeichen äquivalent zu der rechten Seite von Gleichung (4.24) ist. Wir betonen, daß, wenn wir die unteren Schranken aus Abschnitt 4.5 betrachten, wir eigentlich in der Situation von Referenz [Uhl00] mit $\vartheta = \vartheta_1$ sind.

Sowohl für die unteren Schranken für die Zeitkomplexität zur Simulation von unitären Operatoren als auch für die Berechnung der Concurrence ist der wesentliche Punkt, daß das Spektrum von $U\tilde{U}$ und $\rho\tilde{\rho}$ invariant unter lokal unitären Transformationen ist. Dies hebt die Verbindung zwischen Verschränkungsmaßen und unteren Schranken für die Zeitkomplexität zur Simulation von unitären Operatoren hervor.

5. Nicht-lokale Struktur unitärer Transformationen

5.1. Einführung

In Kapitel 4 wurde die Simulation unitärer Transformationen behandelt. Dabei basiert ein wesentlicher Teil der Ergebnisse auf der kanonischen Zerlegung $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ (vgl. die Bemerkung nach der Def. 4.5). Die kanonische Zerlegung entspricht dabei einem symmetrischen Raum (vgl. Abschnitt 4.5.5). Die Struktur der symmetrischen Räume ermöglichte im Zwei-Qubit-Fall eine zeitoptimale Simulation von unitären Transformationen (vgl. Abschnitt 4.4) und im allgemeinem n-Qubit-Fall ($n > 2$) immer noch die Bestimmung unterer Schranken für die Zeitkomplexität bei der Simulation unitärer Transformationen (vgl. Abschnitt 4.5). Für $\mathrm{G} = \mathrm{SU}(2^n)$ und $\mathrm{H} = \mathrm{SU}(2)^{\otimes n}$ ($n > 2$) ist G/H kein symmetrischer Raum. Wir erhalten die Struktur eines homogenen Raumes:

Definition 5.1 (Homogener Raum (siehe z. B. [Arv03, Kapitel 4]))**.** Sei G eine Lie-Gruppe und H eine Lie-Untergruppe von G. Der homogene Raum G/H ist die Menge der (Links-)Nebenklassen $\mathrm{G/H} = \{G\mathrm{H} \colon G \in \mathrm{G}\}$.

Die Lie-Gruppe G operiert per (Links-)Multiplikation transitiv auf G/H ([Bou74, Kap. I, §5.5, Prop. 5]), d. h., für je zwei Elemente $x, y \in \mathrm{G/H}$ existiert ein Element $G \in \mathrm{G}$ mit $x = G \cdot y$. Ein homogener Raum ist insbesondere eine analytische Mannigfaltigkeit im Sinne von Definition A.1 (siehe [Bou89b, Kap. III, §1.6, Prop. 11]). Falls G eine kompakte Lie-Gruppe ist (z. B. $\mathrm{G} = \mathrm{SU}(2^n)$) und H eine Lie-Untergruppe von G ist (z. B. $\mathrm{H} = \mathrm{SU}(2)^{\otimes n}$), so ist der homogene Raum G/H reduktiv (vgl. [Arv03, S. 71]), und wir erhalten die Vektorraum-Zerlegung $\mathfrak{g} = \mathfrak{h} + \mathfrak{m}$ der Lie-Algebra $\mathfrak{g}$ von G mit den Eigenschaften $[\mathfrak{h}, \mathfrak{h}] \subset \mathfrak{h}$ und $[\mathfrak{h}, \mathfrak{m}] \subset \mathfrak{m}$. Hierbei bezeichnet $\mathfrak{h}$ die Lie-Algebra von H. Es ist dabei wichtig, daß z. B. für $\mathrm{G} = \mathrm{SU}(2^n)$ und $\mathrm{H} = \mathrm{SU}(2)^{\otimes n}$ ($n > 2$) die Eigenschaft $[\mathfrak{m}, \mathfrak{m}] \subset \mathfrak{h}$ aus der Definition der kanonischen Zerlegung (vgl. die Bemerkung nach der Def. 4.5) nicht gilt.

Die Lie-Untergruppe $\mathrm{H} = \mathrm{SU}(2)^{\otimes n}$ der Lie-Gruppe $\mathrm{G} = \mathrm{SU}(2^n)$ wurde in Kapitel 4 als lokal unitäre Transformationen bezeichnet. Diese Definition dient uns in diesem Kapitel als motivierendes Beispiel für den allgemeinen Fall:

Definition 5.2 (Lokal unitäre Transformationen)**.** Wir bezeichnen als lokal unitäre Transformationen eine beliebige, aber festgelegte Lie-Untergruppe H der Lie-Gruppe $\mathrm{G} = \mathrm{SU}(d)$.

Ein wichtiger Spezialfall ergibt sich, falls der komplexe Hilbertraum $\mathcal{H} = \mathbb{C}^d$ eine Tensorproduktstruktur $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$ (siehe Def. 1.5) bzgl. der Quantensysteme $\mathcal{H}_i$ besitzt. Dann können wir die lokal unitären Transformationen z. B. als die Lie-Gruppe $\mathrm{H} = \mathrm{SU}(\dim(\mathcal{H}_1)) \otimes \ldots \otimes \mathrm{SU}(\dim(\mathcal{H}_n))$ wählen.

Ausgehend von der Wahl der lokal unitären Transformationen können wir den homogenen Raum G/H als den Raum der Äquivalenzklassen der nicht-lokalen unitären Transformationen wählen. Diese Definition ist vergleichbar mit dem Ansatz aus Referenz [DC02].

Das Thema dieses Kapitels ist die Analyse der nicht-lokalen Struktur der unitären Transformationen. Wir verwenden Methoden der Topologie und der Differentialgeometrie um die nicht-lokalen Transformationen zu charakterisieren. Hierbei nimmt die Entwicklung von Methoden zur Analyse der nicht-lokalen Struktur einen großen Raum ein. Dies dient als Grundstein für eine anschließende Anwendung der Analysemethoden, die im Rahmen dieser Arbeit teilweise nur exemplarisch erfolgt.

5.2. Differentialformen und der de-Rham-Komplex

In diesem Abschnitt geben wir eine kurze Einführung in die Analysis auf Mannigfaltigkeiten, wobei wir uns am Ende auf reelle Mannigfaltigkeiten einschränken. Für eine ausführlichere Darstellung verweisen wir auf die Referenzen [Bou71b; Bou71a; Jän01; GHV72; Spi99a; Nak90; KN91; AI95; MT97; Fra04].

Eine Mannigfaltigkeit M besitzt an jedem Punkt x einen Tangentialraum $\mathrm{T}_x(M)$ (vgl. Definition A.3). Wir bezeichnen den Tangentialraum $\mathrm{T}(M)$ der Mannigfaltigkeit M als die Menge der Tangentialräume $\mathrm{T}_x(M)$ aller Punkte $x \in M$ (siehe [Bou71a, S. 9, §8.1.1]). Sei U eine Teilmenge von M und seien $u^1, \ldots, u^n$ Abbildungen von U nach $\mathbb{K}$. Wir bezeichnen $u = (u^1, \ldots, u^n)$ als ein System von Koordinaten von M in U, falls $(U, u, \mathbb{K}^n)$ eine Karte von M ist (vgl. Abschnitt A.1 und [Bou71b, S. 37, §5.1.10]). Hierbei werden die Abbildungen $u^1, \ldots, u^n$ oft auch als Koordinatenfunktionen bezeichnent (siehe z. B. [Nak90, S. 133]). Sei im folgenden f eine Funktion von M nach $\mathbb{K}$ und $x \in U$ ein Punkt mit den Koordinaten $u(x) = (u^1(x), \ldots, u^n(x)) = (x^1, \ldots, x^n)$.

Die partielle Ableitung $\partial/\partial u^i$ ($i \in \{1, \ldots, n\}$) von einer Funktion f an einem Punkt $x \in U$ ist als die Ableitung der Funktion $g_i \colon \mathbb{K} \to \mathbb{K}$, $z \mapsto f(x^1, \ldots, x^{i-1}, z, x^{i+1}, \ldots, x^n)$ am Punkt x^i definiert, falls diese Ableitung existiert (vgl. z. B. [Bou71b, S. 15, §1.6]). Wenn ϕ eine glatte Abbildung von der Mannigfaltigkeit N in die Mannigfaltigkeit M ist, so definieren wir für $x \in N$ die Abbildung

$$\tilde{\phi} \colon\ (f, x) \mapsto (\tilde{\phi} f)(x) = (f \circ \phi)(x)$$

und für $v \in \mathrm{T}(N)$ entsprechend die Abbildung

$$\phi_* \colon\ v \mapsto \phi_* v = v \circ \tilde{\phi} \in \mathrm{T}(M). \tag{5.1}$$

In den Referenzen [GHV72, S. 88], [Spi99a, S. 80], [Nak90, S. 148] und [AI95, S. 8–9] kann eine ausführlichere Einführung der Abbildung ϕ_* gefunden werden.

Das Differential $\mathrm{d}f$ einer Funktion f ist eine Abbildung von $\mathrm{T}(M)$ nach $\mathbb{K}$. In U erhalten wir folgende Definition (vgl. [Jän01, S. 58]):

$$(\mathrm{d}f)(\partial/\partial u^i) = \partial f/\partial u^i. \tag{5.2}$$

Insbesondere gilt für die Koordinatenfunktionen u^i, daß

$$(\mathrm{d}u^i)(\partial/\partial u^j) = \partial u^i/\partial u^j = \delta^i_j = \begin{cases} 1 & \text{für } i = j, \\ 0 & \text{für } i \neq j. \end{cases}$$

Wir erhalten die folgende Darstellung des Differentials (vgl. [Jän01, S. 58], [Bou71b, S. 43–44, §5.5.8] und [Wal90, S. 81–83]):

$$\mathrm{d}f = \sum_{i=1}^{n} \frac{\partial f}{\partial u^i}\, \mathrm{d}u^i.$$

Dabei ist $\mathrm{grad} f = (\partial f/\partial u^1, \ldots, \partial f/\partial u^n)$ der Gradient von f ([Wal90, S. 82]). Nun können wir bzgl. der Karte $(U, u, \mathbb{K}^n)$ eine Basis $(\partial/\partial u^1, \ldots, \partial/\partial u^n)$ des Tangentialraumes $\mathrm{T}(M)$ von M (vgl. [Bou71b, S. 43, §5.5.8] und [Bou71a, S. 10, §8.1.5]) sowie eine Basis $(\mathrm{d}u^1, \ldots, \mathrm{d}u^n)$ des Dualraumes $\mathrm{T}^*(M)$ der Linearformen von $\mathrm{T}(M)$ nach $\mathbb{K}$ (vgl. [Bou71b, S. 43, §5.5.8]) angeben. Für die Definition des Dualraumes $\mathrm{T}^*(M)$ des Tangentialraumes $\mathrm{T}(M)$ verweisen wir auch auf Referenz [Bou71b, S. 42, §5.5.6 und S. 81, §7.7.3] und Referenz [Bou71a, S. 10, §8.2.2]. Wir merken an, daß

$$\mathrm{d}(f \cdot g) = (\mathrm{d}f) \cdot g + f(\mathrm{d}g) \tag{5.3}$$

gilt ([Bou71b, S. 43, §5.5.6]).

Eine Differentialform $\omega \in \Omega^p(M) = \mathrm{Alt}^p(\mathrm{T}(M), \mathbb{K})$ $(p \in \{1, \ldots, \dim(M)\})$ ist eine p-lineare, alternierende und glatte Abbildung von $\mathrm{T}(M)^{\times p} = \mathrm{T}(M) \times \cdots \times \mathrm{T}(M)$ nach $\mathbb{K}$ (vgl. [Bou71b, §7.8-9], [Bou71a, §8.3] und [Jän01, Kap. 3]). In Hinblick auf die Anwendungen schränken wir uns auf glatte, d. h. unendlich oft differenzierbare, Abbildungen ein (vgl. [Spi99a, S. 207], [Jän01, S. 2 und S. 55–57] und [Nak90, S. 160]). Eine Abbildung ω gilt als alternierend, falls $\omega(v_1, \ldots, v_p) = 0$ $(v_i \in \mathrm{T}(M),\ i \in \{1, \ldots, p\})$ unter der Vorraussetzung gilt, daß es zwei Indizes i, j mit $v_i = v_j$ gibt (vgl. [Bou74, Kap. 3, §4.9] und [Jän01, S. 49–50]). Im Fall von $p = 0$ definieren wir $\omega \in \Omega^0(M)$ als eine glatte Funktion von M nach $\mathbb{K}$ (vgl. [Jän01, S. 56]). Weiter gilt $\Omega^1(M) = \mathrm{T}^*(M)$. Sei ϕ eine glatte Abbildung von einer Mannigfaltigkeit N in eine Mannigfaltigkeit M, $\omega \in \Omega^p(M)$ und $v_1, \ldots, v_p \in \mathrm{T}(N)$. Wir führen die Abbildung $\phi^*\colon\ \omega \mapsto \phi^*\omega \in \Omega^p(N)$ ein (siehe Gleichung (5.1) und z. B. Referenz [Bou71a, S. 12, §8.3.1]):

$$(\phi^*\omega)(v_1, \ldots, v_p) = \omega(\phi_* v_1, \ldots, \phi_* v_p). \tag{5.4}$$

Wir definieren das äußere Produkt (vgl. [Bou74, Kap. 3, §7]) von $\omega \in \Omega^p(M)$ und $\omega' \in \Omega^q(M)$ (vgl. [Bou71b, S. 82–83, §7.8.2-3] und [Jän01, S. 133–134]):

$$(\omega \wedge \omega')(v_1, \ldots, v_{p+q}) = \sum_{\pi \in \mathcal{Z}_{p,q}} \varepsilon_\pi\ \omega(v_{\pi(1)}, \ldots, v_{\pi(p)})\ \omega'(v_{\pi(p+1)}, \ldots, v_{\pi(p+q)}),$$

wobei $v_i \in \mathrm{T}(M)$ $(i \in \{1, \ldots, p+q\})$, $\mathcal{Z}_{p,q} = \{\pi \in \mathcal{S}_{p+q} |\ \pi(1) < \ldots < \pi(p)$ und $\pi(p+1) < \ldots < \pi(p+q)\}$ eine Teilmenge der Permutationen $\mathcal{S}_{p+q}$ der Menge $\{1, \ldots, p+q\}$ (vgl. [Bou74, Kap. 1, §4.1, Bsp.]) und $\varepsilon_\pi = \prod_{i<j}(\pi(i) - \pi(j))/(i-j)$ das Signum der Permutation π ist (siehe z. B. [Bos96, S. 221]). Für $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ gilt (siehe z. B. [Jän01, S. 133–134]):

$$(\omega \wedge \omega')(v_1, \ldots, v_{p+q}) = \frac{1}{p!\cdot q!} \sum_{\pi \in \mathcal{S}_{p+q}} \varepsilon_\pi\ \omega(v_{\pi(1)}, \ldots, v_{\pi(p)})\ \omega'(v_{\pi(p+1)}, \ldots, v_{\pi(p+q)}).$$

Bezüglich einer Karte $(U, u, \mathbb{K}^n)$ erhalten wir nun für eine Differentialform die Darstellung (vgl. [Bou71a, S. 13, §8.3.3])

$$\omega = \sum_{i_1<\ldots<i_p} f_{i_1,\ldots,i_p} \quad \mathrm{d}u^{i_1} \wedge \ldots \wedge \mathrm{d}u^{i_p}, \tag{5.5}$$

wobei $f_{i_1,\ldots,i_p}$ Funktionen von U nach $\mathbb{K}$ und $i_j \in \{1, \ldots, n\}$ sind. Wir führen die Notation $\Omega(M) = \oplus_{p\geq 0}\Omega^p(M)$ ein und definieren auf $\Omega(M)$ die äußere Ableitung d von ω aus Gleichung (5.5) bzgl. einer Karte $(U, u, \mathbb{K}^n)$ von M durch die Formel (siehe z. B. [Bou71a, S. 13–14, §8.3.6] oder [Jän01, S. 139])

$$\mathrm{d}\omega = \sum_{i_1<\ldots<i_p} \mathrm{d}f_{i_1,\ldots,i_p} \wedge \mathrm{d}u^{i_1} \wedge \ldots \wedge \mathrm{d}u^{i_p}. \tag{5.6}$$

Wir schränken uns nun auf $\mathbb{K} = \mathbb{R}$, d. h., auf reelle Mannigfaltigkeiten ein.

Faktum 5.3 (Äußere Ableitung (siehe z. B. [Jän01, S. 138–139] oder [Spi99a, S. 212]))**.** Sei M eine reelle und endlichdimensionale Mannigfaltigkeit, so existiert genau eine Weise um eine Sequenz von linearen Abbildungen

$$0 \longrightarrow \Omega^0(M) \xrightarrow{\mathrm{d}} \Omega^1(M) \xrightarrow{\mathrm{d}} \Omega^2(M) \xrightarrow{\mathrm{d}} \cdots$$

einzuführen, so daß die folgenden drei Bedingung erfüllt sind:

1. Für $f \in \Omega^0(M)$ ist $\mathrm{d}f$ das Differential der Funktion f (siehe z. B. Gleichung (5.2)).
2. $\mathrm{d} \circ \mathrm{d} = 0$
3. Für $\omega \in \Omega^p(M)$ und $\omega' \in \Omega^q(M)$ gilt $\mathrm{d}(\omega \wedge \omega') = (\mathrm{d}\omega) \wedge \omega' + (-1)^p\, \omega \wedge (\mathrm{d}\omega')$.

Bemerkung. Ein Beweis der Eindeutgkeit kann auch in [Bou80, §2.10, Prop. 13] gefunden werden.

Faktum 5.3 definiert den de-Rham-Komplex ([Bou80, §2.10]), der ein Komplex im Sinne von [Bou80, §2] ist, d. h., $\mathrm{d} \circ \mathrm{d} = 0$ und d erhöht den Grad von z. B. $\Omega^p(M)$ nach $\Omega^{p+1}(M)$. Zusätzlich zeigt Faktum 5.3, daß die Definition aus Gleichung (5.6) eindeutig ist. Wir verwenden die Bezeichnungen $\mathrm{d}_p = \mathrm{d}|_{\Omega^p(M)}$ und definieren für eine lineare Abbildung $l\colon L_1 \to L_2$ den Kern $\mathrm{Ker}(l) = \{x \in L_1 |\ l(x) = 0\}$ und das Bild $\mathrm{Im}(l) = l(L_1)$.

Definition 5.4 (De-Rham-Kohomologie (siehe z. B. [Jän01, S. 195–196]))**.** Sei M eine reelle und endlichdimensionale Mannigfaltigkeit. Wir definieren die p-te de-Rham-Kohomologie-Gruppe

$$\mathrm{H}^p(\Omega(M), \mathrm{d}) = \frac{\mathrm{Ker}(\mathrm{d}_p)}{\mathrm{Im}(\mathrm{d}_{p-1})} = \frac{\mathrm{Ker}(\mathrm{d}|_{\Omega^p(M)})}{\mathrm{Im}(\mathrm{d}|_{\Omega^{p-1}(M)})}$$

und den de-Rham-Kohomologie-Ring

$$\mathrm{H}^*(\Omega(M), \mathrm{d}) = \bigoplus_{p=0}^{\infty} \mathrm{H}^p(\Omega(M), \mathrm{d}).$$

Bemerkung. Es wurde von Poincaré ([Poi95]) und E. Cartan ([Car28; Car29; Car37]) vermutet und von de Rham ([Rha29; Rha31]) bewiesen, daß die de-Rham-Kohomologie-Gruppen äquivalent zu gewissen topologischen Invarianten sind. Diese topologischen Invarianten werden heute durch das Konzept der singulären Homologie mit reellen Koeffizienten behandelt. Die Vektorraumdimensionen der de-Rham-Kohomologie-Gruppen werden oft als Bettischen Zahlen bezeichnet. Für eine Diskussion der singulären Homologie und ihrer Verbindung zu der de-Rham-Komologie verweisen wir auf die Referenzen [Nak90, Kap. 6] und [Fra04, Kap. 13].

5.3. Integralinvarianten und invariante Differentialformen

Sei M eine n-dimensionale (reelle) Mannigfaltigkeit und (B, ψ) ein orientiertes und parametrisiertes p-Gebiet, das durch eine Orientierung (siehe z. B. [Fra04, S. 83–84]) eines Gebietes $B \subset \mathbb{R}^p$ und eine differenzierbare Abbildung $\psi\colon B \to M$ gegeben ist. Für $\omega \in \Omega^p(M)$ ist es nun möglich das Integral $\int_B \psi^*\omega$ von ω bzgl. des p-Gebietes (B, ψ) zu definieren. Wir verweisen diesbezüglich z. B. auf [Fra04, S. 95–97]. Die Referenzen [Car58, S. 25–26] und [Wei23, S. 363–364] bauen auf so einem allgemeinem Intergalbegriff auf und definieren eine Integralinvariante als ein Integral einer Differentialform ω bzgl. $\psi(B)$, dessen Wert sich durch (eine festgelegte Art von) Transformationen von $\psi(B)$ nicht ändert. Motiviert von dieser Definition werden wir nun Ref. [Abr67, §15] (siehe auch [Whi64, Kap. X]) folgen und eine eingeschränkte Variante der Integralinvariante definieren, die nur über kompakten Gebieten definiert ist.

Ein lokaler Fluß $t \mapsto F_v(t)$ von $v \in \mathrm{T}(M)$ ist bzgl. einer Karte $(U, u, \mathbb{R}^n)$ der Mannigfaltigkeit M die Lösung der Differentialgleichungen $\partial u^i(F_v(t))/\partial t = v^i(F_v(t))$, wobei $v = v^i\partial/\partial u^i$ und $F_v(0) = x \in U \subset M$. Genauer gibt es ein $\epsilon > 0$ und eine Umgebung $V \subset U$ von x, so daß $F_v(t)$ für $-\epsilon < t < \epsilon$ die Lösung der Differentialgleichungen ist (siehe [Fra04, S. 30–33] und [Nak90, S. 150–151]).

Wir benötigen zusätzlich den Begriff einer Mannigfaltigkeit N mit Rand ([AMR88, S. 478] und [Fra04, S. 105–106], vgl. auch [Bou71a, S. 46, §11.1.1-2]). Dabei ist N eine p-dimensionale Mannigfaltigkeit und für jede Karte $(U, u, \mathbb{R}^p)$ ist das Bild $u(U) \subset \mathbb{R}^p$ in einem Halbraum $\{x|\ c(x) \leq k\}$ bzgl. einem Funktional $c\colon \mathbb{R}^p \to \mathbb{R}$ und einer Konstante $k \in \mathbb{R}$ enthalten. Nun kann das Integral $\int_N \phi^*\omega$ einer Differentialform $\omega \in \Omega^p(M)$ bzgl. einer kompakten und orientierten p-dimensionalen Untermannigfaltigkeit N der n-dimensionalen Mannigfaltigkeit M definiert werden. Dabei kann N einen Rand haben. Für die formale Definition von $\int_N \phi^*\omega$ verweisen wir auf [Fra04, S. 108–109].

Definition 5.5 (Integralinvariante (motiviert durch [Abr67, S. 103]))**.** Sei N eine beliebige kompakte, orientierte und p-dimensionale Untermannigfaltigkeit mit Rand einer n-dimensionalen Mannigfaltigkeit M und ϕ eine glatte Abbildung von N nach M. Eine Integralinvariante ist ein Integral $\int_N \phi^*\omega$ einer Differentialform $\omega \in \Omega^p(M)$, das invariant unter (einer festgelegten Art von) Transformationen ist. Insbesondere bezeichnen wir $\int_N \phi^*\omega$ als eine Integralinvariante bzgl. eines Elementes $v \in \mathrm{T}(M)$, falls $\int_N \phi^*\omega = \int_N (F_v(t)\phi)^*\omega$ für alle t gilt, für die $F_v(t)$ definiert ist.

Zusätzlich führen wir noch den Begriff der invarianten Differentialform ein:

Definition 5.6 (Invariante Differentialform (vgl. [Abr67, S. 103]))**.** Eine Differentialform ist invariant, wenn sie invariant unter (einer festgelegten Art von) Transformationen ist. Insbesondere bezeichenen wir eine Differentialform als invariant bzgl. eines Elementes $v \in \mathrm{T}(M)$, falls $\omega = (F_v(t))^*\omega$ für alle t gilt, für die $F_v(t)$ definiert ist.

Für $v, v_1, \ldots, v_{p-1} \in \mathrm{T}(M)$ definieren wir das innere Produkt $i(v)(\omega)$ von v und $\omega \in \Omega^p(M)$ (siehe [Bou71a, S. 12, §8.3.2], [Bou71b, S. 83, §7.8.4] und [Bou74, Kap. III, §11.9]):

$$(i(v)(\omega))(v_1, \ldots, v_{p-1}) = \begin{cases} \omega(v, v_1, \ldots, v_{p-1}) & \text{für } p > 0 \\ 0 & \text{für } p = 0 \end{cases} \tag{5.7}$$

Zusätzlich benötigen wir noch die Lie-Ableitung $\theta(v)(\omega)$, die für $\omega \in \Omega^p(M)$ und $v \in \mathrm{T}(M)$ auf folgende Weise definiert ist (siehe [Bou71a, S. 15, §8.4.7] und [Fra04, S. 135]):

$$\theta(v)(\omega) = d(i(v)\omega) + i(v)(\mathrm{d}\omega). \tag{5.8}$$

Aufgrund des folgenden Faktums können wir von einer weiteren Betrachtung von Integralinvarianten absehen und uns nur noch mit invarianten Differentialformen beschäftigen.

Faktum 5.7 (siehe [Abr67, Prop. 15.2 und Thm. 15.3])**.** Sei M eine n-dimensionale (reelle) Mannigfaltigkeit, $\omega \in \Omega^p(M)$ eine Differentialform und $v \in \mathrm{T}(M)$. Die folgenden Bedingungen sind äquivalent:

1. Die Differentialform ω ist invariant unter v.
2. $\theta(v)(\omega) = 0$.
3. Für alle kompakten, orientierten und p-dimensionalen Untermannigfaltigkeiten N vom M mit Rand und alle glatten Abbildungen ϕ von N nach M ist $\int_N \phi^*\omega$ eine Integralinvariante.

Bemerkung. Der Begriff der Integralinvariante wurde ursprünglich von Poincaré ([Poi90]) eingeführt. Wir verweisen auf die Referenzen [Car58; Whi64; Abr67].

5.4. De-Rham-Kohomologie homogener Räume

In diesem Abschnitt stellen wir Methoden vor, die die Grundlage zur Berechnung der de-Rham-Kohomologie homogener Räume bilden. Diese Methoden wurden hauptsächlich in den Referenzen [Car29; CE48; Wei79; Kos50b; Car50b; Car50a; Kos50a; Che52b; Bor53] entwickelt. Wir verweisen weiter auf die Artikel [Car36b; Car37; CE48; Sam52; Bor55; Che52a; Dyn57; And62; Roz67; Ras69; Che72; Tam04] sowie die Bücher [Col50; Spi99b; GHV72; GHV73; GHV76; Dup78; Gui80; DFN85; DFN90; Oni94; GS99; Dup03] für eine Einführung oder einen Überblick über die bekannte Theorie. Wir werden im folgenden für die Berechnung der de-Rham-Kohomologie wichtige Ergebnisse wiedergeben. Dabei ist insbesondere der Ansatz aus den Referenzen [Kos50a; Roz67; Ras69] von besonderer Bedeutung.

Sei nun M eine n-dimensionale (reelle) Mannigfaltigkeit und bezeichne τ im folgenden eine Transformation der Mannigfaltigkeit M durch die Operation $\tau_G\colon\ (G, x) \mapsto Gx$ ($G \in \mathrm{G}, x \in M$) der kompakten und zusammenhängenden Lie-Gruppe G auf M (siehe z. B. [Bou05, Kap. IX, §6.5] oder [GHV73, S. 109–110]). Wir bezeichnen mit $\Omega(M)^{\mathrm{G}} \subset \Omega(M)$ die unter τ invarianten Differentialformen. Da G kompakt und zusammenhängend ist, ist die Bedingung, daß $\theta(g)\omega = 0$ für alle $g \in \mathfrak{g}$ gilt, äquivalent dazu, daß ω invariant unter G ist (siehe [Bou05, Kap. IX, §6.5] und [GHV73, Kap. III, §4, Prop. VI], vgl. auch Faktum 5.7). Nach einem Ergebnis von E. Cartan ([Car29]) können wir uns bei der Betrachtung der de-Rham-Kohomologie von M auf invariante Differentialformen einschränken:

Faktum 5.8 (siehe z. B. [Bou05, Kap. IX, §6.5, Thm. 2])**.** $\mathrm{H}^*(\Omega(M)^{\mathrm{G}}, \mathrm{d}) \cong \mathrm{H}^*(\Omega(M), \mathrm{d})$

Im Fall von $M = \mathrm{G}$ gilt, daß die invarianten Differentialformen $\Omega(\mathrm{G})^{\mathrm{G}}$ vom Grad p isomorph zu den p-linearen und alternierenden Abbildungen $\mathrm{Alt}^p(\mathfrak{g}, \mathbb{R})$ von $\mathfrak{g}^{\times p} = \mathfrak{g} \times \cdots \times \mathfrak{g}$ nach $\mathbb{R}$ sind (siehe [Bou89b, Kap. III, §6.13, Prop. 50] oder [GHV73, Kap. IV, §2, Prop. II]). Wir können nun die Operatoren d, $i(a)$ und $\theta(a)$ ($a \in \mathfrak{g}$) auch auf $\mathrm{Alt}(\mathfrak{g}, \mathbb{R}) = \otimes_{p\geq 0}\mathrm{Alt}^p(\mathfrak{g}, \mathbb{R})$ definieren. Diese Operatoren entsprechen den Operatoren d, $i(v)$ und $\theta(v)$ ($v \in \mathrm{T}(M)$) auf $\Omega(M)$ (siehe Gleichungen 5.6, 5.7 und 5.8). Wir erhalten für $g, g_1, \ldots, g_{p+1} \in \mathfrak{g}$ und $\omega \in \mathrm{Alt}^p(\mathfrak{g}, \mathbb{R})$ (siehe z. B. [Bou05, Kap. IX, §6.5], vgl. auch [Bou71a, S. 18, §8.5.7]):

$$(\mathrm{d}\omega)(g_1, \ldots, g_{p+1}) = \sum_{i<j}(-1)^{i+j}\omega([g_i, g_j], g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_{j-1}, g_{j+1}, \ldots, g_{p+1}) \tag{5.9}$$

$$(\theta(g)\omega)(g_1, \ldots, g_p) = -\sum_i \omega(g_1, \ldots, g_{i-1}, [g, g_i], g_{i+1}, \ldots, g_p) \tag{5.10}$$

$$(i(g)\omega)(g_1, \ldots, g_{p-1}) = \omega(g, g_1, \ldots, g_{p-1}) \tag{5.11}$$

Weiter bezeichnen wir mit $\mathrm{Alt}(\mathfrak{g}, \mathbb{R})^{\mathrm{Ad(G)}}$, die Elemente $\omega \in \mathrm{Alt}(\mathfrak{g}, \mathbb{R})$, die invariant unter der adjungierten Darstellung Ad(G) von G auf $\mathfrak{g}$ sind, d. h., $\theta(g)(\omega) = 0$ gilt für alle $g \in \mathfrak{g}$. Es ergibt sich folgende Konsequenz von Faktum 5.8:

Faktum 5.9 (siehe z. B. [Bou05, Kap. IX, §6.5, Kor. 1 zu Thm. 2])**.** Die beiden Vektorräume $\mathrm{H}^*(\Omega(\mathrm{G}), \mathrm{d})$ und $\mathrm{Alt}(\mathfrak{g}, \mathbb{R})^{\mathrm{Ad(G)}}$ sind isomorph.

Die Menge $\mathrm{Sym}^p(\mathfrak{g}, \mathbb{R})$ der p-linearen und symmetrischen Abbildungen von $\mathfrak{g}^{\times p} = \mathfrak{g} \times \cdots \times \mathfrak{g}$ nach $\mathbb{R}$ wird im folgenden eine besondere Bedeutung spielen. Eine Abbildung $s(g_1, \ldots, g_p)$ mit $g_1, \ldots, g_p \in \mathfrak{g}$ gilt dabei als symmetrisch, falls für alle Permutationen $\pi \in \mathcal{S}_p$ der Menge $\{1, \ldots, p\}$ die Gleichung $s(g_{\pi(1)}, \ldots, g_{\pi(p)}) = s(g_1, \ldots, g_p)$ gilt (vgl. [Bou74, Kap. III, §6.3]). Wir benutzen die Schreibweise $\mathrm{Sym}(\mathfrak{g}, \mathbb{R}) = \oplus_{p\geq 0}\mathrm{Sym}^p(\mathfrak{g}, \mathbb{R})$ und führen die Teilmenge $\mathrm{Sym}(\mathfrak{g}, \mathbb{R})^{\mathrm{Ad(G)}} \subset \mathrm{Sym}(\mathfrak{g}, \mathbb{R})$ der unter der Operation der adjungierten Darstellung Ad(G) invarianten Elemente ein. Bezeichne $\varepsilon_\pi = \prod_{i<j}(\pi(i) - \pi(j))/(i - j)$ das Signum einer Permutation π (siehe z. B. [Bos96, S. 221]).

Definition 5.10 (Cartan-Abbildung ([Wei79, S. 435–436], [Dyn57, S. 306], [GHV76, Kap. VI, §2, Prop. IV] oder [Oni94, Kap. 3, §10.10]))**.** Die Cartan-Abbildung

$$c\colon\ \mathrm{Sym}^p(\mathfrak{g}, \mathbb{R}) \to \mathrm{Alt}^{2p-1}(\mathfrak{g}, \mathbb{R})$$

ist durch die Gleichung

$$s(g_1,\ldots,g_p) \mapsto \frac{(-1)^{p-1}(p-1)!}{2^{p-1}(2p-1)!} \sum_{\pi\in\mathcal{S}_{2p-1}} \varepsilon_\pi \; s(g_{\pi(1)},[g_{\pi(2)},g_{\pi(3)}],\ldots,[g_{\pi(2p-2)},g_{\pi(2p-1)}]) \tag{5.12}$$

gegeben, wobei $g_1,\ldots,g_{2p-1} \in \mathfrak{g}$.

Eine wichtige Eigenschaft der Cartan-Abbildung ist im folgenden Faktum enthalten:

Faktum 5.11 ([Car50a, S. 58–60], [GHV76, Kap. VI, §4, Thm. II], [Oni94, Kap. 3, §10.7] oder [Ras69, S. 61–62])**.** Die Cartan-Abbildung bildet die Erzeuger von $\mathrm{Sym}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ bijektiv auf die Erzeuger von $\mathrm{Alt}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ ab.

Damit sind wird nun in der Lage die de-Rham-Kohomologie von G mit Hilfe von Faktum 5.9 und Faktum 5.11 zu berechnen. Wir identifizieren im folgenden oft die Menge $\mathrm{Sym}^p(\mathfrak{g},\mathbb{R})$ der p-linearen und symmetrischen Abbildungen von $\mathfrak{g}^{\times p} = \mathfrak{g}\times\cdots\times\mathfrak{g}$ nach $\mathbb{R}$ mit den Polynomen vom Grad p über den linearen Abbildungen von $\mathfrak{g}$ nach $\mathbb{R}$ (siehe [Bou81, Kap. IV, §5.11]).

Bemerkung. Im Fall von $\mathrm{G} = \mathrm{SU}(d)$ sind die Erzeuger von $\mathrm{Sym}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ durch die Koeffizienten des charakteristischen Polynoms eines allgemeinen Elementes von $\mathfrak{g}$ gegeben (siehe z. B. [Oni94, S. 186–187]). Im Fall von $\mathrm{G} = \mathrm{SU}(2)$ erhalten wir für $x_1,x_2,x_3 \in \mathbb{R}$ die Darstellung

$$\mathfrak{su}(2) \cong iL = i\begin{pmatrix} x_3 & x_1 - ix_2 \\ x_1 + ix_2 & -x_3 \end{pmatrix}.$$

Die Algebra $\mathrm{Sym}(\mathfrak{su}(2),\mathbb{R})^{\mathrm{Ad(SU(2))}}$ wird von dem Element $x_1^2+x_2^2+x_3^2$ erzeugt, da

$$z^2 + 0z - (x_1^2+x_2^2+x_3^2)$$

das charakteristische Polynom von L in der Variable z ist. Hierbei entsprechen die x_i den linearen (und symmetrischen) Abbildungen

$$g \in \mathfrak{g} \mapsto x_i(g)$$

und $x_1^2+x_2^2+x_3^2$ der 2-linearen und symmetrischen Abbildung

$$(g_1,g_2) \in \mathfrak{g}^2 \mapsto x_1(g_1)\cdot x_1(g_2) + x_2(g_1)\cdot x_2(g_2) + x_3(g_1)\cdot x_3(g_2).$$

Wir betrachten nun den Fall $M = \mathrm{G/H}$, wobei wir als Transformationen die Operation der (kompakten) Lie-Gruppe G per Linksmultiplikation auf G/H annehmen. Diese Operation ist transitiv (siehe Abschnitt 5.1). Wir erinnern an die Zerlegung $\mathfrak{g} = \mathfrak{h} + \mathfrak{m}$ der Lie-Algebra (siehe Abschnitt 5.1). Nach [Bou89b, Kap. III, §1.8, Kor. 1 zu Prop. 17] (vgl. auch [Car29, S. 187]) können $\Omega(\mathrm{G/H})^{\mathrm{G}}$ und

$$\mathcal{A}(\mathfrak{g},\mathfrak{h}) = \{\omega \in \mathrm{Alt}(\mathfrak{g},\mathbb{R})|\ i(h)(\omega) = 0 \text{ und } \theta(h)(\omega) = 0 \text{ für alle } h \in \mathfrak{h}\}$$

identifiziert werden und es ergibt sich bei entsprechender Wahl von d:

Faktum 5.12 (siehe z. B. [Bou05, Kap. IX, §6.5, Kor. 2 zu Thm. 2])**.** $\mathrm{H}^*(\Omega(\mathrm{G/H}),\mathrm{d}) \cong \mathrm{H}^*(\Omega(\mathrm{G/H})^{\mathrm{G}},\mathrm{d}) \cong \mathrm{H}^*(\mathcal{A}(\mathfrak{g},\mathfrak{h}),\mathrm{d})$

Im folgenden spielt die Algebra $\mathrm{Sym}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ (bzw. $\mathrm{Sym}(\mathfrak{h},\mathbb{R})^{\mathrm{Ad(H)}}$) der multilinearen und symmetrischen Abbildungen von $\mathfrak{g}$ (bzw. von $\mathfrak{h}$) nach $\mathbb{R}$, die invariant unter adjungierten Darstellung Ad(G) (bzw. Ad(H)) sind, eine besondere Rolle. Die Algebra $\mathrm{Sym}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ (bzw. $\mathrm{Sym}(\mathfrak{h},\mathbb{R})^{\mathrm{Ad(H)}}$) sei von den Elementen g_i (bzw. h_j) mit $i \in \{1,\ldots,\alpha\}$ (bzw. $j \in \{1,\ldots,\beta\}$) erzeugt, wobei die Erzeuger algebraisch unabhängig sind. (Wir merken an, daß die Erzeuger der Algebra $\mathrm{Sym}(\mathfrak{h},\mathbb{R})^{\mathrm{Ad(H)}}$ durch Terme der Form $\mathrm{Tr}(\rho^2)$ dargestellt werden können, falls wir die Lie-Algebra $\mathfrak{g}$ mit den Dichtematrizen (siehe Seite 64) identifizieren und ρ eine reduzierte Dichtematrix (siehe z. B. [BŻ06, §9.1]) bezeichnet.) Wir betrachten nun die Einschränkung von $\mathrm{Sym}(\mathfrak{g},\mathbb{R})^{\mathrm{Ad(G)}}$ auf Elemente von $\mathrm{Sym}(\mathfrak{h},\mathbb{R})$, dabei bezeichne $\tilde{\mathrm{g}}_i$ das Bild von g_i unter dieser Einschränkung. Nun können wir die Abbildungen $\tilde{\mathrm{g}}_i$ als Polynome f_i in den Abbildungen h_j darstellen (siehe z. B. [Roz67, S. 313–314]). Dabei identifizieren wir die Abbildungen h_j mit formalen Variabeln eines Polynomrings $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$ über $\mathbb{R}$. Dies ist möglich, da die Abbildungen h_j algebraisch unabhängig gewählt wurden. Falls R ein (kommutativer) Ring ist, bezeichnen wir eine Untergruppe I (bzgl. der Addition) als ein Ideal, falls für alle $\mathrm{r} \in \mathrm{R}$ und alle $\mathrm{f} \in \mathrm{I}$ die Bedingung $\mathrm{r}\cdot\mathrm{f} \in \mathrm{I}$ erfüllt ist ([Bou74, Kap. III, §8.6]). Im folgenden verwenden wir R zur Bezeichnung eines allgemeinen Polynomringes und $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$ zur Bezeichnung des speziellen (reellen) Polynomringes mit den Variabeln h_j ($j \in \{1,\ldots,\beta\}$). Weiterhin verwenden wir die Symbole f und f_i gleichzeitig als Bezeichner für Elemente von R und $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$, wobei die entsprechende Bedeutung aus dem Kontext ersichtlich ist.

Faktum 5.13 ([Car50a, S. 69])**.** Die Struktur von $\mathrm{H}^*(\Omega(\mathrm{G/H}),\mathrm{d})$ ist eindeutig durch das von den Polynomen $\mathrm{f}_i \in \mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$) erzeugten Ideal festgelegt.

Im folgenden identifizieren wir das von den f_i erzeugte Ideal I mit dem von den f_i erzeugten R-Modul $\mathrm{M_I}$, d. h., jedes Element von $\mathrm{M_I}$ kann nun in der Form $\sum_i \mathrm{r}_i\cdot\mathrm{f}_i$ mit $\mathrm{r}_i \in \mathrm{R}$ dargestellt werden. Für die weitere Argumentation benötigen wir den Begriff der Syzygie (vgl. [Hil90]):

Definition 5.14 (Syzygien (vgl. [Vas98, S. 12, Def. 1.2.1] und [BW93, S. 136]))**.** Sei R ein Ring und M ein Modul, der von der Menge $\{\mathrm{f}_1,\ldots,\mathrm{f}_l\} \subset \mathrm{M}$ erzeugt wird. Die Syzygien der f_i sind die Tupel $\mathrm{s} = (\mathrm{s}_1,\ldots,\mathrm{s}_l) \in \mathrm{R}^l$, so daß die Gleichung $\sum_{i=1}^{l} \mathrm{s}_i\cdot\mathrm{f}_i = 0$ gilt. Der von den Syzygien erzeugte Modul $\mathrm{Syz}(\mathrm{f}_1,\ldots,\mathrm{f}_l)$ wird als der Syzygien-Modul von M bezeichnet.

Für $a,b \in \{1,\ldots,l\}$ mit $a \neq b$ führen wir die spezielle Syzygie $\mathrm{s} = (\mathrm{s}_1,\ldots,\mathrm{s}_l) \in \mathrm{R}^l$ mit

$$\mathrm{s}_i = \begin{cases} \mathrm{f}_b & \text{für } i = a \\ -\mathrm{f}_a & \text{für } i = b \\ 0 & \text{für } i \neq a \text{ und } i \neq b \end{cases} \tag{5.13}$$

ein. Wir erhalten die Gleichung $(\mathrm{f}_b)\cdot\mathrm{f}_a + (-\mathrm{f}_a)\cdot\mathrm{f}_b = 0$. Wir bezeichnen eine Syzygie, die die Form aus Gleichung (5.13) hat, und jede R-Linearkombination derartiger Syzygien als trivial (vgl. [Roz67, S. 278]). Mit dem Symbol $\mathrm{Alt}(\{\mathrm{z}_1,\ldots,\mathrm{z}_v\};\mathfrak{g},\mathbb{R})$ bezeichnen wir die von den Elementen $\mathrm{z}_1,\ldots,\mathrm{z}_v \in \mathrm{Alt}(\mathfrak{g},\mathbb{R})$ erzeugte Unteralgebra von $\mathrm{Alt}(\mathfrak{g},\mathbb{R})$.

Faktum 5.15 ([Roz67, S. 277–279])**.** Sei c die Cartan-Abbildung (Gleichung (5.12)). Wir identifizieren $\mathrm{Sym}(\mathfrak{h},\mathbb{R})^{\mathrm{Ad(H)}}$ mit dem Polynomring $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$. Seien die $\mathrm{f}_1,\ldots,\mathrm{f}_l$ Erzeuger des Ideals I und die $\mathrm{s}_1,\ldots,\mathrm{s}_k$ mit $\mathrm{s}_a = (\mathrm{s}_{a,1},\ldots,\mathrm{s}_{a,l}) \in \mathrm{P}^l$ Repräsentanten für die Menge der nicht trivialen Syzygien aus $\mathrm{Syz}(\mathrm{f}_1,\ldots,\mathrm{f}_l)$. Es folgt, daß $\mathrm{H}^*(\mathcal{A}(\mathfrak{g},\mathfrak{h}),\mathrm{d})$ äquivalent zu einem H^* ist, so daß die folgende Bedingung erfüllt ist:

$$\mathrm{H}^* \supset \mathrm{P/I} \otimes \mathrm{Alt}\left(\left\{\sum_j \mathrm{s}_{a,j}\cdot c(\mathrm{g}_j)\colon a\in\{1,\ldots,k\}\right\};\mathfrak{g},\mathbb{R}\right)$$

Nach Faktum 5.13 wissen wir, daß die Kohomologie nicht von den Erzeugern f_i des Ideals I abhängt. Das folgende Faktum macht die Wirkung von möglichen Transformationen auf den Erzeugern explizit.

Faktum 5.16 ([Ras69, S. 86–87])**.** Seien die $\mathrm{f}_1,\ldots,\mathrm{f}_l$ die Erzeuger des Ideals I über dem Polynomring $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$. Wenn $\mathrm{f}_{\mu_v} = \sum_{i=1}^{v-1} \mathrm{p}_i\cdot\mathrm{f}_{\mu_i}$ mit $\mathrm{p}_i \in \mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$ in dem von den $\mathrm{f}_{\mu_1},\ldots,\mathrm{f}_{\mu_{v-1}}$ erzeugten Ideal liegt, können wir bei der Berechnung der Kohomologie $\mathrm{H}^*(\mathcal{A}(\mathfrak{g},\mathfrak{h}),\mathrm{d})$ das Polynom f_{μ_v} in den Erzeugern des Ideals I durch $\mathrm{f}'_{\mu_v} = \mathrm{f}_{\mu_v} - \sum_{i=1}^{v-1}\mathrm{p}_i\cdot\mathrm{f}_{\mu_i}$ ersetzen, und wir erhalten unter der Cartan-Abbildung c (Gleichung (5.12)) zusätzlich die Identität

$$c\left(\mathrm{g}_{\mu_v} - \sum_{i=1}^{v-1}\mathrm{p}_i\cdot\mathrm{g}_{\mu_i}\right) = c(\mathrm{g}_{\mu_v}) - \sum_{i=1}^{v-1}\mathrm{p}_i\cdot c(\mathrm{g}_{\mu_i}).$$

Später werden wir Fälle betrachten, in denen die Anzahl der nicht verschwindenden f_i kleiner gleich der Anzahl der h_j ist. In diesen Fällen hilft das folgende Faktum.

Faktum 5.17 ([Ras69, S. 86–87])**.** Seien die $\mathrm{f}_1,\ldots,\mathrm{f}_l$ die Erzeuger des Ideals I über dem Polynomring $\mathrm{P} = \mathbb{R}[\mathrm{h}_1,\ldots,\mathrm{h}_\beta]$ und bezeichnet die Menge $\{\mathrm{f}_{\mu_1},\ldots,\mathrm{f}_{\mu_v}\}$ die Elemente, für die $\mathrm{f}_{\mu_i} = 0$ gilt. Ist die Anzahl der nicht verschwindenden f_i kleiner gleich der Anzahl β der h_j, dann erhalten wir:

$$\mathrm{H}^*(\mathcal{A}(\mathfrak{g},\mathfrak{h}),\mathrm{d}) \cong \mathrm{P/I}\otimes\mathrm{Alt}\left(\{c(\mathrm{g}_{\mu_1}),\ldots,c(\mathrm{g}_{\mu_v})\};\mathfrak{g},\mathbb{R}\right)$$

5.5. Zwei-Qubit-Fall

Wir betrachten nun den Fall $\mathrm{G/H} = \mathrm{SU}(4)/(\mathrm{SU}(2)\otimes\mathrm{SU}(2))$. Unter Benutzung der Notation $\sigma_0 = \mathrm{Id}$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, und $\sigma_3 = \sigma_z$ definieren wir (vgl. Abschnitt 4.2.3)

$$B_1 := i\sigma_0\otimes\sigma_1, B_2 := i\sigma_0\otimes\sigma_2, B_3 := i\sigma_0\otimes\sigma_3, B_4 := i\sigma_1\otimes\sigma_0, B_5 := i\sigma_1\otimes\sigma_1,$$
$$B_6 := i\sigma_1\otimes\sigma_2, B_7 := i\sigma_1\otimes\sigma_3, B_8 := i\sigma_2\otimes\sigma_0, B_9 := i\sigma_2\otimes\sigma_1, B_{10} := i\sigma_2\otimes\sigma_2,$$
$$B_{11} := i\sigma_2\otimes\sigma_3, B_{12} := i\sigma_3\otimes\sigma_0, B_{13} := i\sigma_3\otimes\sigma_1, B_{14} := i\sigma_3\otimes\sigma_2, B_{15} := i\sigma_3\otimes\sigma_3.$$

Ein allgemeines Element $g \in \mathfrak{g} = \mathfrak{su}(4)$ parametrisieren wir nun durch $g = \sum_{j=1}^{15} x_j B_j$, wobei $x_1,\ldots,x_{15}$ die Variabeln des Polynomrings $\mathbb{R}[x_1,\ldots,x_{15}]$ sind. Die Variabeln

$x_1, \ldots, x_4, x_8, x_{12}$ entsprechen bzgl. der Zerlegung $\mathfrak{g} = \mathfrak{h} + \mathfrak{m}$ (siehe Abschnitt 5.1) Abbildungen von $\mathfrak{h}$ nach $\mathbb{R}$. Die anderen Variabeln entsprechen Abbildungen von $\mathfrak{m}$ nach $\mathbb{R}$. Wir folgen Abschnitt 5.4 und erhalten die Polynome (vgl. Bemerkung auf Seite 74)

$$\mathrm{h}_1 = x_4^2 + x_8^2 + x_1^2$$

und

$$\mathrm{h}_2 = x_1^2 + x_2^2 + x_3^2$$

als Erzeuger von $\mathrm{Sym}(\mathfrak{h}, \mathbb{R})^{\mathrm{Ad(H)}}$. Entsprechen ergeben sich aus dem charakteristischen Polynom von g/i die Polynome

$$\mathrm{g}_1 = -2 \sum_i x_i^2,$$

$$\begin{aligned}\mathrm{g}_2 = 8(&-x_1x_4x_5 - x_1x_8x_9 - x_1x_{12}x_{13} - x_2x_4x_6 - x_2x_8x_{10} - x_2x_{12}x_{14} - x_3x_4x_7\\ &-x_3x_8x_{11} - x_3x_{12}x_{15} + x_5x_{10}x_{15} - x_5x_{11}x_{14} - x_6x_9x_{15} + x_6x_{11}x_{13} + x_7x_9x_{14} - x_7x_{10}x_{13})\end{aligned}$$

und

$$\begin{aligned}\mathrm{g}_3 = (&\sum_{i=1}^{15} x_i^4) + 2(x_1^2x_2^2 + x_1^2x_3^2 + x_1^2x_6^2 + x_1^2x_7^2 + x_1^2x_{10}^2 + x_1^2x_{11}^2 + x_1^2x_{14}^2 + x_1^2x_{15}^2 + x_2^2x_3^2\\ &+x_2^2x_5^2 + x_2^2x_7^2 + x_2^2x_9^2 + x_2^2x_{11}^2 + x_2^2x_{13}^2 + x_2^2x_{15}^2 + x_3^2x_5^2 + x_3^2x_6^2 + x_3^2x_9^2 + x_3^2x_{10}^2 + x_3^2x_{13}^2\\ &+x_3^2x_{14}^2 + x_4^2x_8^2 + x_4^2x_9^2 + x_4^2x_{10}^2 + x_4^2x_{11}^2 + x_4^2x_{12}^2 + x_4^2x_{13}^2 + x_4^2x_{14}^2 + x_4^2x_{15}^2 + x_5^2x_6^2 + x_5^2x_7^2\\ &+x_5^2x_8^2 + x_5^2x_9^2 + x_5^2x_{12}^2 + x_5^2x_{13}^2 + x_6^2x_7^2 + x_6^2x_8^2 + x_6^2x_{10}^2 + x_6^2x_{12}^2 + x_6^2x_{14}^2 + x_7^2x_8^2 + x_7^2x_{11}^2\\ &+x_7^2x_{12}^2 + x_7^2x_{15}^2 + x_8^2x_{12}^2 + x_8^2x_{13}^2 + x_8^2x_{14}^2 + x_8^2x_{15}^2 + x_9^2x_{10}^2 + x_9^2x_{11}^2 + x_9^2x_{12}^2 + x_9^2x_{13}^2\\ &+x_{10}^2x_{11}^2 + x_{10}^2x_{12}^2 + x_{10}^2x_{14}^2 + x_{11}^2x_{12}^2 + x_{11}^2x_{15}^2 + x_{13}^2x_{14}^2 + x_{13}^2x_{15}^2 + x_{14}^2x_{15}^2) - 2(x_1^2x_4^2\\ &+x_1^2x_5^2 + x_1^2x_8^2 + x_1^2x_9^2 + x_1^2x_{12}^2 + x_1^2x_{13}^2 + x_2^2x_4^2 + x_2^2x_6^2 + x_2^2x_8^2 + x_2^2x_{10}^2 + x_2^2x_{12}^2 + x_2^2x_{14}^2\\ &+x_3^2x_4^2 + x_3^2x_7^2 + x_3^2x_8^2 + x_3^2x_{11}^2 + x_3^2x_{12}^2 + x_3^2x_{15}^2 + x_4^2x_5^2 + x_4^2x_6^2 + x_4^2x_7^2 + x_5^2x_{10}^2 + x_5^2x_{11}^2\\ &+x_5^2x_{14}^2 + x_5^2x_{15}^2 + x_6^2x_9^2 + x_6^2x_{11}^2 + x_6^2x_{13}^2 + x_6^2x_{15}^2 + x_7^2x_9^2 + x_7^2x_{10}^2 + x_7^2x_{13}^2 + x_7^2x_{14}^2 + x_8^2x_9^2\\ &+x_8^2x_{10}^2 + x_8^2x_{11}^2 + x_9^2x_{14}^2 + x_9^2x_{15}^2 + x_{10}^2x_{13}^2 + x_{10}^2x_{15}^2 + x_{11}^2x_{13}^2 + x_{11}^2x_{14}^2 + x_{12}^2x_{13}^2 + x_{12}^2x_{14}^2\\ &+x_{12}^2x_{15}^2) + 8(x_1x_4x_{10}x_{15} + x_1x_6x_{11}x_{12} + x_1x_7x_8x_{14} + x_2x_4x_{11}x_{13} + x_2x_5x_8x_{15}\\ &+x_2x_7x_9x_{12} + x_3x_4x_9x_{14} + x_3x_5x_{10}x_{12} + x_3x_6x_8x_{13} + x_5x_6x_9x_{10} + x_5x_6x_{13}x_{14}\\ &+x_5x_7x_9x_{11} + x_5x_7x_{13}x_{15} + x_6x_7x_{10}x_{11} + x_6x_7x_{14}x_{15} + x_9x_{10}x_{13}x_{14} + x_9x_{11}x_{13}x_{15}\\ &+x_{10}x_{11}x_{14}x_{15}) - 8(x_1x_2x_5x_6 + x_1x_2x_9x_{10} + x_1x_2x_{13}x_{14} + x_1x_3x_5x_7 + x_1x_3x_9x_{11}\\ &+x_1x_3x_{13}x_{15} + x_1x_4x_{11}x_{14} + x_1x_6x_8x_{15} + x_1x_7x_{10}x_{12} + x_2x_3x_6x_7 + x_2x_3x_{10}x_{11}\\ &+x_2x_3x_{14}x_{15} + x_2x_4x_9x_{15} + x_2x_5x_{11}x_{12} + x_2x_7x_8x_{13} + x_3x_4x_{10}x_{13} + x_3x_5x_8x_{14}\\ &+x_3x_6x_9x_{12} + x_4x_5x_8x_9 + x_4x_5x_{12}x_{13} + x_4x_6x_8x_{10} + x_4x_6x_{12}x_{14} + x_4x_7x_8x_{11}\\ &+x_4x_7x_{12}x_{15} + x_8x_9x_{12}x_{13} + x_8x_{10}x_{12}x_{14} + x_8x_{11}x_{12}x_{15})\end{aligned}$$

als Erzeuger von $\mathrm{Sym}(\mathfrak{g}, \mathbb{R})^{\mathrm{Ad(G)}}$. Nun können wir die Polynome $\tilde{\mathrm{g}}_i$ als Polynome $\mathrm{f}_i \in \mathrm{P} = \mathbb{R}[\mathrm{h}_1, \ldots, \mathrm{h}_\beta]$ in den Variabeln h_j darstellen. Wir erhalten $\mathrm{f}_1 = -2(\mathrm{h}_1 + \mathrm{h}_2)$, $\mathrm{f}_2 = 0$ und $\mathrm{f}_3 = (\mathrm{h}_1 - \mathrm{h}_2)^2$. Die einzige Syzygie, die nicht trivial ist, entsteht durch die Tatsache, daß $\mathrm{f}_2 = 0$ ist. Es bezeichne I das von den f_i ($i \in \{1, 2, 3\}$) erzeugte Ideal (siehe Faktum 5.13), c die Cartan-Abbildung (siehe Gleichung (5.12)) und $\mathrm{Alt}(\{\mathrm{z}_1, \ldots, \mathrm{z}_v\}; \mathfrak{g}, \mathbb{R})$

die von den Elementen $z_1, \ldots, z_v \in \mathrm{Alt}(\mathfrak{g}, \mathbb{R})$ erzeugte Unteralgebra von $\mathrm{Alt}(\mathfrak{g}, \mathbb{R})$. Da in dem betrachteten Fall die Anzahl der f_i mit $f_i \neq 0$ kleiner gleich der Anzahl β der h_j ist, folgt aus Faktum 5.15 und Faktum 5.17:

Theorem 5.18. Der de-Rham-Kohomologie-Ring von $\mathrm{SU}(4)/(\mathrm{SU}(2) \otimes \mathrm{SU}(2))$ ist äquivalent zu $\mathrm{P/I} \otimes \mathrm{Alt}(\{c(g_2)\}; \mathfrak{g}, \mathbb{R})$, wobei $\mathrm{P} = \mathbb{R}[h_1, \ldots, h_\beta]$.

Bemerkung. Die topologische Herangehensweise zeichnet die symmetrische Invariante g_2 sowie ihre antisymmetrische Entsprechung $c(g_2)$ aus.

5.6. Drei-Qubit-Fall

Wir betrachten nun den Fall $\mathrm{G/H} = \mathrm{SU}(8)/(\mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \mathrm{SU}(2))$. Sei

$$B_{j*16+k*4+l} = i\sigma_j \otimes \sigma_k \otimes \sigma_l$$

mit $(0,0,0) \neq (i,j,k) \in \{0,1,2,3\}^3$ eine Basis von $\mathfrak{g}$. Ein allgemeines Element $g \in \mathfrak{g} = \mathfrak{su}(8)$ parametrisieren wir durch $g = \sum_{j=1}^{63} x_j B_j$. Die Variabeln

$$x_1, \ldots, x_4, x_8, x_{12}, x_{16}, x_{32}, x_{48} \in \mathbb{R}[x_1, \ldots, x_{63}]$$

entsprechen bzgl. der Zerlegung $\mathfrak{g} = \mathfrak{h} + \mathfrak{m}$ Abbildungen von $\mathfrak{h}$ nach $\mathbb{R}$. Die anderen Variabeln entsprechen Abbildungen von $\mathfrak{m}$ nach $\mathbb{R}$. Die Polynome $h_1 = x_{16}^2 + x_{32}^2 + x_{48}^2$, $h_2 = x_4^2 + x_8^2 + x_{12}^2$ und $h_3 = x_1^2 + x_2^2 + x_3^2$ erzeugen $\mathrm{Sym}(\mathfrak{h}, \mathbb{R})^{\mathrm{Ad(H)}}$. Wir erhalten die folgenden Polynome ($f_i \in \mathrm{P} = \mathbb{R}[h_1, \ldots, h_\beta]$):

$$f_1 = -4(h_1 + h_2 + h_3),\ f_2 = 0,\ f_3 = 6h_1^2 + 4h_1h_2 + 6h_2^2 + 4h_1h_3 + 4h_2h_3 + 6h_3^2,$$
$$f_4 = 0,\ f_5 = 4(-10h_1h_2h_3 - h_1^3 - h_2^3 - h_3^3 + h_1^2h_2 + h_1h_2^2 + h_1^2h_3 + h_2^2h_3 + h_1h_3^2 + h_2h_3^2),$$
$$f_6 = 0,\ f_7 = h_1^4 + h_2^4 + h_3^4 + 6(h_1^2h_2^2 + h_1^2h_3^2 + h_2^2h_3^2)$$
$$+4(-h_1^3h_2 - h_1h_2^3 - h_1^3h_3 + h_1^2h_2h_3 + h_1h_2^2h_3 - h_2^3h_3 + h_1h_2h_3^2 - h_1h_3^3 - h_2h_3^3)$$

Zur Berechnung der f_i haben wir die Polynome g_i nicht explizit bestimmt. Zusätzlich zu den Syzygien, die aufgrund der Gleichungen $f_2 = 0$, $f_4 = 0$ und $f_6 = 0$ entstehen, erhalten wir die folgende nichttriviale Syzygie:

$$(-8h_1h_2h_3) \cdot f_1 + ((h_1^2 + h_2^2 + h_3^2)/2 - h_1h_2 - h_1h_3 - h_2h_3) \cdot f_3 + (h_1 + h_2 + h_3)/2 \cdot f_5 - f_7 = 0$$

Aufgrund von Faktum 5.16 können wir f_7 durch $f_7' = (-8h_1h_2h_3) \cdot f_1 + ((h_1^2 + h_2^2 + h_3^2)/2 - h_1h_2 - h_1h_3 - h_2h_3) \cdot f_3 + (h_1 + h_2 + h_3)/2 \cdot f_5 - f_7 = 0$ ersetzen. Die Anzahl der nicht verschwindenden Elemente von $\{f_1, \ldots, f_6, f_7'\}$ ist kleiner gleich der Anzahl β der h_j und wir erhalten mit Faktum 5.15 und Faktum 5.17:

Theorem 5.19. Der de-Rham-Kohomologie-Ring von $\mathrm{SU}(8)/(\mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \mathrm{SU}(2))$ ist äquivalent zu

$$\mathrm{P/I} \otimes \mathrm{Alt}\left(\{r,\, c(g_2), c(g_4), c(g_6)\}\,; \mathfrak{g}, \mathbb{R}\right),$$

wobei $r := (-8h_1h_2h_3) \cdot c(g_1) + ((h_1^2 + h_2^2 + h_3^2)/2 - h_1h_2 - h_1h_3 - h_2h_3) \cdot c(g_3) + (h_1 + h_2 + h_3)/2 \cdot c(g_5) - c(g_7)$ und $\mathrm{P} = \mathbb{R}[h_1, \ldots, h_\beta]$.

Die topologische Herangehensweise zeichnet die antisymmetrischen Elemente r, $c(\mathrm{g}_2)$, $c(\mathrm{g}_4)$ und $c(\mathrm{g}_6)$ sowie ihre symmetrischen Entsprechungen aus. Die berechneten Invarianten von Lie-Algebra-Elementen lassen sich auch als spezielle Invarianten von Quantenzuständen und Dichtematrizen (siehe Seite 64) auffassen, die dem in der Literatur oft betrachteten Ansatz der Berechnung von Invarianten bzgl. der Operation mit lokal unitären Transformationen entsprechen (siehe z. B. [SM95; SM96; GRB98; LP98; CLPS99; LPS99; CS00; Sud01; BL01; Bry02; MW02; BB02a; Gra02; LT03; BLT03; BLTV04; Wal05; KW06; LT06]). Dabei werden Methoden der klassischen Invariantentheorie ([Stu93; PV94; Olv99; DK02]) verwendet.

Wir haben die (mathematische) Struktur der homogenen Räume durch die Berechnung der de-Rham-Kohomologie-Ring genauer charakterisiert. Ein Verständnis der Bedeutung der de-Rham-Kohomologie für die Struktur der Verschränkung ([BŻ06], vgl. auch Abschnitt 4.7) sowie insbesondere für die effiziente Erzeugung von unitären Transformationen bedarf weiterer Untersuchungen.

6. Leitfaden und Ausblick

In diesem Kapitel geben wir einen Überblick über die Ergebnisse dieser Arbeit und einen Ausblick. Das Thema der Arbeit ist die Erzeugung unitärer Transformation, wobei die unitären Transformationen die durchführbaren Operationen sind und zugleich eine Beschreibungssprache für Algorithmen auf Quantenrechnern bilden. Wir betrachten in dieser Arbeit verschiedene Aspekte und Szenarien der Erzeugung unitärer Transformationen. Dabei basieren die unterschiedlichen Aspekte teilweise auf verschiedenen Mengen von Grundoperationen. Wir verwenden durchgehend Lie-theoretische Methoden, und diese zeigen sich als ein geeignetes Werkzeug zur Beschreibung, Analyse und Lösung der zugrundeliegenden Fragestellungen.

Abschnitt 1.1 dient als Grundlage für die gesamte Arbeit: Es werden verschiedene Möglichkeiten zur Realisierung von Algorithmen auf Quantenrechnern vorgestellt. Die verwendete formale und mathematische Modellierung erlaubt es, auftretende Szenarien in einer einheitlichen Sprache zu formulieren. Bei der Modellbildung wird zwischen der Beschreibung von Algorithmen und deren Erzeugung unterschieden. Einerseits sprechen wir von Zustandsübergangsoperatoren (Definition 1.1), die Äquivalenzklassen unitärer Transformationen und damit Algorithmen auf Quantenrechnern beschreiben, und andererseits sprechen wir von Implementierung (Definition 1.2) und Zerlegung (Definition 1.3), die verschiedene Möglichkeiten zur Erzeugung unitärer Transformationen bilden. Dies spiegelt die Tatsache wider, daß in der Literatur sowohl kontinuierliche als auch diskrete Modelle vorkommen. Teilweise werden diese unterschiedlichen Modelle in der Literatur nebeneinander oder sogar gleichzeitig verwendet. Deshalb betrachten wir auch den Fall der Zerlegung mit anschließender Implementierung der Zerlegungsschritte.

Als ein Beispiel für ein diskretes Modell diskutieren wir in Abschnitt 1.2 Quantenschaltkreise. Quantengatter (Definition 1.4) sind unitäre Transformationen, die auf einem Teilsystem des Quantensystems operieren. Sie bilden die Grundbausteine für Quantenschaltkreise. Die Wirkung der Quantengatter ist gegeben durch die Einbettung (Definition 1.6) der Quantengatter bzgl. der auf dem Quantensystem gewählten Tensorproduktstruktur (Definition 1.5). Wir definieren die Einbettung allgemein (und nicht nur für Qubitsysteme) durch die explizite Angabe der Wirkung der Transformation auf dem Gesamtsystem. Dies ermöglicht uns eine explizite und allgemeine Definition von Quantenschaltkreisen (Definition 1.7) unter Benutzung der Begriffe Zerlegung und Einbettung. In Abschnitt 1.3 führen wir Kontrollsysteme als ein Beispiel für ein kontinuierliches Modell ein. Insbesondere heben wir die Verbindungen zwischen der Universalität von Quantenschaltkreisen und der Kontrollierbarkeit von Kontrollsystemen hervor.

In den Abschnitten 1.4 und 1.5 behandeln wir Systeme von Einparameter-Gruppen und Einparameter-Halbgruppen in Bezug auf die Frage, unter welchen Bedingungen jede unitäre Transformation in ein Produkt mit einer endlichen und gleichmäßig beschränkten Anzahl von Faktoren zerlegt werden kann. Dabei sind die Faktoren Elemente der Einparameter-Gruppen bzw. Einparameter-Halbgruppen. Wir korrigieren einen Beweis

aus der Literatur (siehe Theorem 1.13) für die Tatsache, daß jedes Element einer reellen, endlichdimensionalen und zusammenhängenden Lie-Gruppe als ein endliches Produkt von Elementen einer Menge von Einparameter-Gruppen dargestellt werden kann, falls die Lie-Algebra der Lie-Gruppe durch die infinitesimalen Erzeuger der Einparameter-Gruppen erzeugt wird. Unter der zusätzlichen Bedingung, daß die betrachtete Lie-Gruppe kompakt ist, zeigen wir (siehe Theorem 1.17) dies auch für Einparameter-Halbgruppen. A priori wäre es möglich, daß zwar jedes Element einer Lie-Gruppe als endliches Produkt darstellbar wäre, daß es aber unabhängig vom gewählten Element keine gemeinsame und endliche obere Schranke für die Anzahl der Faktoren gäbe. Wir zeigen allgemein für Einparameter-Halbgruppen (siehe Theorem 1.19), daß es für reelle, endlichdimensionale, zusammenhängende und kompakte Lie-Gruppen eine gemeinsame und endliche obere Schranke für die Anzahl der Faktoren gibt. Für Zerlegungen von unitären oder speziell unitären Transformationen in Einparameter-Gruppen bzw. Einparameter-Halbgruppen erhalten wir insbesondere, daß eine Zerlegung mit einer endlichen und gleichmäßig beschränkten Anzahl der Faktoren möglich ist. Damit müssen wir in diesem Szenario keine unendlichen oder unbeschränkten Produkte zur Erzeugung von Algorithmen in Quantenrechnern betrachten.

Einen Überblick über die Geometrie der Ein-Qubit-Operationen geben wir in Abschnitt 2.1. Theorem 2.1 enthält einen algebraischen Beweis für die Darstellung von Rotationen als orthogonale Transformationen. Dieser Beweis ist durch die Arbeit von Euler motiviert. Weiter beweisen wir in Theorem 2.2 die Parametrisierung von Rotationen durch Angabe von drei Winkelparametern. Der Beweis erfolgt auf algebraische Weise und basiert auf Ideen von Euler. Die Existenz der 2-1-Abbildung von der Gruppe SU(2) auf die Gruppe SO(3) haben wir in Theorem 2.6 auf rein algebraische Weise gezeigt. Aufbauend auf der Beschreibung der Geometrie der Ein-Qubit-Operationen diskutieren wir in Abschnitt 2.2 ausgewählte Ansätze aus der Literatur zur Erzeugung von Ein-Qubit-Operationen.

In Abschnitt 2.3 entwickeln wir ein Werkzeug zur Bestimmung einer oberen Schranke für die Anzahl der Faktoren bei der Zerlegung von speziell unitären Transformationen auf Ein-Qubitsystemen in Einparameter-Gruppen. Dieses Werkzeug basiert auf einem Raffke-artigen Algorithmus, der schrittweise alle erreichbaren unitären Transformationen abdeckt. Diese Methode wird durch zwei Beispiele von zwei bzw. drei Einparameter-Gruppen vorgeführt.

In Kapitel 3 behandeln wir die Approximation von Quantenschaltkreisen. Eine erste Frage ist zu entscheiden (siehe Abschnitt 3.2), ob eine endlich erzeugte Untergruppe der speziell unitären Gruppe jede speziell unitäre Transformation approximieren kann. Wir vervollständigen einen Beweis aus der Literatur (siehe Theorem 3.4), daß für eine endlichdimensionale, reelle, halbeinfache und kompakte Lie-Gruppe eine endlich erzeugte Untergruppe genau dann dicht ist (d. h. jedes Element der Lie-Gruppe approximieren kann), falls die Nebenklassen der Untergruppe bzgl. jeder echten normalen und zusammenhängenden Lie-Untergruppe der Lie-Gruppe unendlich viele Elemente enthält und die Gruppenalgebren der Lie-Gruppe und der Untergruppe bzgl. einer speziellen Darstellung gleich sind. Die Bedingungen können mit Computeralgebrasystemen getestet werden, wobei aber teilweise Effizienzprobleme auftreten können.

Wir verallgemeinern in Abschnitt 3.3 eine aus der Literatur bekannte Bedingung für die effiziente (nicht-konstruktive) Approximation durch eine endlich erzeugte Untergrup-

pe von der speziell unitären Gruppe auf jede endlichdimensionale, zusammenhängende und kompakte reelle Lie-Gruppe. Dabei muß die gewählte endlich erzeugte Untergruppe eine spezielle spektrale Bedingung erfüllen (siehe Theorem 3.14). In diesem Zusammenhang bezeichnen wir eine Approximation als effizient, falls die Approximation in ein Produkt der Erzeuger der Untergruppe eine logarithmisch in der Genauigkeit der Approximation beschränkte Anzahl von Faktoren besitzt. Unter den genannten Voraussetzungen garantiert dies die Möglichkeit einer in der Genauigkeit der Approximation effizienten Approximation jeder unitären Transformation und damit auch von jedem Algorithmus auf einem Quantenrechner. Die aus der Literatur bekannte effiziente und konstruktive Approximation wird in Abschnitt 3.4 behandelt. Dabei wird darauf hingewiesen, daß es zur Zeit nicht geklärt ist, ob der (vorberechenbare) Schritt zur Erzeugung einer Startapproximation für die konstruktive Approximation eine endliche Komplexität besitzt.

Die Simulation von unitären Transformationen und Hamilton-Operatoren wird in Kapitel 4 behandelt. Bei der Simulation wird die Zeitentwicklung eines Hamilton-Operators ergänzt durch lokale unitäre Operationen, wobei die lokalen unitären Operationen in einer vernachlässigbaren Zeit angewendet werden können. Wir charakterisieren optimale und effiziente Möglichkeiten zur Erzeugung von unitären Transformationen. In Abschnitt 4.1 geben wir mathematische Definitionen für die globale (siehe Definition 4.1) und infinitesimale (siehe Definition 4.2) Simulation an, die die teilweise in der Literatur verwendeten verbalen Definitionen und deren Motivation formalisieren. Dabei unterscheidet sich die infinitesimale Simulation von der globalen Simulation dadurch, daß die infinitesimale Simulation nur in einer Umgebung der Identität der speziell unitären Gruppe definiert ist. Weiter beweisen wir (siehe Lemma 4.3), daß eine in der Literatur eingeführte Bedingung äquivalent zu unserer Definition der infinitesimalen Simulation ist. Die erwähnten Definitionen dienen einer exakten und expliziten Modellierung der zugrundeliegenden Fragestellungen. Eine Zusammenstellung der benötigten Lie-theoretischen Hilfsmittel ist in Abschnitt 4.2 zu finden.

In den Abschnitten 4.3 und 4.4 entwickeln wir eine einheitliche Theorie zur zeitoptimalen Simulation von unitären Transformationen und Hamilton-Operatoren auf Zwei-Qubit-Systemen. Wir merken hierbei an, daß die Menge der unitären Transformationen schon im Fall von zwei Qubits universell ist, d. h., daß alle unitären Transformationen unter Verwendung der unitären Transformationen auf zwei Qubits erzeugt werden können. Aus diesem Grund sind selbst Zwei-Qubit-Systeme von besonderem Interesse. Wir vereinheitlichen verschiedene aus der Literatur bekannte Ergebnisse mit Lie-theoretischen Methoden. Wir bestimmen in Theorem 4.17 ein konvexes Gebiet, so daß es für eine Simulation eines Hamilton-Operators in einer gewählten Zeit t notwendig und hinreichend ist, daß das $1/t$-fache des Hamilton-Operators in dem konvexen Gebiet enthalten ist. Unter Benutzung von Theorem 4.17 können wir einen Lie-theoretischen Beweis für das aus der Literatur bekannte Theorem 4.18 geben, wobei Theorem 4.18 eine einfachere notwendige und hinreichende Bedingung für die Simulierbarkeit eines Hamilton-Operators enthält. Die Nicht-Eindeutigkeit einer Lie-Gruppen-Zerlegung behandeln wir in den Lemmata 4.26 und 4.27 und insbesondere machen wir die Form der Nicht-Eindeutigkeit explizit. Diese Ergebnisse werden in einem Lie-thoeretischen Beweis (siehe Korollar 4.28) für ein aus der Literatur bekanntes Ergebnis verwendet, in dem einfach überprüfbare Bedingungen für die Simulation einer unitären Transformation in

einer gewählten Zeit genannt werden. Die Ergebnisse für Zwei-Qubit-Systeme basieren auf der speziellen Struktur eines symmetrischen Raumes, die in den Nebenklassen der speziell unitären Transformationen bzgl. der lokalen Operationen vorhanden ist.

Daran anschließend (siehe Abschnitt 4.5) betrachten wir die Simulation von unitären Transformationen auf Quantensystemen mit mehr als zwei Qubits. Im Gegensatz zu Zwei-Qubit-Systemen ist es in diesem Fall (bisher) nicht möglich, notwendige und hinreichende Bedingungen für eine zeitoptimale Simulation anzugeben. Die spezielle Struktur des symmetrischen Raumes ist in diesem Fall für die Nebenklassen der speziell unitären Transformationen bzgl. der lokalen Operationen nicht mehr gegeben. Trotzdem können wir in Theorem 4.43 untere Schranken für die Zeitkomplexität bei der Simulation unitärer Transformationen beweisen. Diese Schranken basieren auf der Tatsache, daß bzgl. einer Menge, die die lokalen Operationen enthält, die Struktur des symmetrischen Raumes der Nebenklassen weiterhin gegeben ist. In Theorem 4.36 können wir diese Menge für den Fall einer geraden und einer ungeraden Anzahl von Qubits bestimmen. Ferner können wir die den Simulationsergebnissen zugrundeliegende Struktur der symmetrischen Räume auch in speziellen Verschränkungsmaßen identifizieren (siehe Abschnitt 4.7).

Motiviert von den Ergebnissen zur Simulation analysieren wir die Struktur der Nebenklassen bzgl. den lokalen Operationen in Kapitel 5 genauer. Hierbei nimmt die Entwicklung der Analysemethoden einen großen Raum ein. In Abschnitt 5.1 führen wir einige Grundbegriffe in Bezug auf die Nebenklassen ein. Die Grundlage für unsere Analyse bildet die de-Rham-Kohomologie. Die de-Rham-Kohomologie ist durch alternierende Invarianten der Nebenklassen gegeben und beschreibt topologische Eigenschaften. Wir definieren die de-Rham-Kohomologie formal in Abschnitt 5.2 unter Benutzung der Theorie der Differentialformen, wobei wir die benötigten Aspekte der Theorie systematisch einführen. Die Methoden zur Berechnung der de-Rham-Kohomologie der Nebenklassen stellen wir in Abschnitt 5.4 zusammen. Dabei liegt unser Augenmerk auf der expliziten Berechnung mit Hilfe von Computeralgebrasystemen. Wir führen die Rechnungen exemplarisch für den Fall von Zwei-Qubit-Systemen (siehe Abschnitt 5.5) und Drei-Qubit-Systemen (siehe Abschnitt 5.6) aus. Schon im Fall von drei Qubits, für den die Struktur des symmetrischen Raumes nicht mehr gegeben ist, spiegelt sich die komplexere Struktur der Nebenklassen in den Invarianten wider.

In Zukunft können insbesondere zwei Aspkte für die effiziente (oder optimale) Erzeugung von unitären Transformationen eine besondere Rolle spielen. In erster Linie ist die detaillierte Bestimmung der Struktur der verbundenen Kontrollprobleme von Bedeutung. Wir haben in dieser Arbeit aufgezeigt, daß dabei die Struktur der Nebenklassen der unitären Transformationen bzgl. der lokalen Operationen ein wichtiges Beispiel ist. Verbindungen zur Beschreibung und Analyse der Verschränkung von Quantensystemen ergeben sich dadurch, daß die Nebenklassen nicht-lokale Eigenschaften von unitären Transformationen erfassen. Durch die Beziehung zwischen Zuständen und Transformationen spiegeln sich die nicht-lokalen Eigenschaften der Transformationen auch in den nicht-lokalen Eigenschaften der Zustände wider. Und mit der Nicht-Lokalität behandeln wir eine zentrale Fragestellung der Quantenmechanik und der Quanteninformatik. Für die Strukturanalyse benötigen wir weitere und effizientere Werkzeuge. Dabei müssen wir lernen, mit der kombinatorischen Explosion umzugehen, die bei den expliziten Rechnungen auftritt und in der Hochdimensionalität der Kontrollprobleme begründet ist.

In zweiter Linie müssen wir (besser) verstehen, auf welche Weise die Struktureigenschaften wie z. B. Invarianten dafür genutzt werden können, die betrachteten Kontrollprobleme zu lösen. Hierbei treten die Kontrollprobleme oft in der Form von Differentialgleichungen auf. Die Lösbarkeit von (Systemen von) Differentialgleichungen mittels algebraischen Methoden bildet dabei eine Hauptforschungsrichtung und die grundlegende Motivation für die Lie-Theorie.

A. Lie-Theorie

In diesem Anhang werden einige Grundbegriffe aus der Lie-Theorie behandelt. Weitergehende Konzepte und Ergebnisse aus der Lie-Theorie werden bei Bedarf im Hauptteil dieser Arbeit eingeführt oder aus der umfangreichen Literatur zitiert. Als Referenz dienen uns teilweise die Arbeiten [Bou89b; Bou02; Bou05; OV90; Oni93; OV94]. Wir verweisen auch auf die Arbeiten [Che99; Che51; Che55; KN91; KN96; Loo69a; Loo69b; Jac79; Var84; Wol84; BD85; Sam99; HN91; Gil94; Bor98; DK00; Hel01; Kna02; Ros02; EOM02a; Arv03; TY05]. Wir betonen, daß wir in dieser Arbeit nur reelle und komplexe Lie-Gruppen und Lie-Algebren verwenden, die zugleich endlichdimensional sind.

A.1. Analytische Mannigfaltigkeiten

Wir folgen Referenz [Bou71b] und führen den Begriff der analytischen Mannigfaltigkeit ein. Sei im folgenden M eine Menge. Ein Banach-Raum ist ein Vektorraum über einem (Schief-)Körper $\mathbb{K}$ (mit einer nicht diskret-wertigen Betragsfunktion), der mit einer Norm versehen ist, so daß jede Cauchy-Folge bzgl. der Norm einen Grenzwert besitzt (vgl. [Bou87, Kap. I, §1.4, Def. 2] oder [Wal90, S. 15]). Eine Karte von M ist ein Tripel $c = (U, \phi, E)$, wobei U eine Teilmenge von M, E ein Banach-Raum und ϕ eine bijektive Abbildung von U auf eine offene Umgebung von E ist. Wir bezeichnen U als den Definitionsbereich der Karte c. Zwei Karten $c = (U, \phi, E)$ und $c' = (U', \phi', E')$ der Menge M sind kompatibel, falls

1. $\phi(U \cap U')$ (bzw. $\phi'(U \cap U')$) offen in E (bzw. E') ist und
2. die Abbildung $\phi \circ \phi'^{-1}$ (bzw. $\phi' \circ \phi^{-1}$) von $\phi'(U \cap U')$ nach $\phi(U \cap U')$ (bzw. von $\phi(U \cap U')$ nach $\phi'(U \cap U')$) $\mathbb{K}$-analytisch ist.

Dabei bezeichnen wir eine Abbildung f von einer offenen Teilmenge U eines Banach-Raumes E in einen Banach-Raum F als $\mathbb{K}$-analytisch in U, falls für jeden Punkt $a \in U$ eine konvergente Potenzreihe mit Grenzwert $f_a : E \to F$ existiert, so daß $f(a + x) = f_a(x)$ für alle Elemente x aus einer Umgebung der Null von E gilt. Ein Atlas einer Menge M ist eine Menge von Karten von M, so daß jede Karte zu jeder Karte kompatibel ist und daß M die Vereinigung der Definitionsbereiche aller Karten ist.

Definition A.1 (Analytische Mannigfaltigkeit (siehe [Bou71b, S. 35]))**.** Eine analytische $\mathbb{K}$-Mannigfaltigkeit ist eine Menge M versehen mit einer Äquivalenzklasse von Atlanten. Dabei sind zwei Atlanten $\mathcal{A}$ und $\mathcal{B}$ der Menge M äquivalent, falls $\mathcal{A} \cup \mathcal{B}$ auch ein Atlas von M ist.

Ein Atlas $\mathcal{A}$ wird als ein Atlas einer analytischen Mannigfaltigkeit M bezeichnet, falls $\mathcal{A}$ in der Äquivalenzklasse von Atlanten von M liegt. Weiter bezeichnen wir eine Karte eines Atlanten einer analytischen Mannigfaltigkeit M als Karte von M. Eine (reine)

analytische $\mathbb{K}$-Mannigfaltigkeit M hat die Dimension $n < \infty$, falls alle in Karten von M vorkommende Banachräume gleich $\mathbb{K}^n$ sind. In dieser Arbeit verwenden wir nur reell ($\mathbb{K} = \mathbb{R}$) und komplex ($\mathbb{K} = \mathbb{C}$) analytische Mannigfaltigkeiten endlicher Dimension. Falls M und N analytische $\mathbb{K}$-Mannigfaltigkeiten sind, dann ist $M \times N$ auch eine (eindeutige) analytische $\mathbb{K}$-Mannigfaltigkeit ([Bou71b, S. 44]). Wir bezeichnen nun eine Abbildung f von einer $\mathbb{K}$-Mannigfaltigkeit M in eine $\mathbb{K}$-Mannigfaltigkeit N als analytisch, falls sie stetig ist und falls für jede Karte (V, ψ, F) von N und für jede Karte (U, ϕ, E) von M die Abbildung $\psi \circ f \circ \phi^{-1}$ von der offenen Teilmenge $\phi(\{\, x \in U |\ f(x) \in V\})$ des Banach-Raumes E in den Banach-Raum F analytisch ist (vgl. [Bou71b, S. 38–39] und [Jän01, S. 3–5]).

Jede analytische $\mathbb{K}$-Mannigfaltigkeit M ist insbesondere ein topologischer Raum (siehe [Bou71b, S. 36, §5.1.6]). Ferner ist auch jede Teilmenge $N \subset M$ ein topologischer Unterraum (siehe [Bou89a, Kap. I, §3.1]) von M. Ein Homöomorphismus von einem topologischen Raum N auf einen topologischen Raum M ist eine bijektive Abbildung von N auf M, die die offenen Teilmengen von N auf die offenen Teilmengen von M abbildet (siehe [Bou89a, Kap. I, §1.1, Def. 3]). Wir erhalten folgende Definition einer Untermannigfaltigkeit:

Definition A.2 (Untermannigfaltigkeit ([Bou71b, S. 47–48, §5.8])**.** Sei N ein topologischer Unterraum der analytischen Mannigfaltigkeit M und f die (kanonische) injektive Abbildung von N nach M. Falls für jedes Element $x \in N$ eine offene Umgebung $V \subset N$ von x und eine Karte (U, ϕ, E) von M mit $f(V) \subset U$ existiert, so daß $\phi \circ f$ ein Homöomorphismus von V auf den Schnitt von $\phi(U)$ mit einem Untervektorraum von E ist, wobei der Untervektorraum abgeschlossen ist und ein topologisches Komplement besitzt, so bezeichnen wir N als eine Untermannigfaltigkeit von M.

Ein topologisches Komplement zu einem Unterverktorraum ist ein komplementärer Vektorraum, der abgeschlossen ist (vgl. [Bou87, Kap. I, §1.3, Remark]). Jeder abgeschlossene Untervektorraum eines Banach-Raumes mit endlicher Kodimension besitzt ein topologisches Komplement (siehe [Bou87, Kap. I, §2.3, Prop. 3], vgl. auch [Bou71b, S. 46]) und jeder endlicher Vektorraum über den reellen oder komplexen Zahlen ist abgeschlossen ([Bou87, Kap. I, §2.3, Kor. 1 zu Prop. 2]).

Wir führen den Begriff des Tangentialraumes einer analytischen Mannigfaltigkeit ein. Sei M eine analytische Mannigfaltigkeit und $x \in M$. Wir betrachten die Tupel (c, h), wobei $c = (U, \phi, E)$ eine Karte von M und h ein Element von E ist. Zwei solche Tupel (c, h) und (c', h') sind äquivalent, falls die Ableitung von $\phi' \circ \phi^{-1}$ am Punkt $\phi(x)$ das Element $h \in E$ auf das Element $h' \in E'$ abbildet. Dabei ist $\phi' \circ \phi^{-1}$ in einer Umgebung von $\phi(x)$ definiert.

Definition A.3 (Tangentialraum ([Bou71b, S. 41, §5.5.1]))**.** Ein Tangentialvektor an einem Punkt x einer analytischen Mannigfaltigkeit M ist eine Äquivalenzklasse von Tupeln der Form (c, h), wobei $c = (U, \phi, E)$ eine Karte von M und h ein Element von E ist. Der Tangentialraum $\mathrm{T}_x(M)$ an einem Punkt x einer analytischen Mannigfaltigkeit M ist die Menge aller Tangentialvektoren am Punkt x der Mannigfaltigkeit M.

A.2. Lie-Gruppen und Lie-Algebren

Definition A.4 (Lie-Gruppe ([Bou89b, Kap. III, §1.1, Def. 1]))**.** Eine Lie-Gruppe G über dem (Schief-)Körper $\mathbb{K}$ ist eine analytische $\mathbb{K}$-Mannigfaltigkeit mit einer Gruppenstruktur, so daß die Abbildung $(G, H) \mapsto GH^{-1}$ von der analytischen $\mathbb{K}$-Mannigfaltigkeit $\mathrm{G} \times \mathrm{G}$ in die analytische $\mathbb{K}$-Mannigfaltigkeit G analytisch ist.

Wir bezeichnen eine Lie-Gruppe als reell (bzw. komplex), falls $\mathbb{K} = \mathbb{R}$ (bzw. $\mathbb{K} = \mathbb{C}$) ist. Wir benötigen auch den Begriff der Lie-Untergruppe:

Definition A.5 (Lie-Untergruppe (siehe [Bou89b, Kap. III, §1.3, Def. 3]))**.** Sei G eine Lie-Gruppe. Eine Teilmenge H von G wird als Lie-Untergruppe von G bezeichnet, falls H sowohl eine Untergruppe von G als auch eine Untermannigfaltigkeit von G ist.

Eine Lie-Gruppe G gilt als auflösbar (siehe [EOM02e]), wenn die zugehörige Gruppe G auflösbar ist ([Bou74, Kap. I, §6.4, Def. 8]), d. h., es existiert ein $n \in \mathbb{N} \cup \{0\}$, so daß $\mathrm{G}^{(n)} = \{\mathrm{Id}\}$, wobei $\mathrm{G}^{(0)} := \mathrm{G}$ und $\mathrm{G}^{(n+1)} := \{GHG^{-1}H^{-1} \colon G, H \in \mathrm{G}^{(n)}\}$ gilt. Eine zusammenhängende Lie-Gruppe G gilt als halbeinfach, falls sie keine nichtrivialen Untergruppen enthält, die zusammenhängend, normal in G und auflösbar sind ([EOM02d]). Zusätzlich bezeichnen wir eine zusammenhängende Lie-Gruppe als einfach, falls sie keine nichtrivialen Untergruppen ($\neq \mathrm{G}$) enthält, die normal in G und zusammenhängend sind ([EOM02d]). Wir führen nun den Begriff der Lie-Algebra ein:

Definition A.6 (Lie-Algebra ([Bou89b, Kap. I, §1.2, Def. 1]))**.** Eine Algebra $\mathfrak{g}$ über einem (Schief-)Körper $\mathbb{K}$ ist eine Lie-Algebra über $\mathbb{K}$, falls ihre Multiplikation $(x, y) \mapsto [x, y]$ für alle $x, y, z \in \mathfrak{g}$ die folgenden Eigenschaften hat:

1. $[x, x] = 0$ und
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (Jacobi-Identität)

Der Tangentialraum $\mathrm{T}_e(M)$ an der Identität e der Lie-Gruppe G ist (bei geeigneter Wahl der Lie-Multiplikation auf $\mathrm{T}_e(M)$ (siehe [Bou89b, Kap. III, §3])) eine Lie-Algebra ([Bou89b, Kap. III, §3.7, Prop. 24]) und wird als die Lie-Algebra $\mathfrak{g}$ der Lie-Gruppe G bezeichnet ([Bou89b, Kap. III, §3.7, Def. 6]). In dieser Arbeit bezeichnen wir eine Lie-Gruppe z. B. mit G und die zugehörige Lie-Algebra mit $\mathfrak{g}$.

Die Abbildung $\mathrm{ad}_{\mathfrak{g}}(g)$ ([Bou89b, Kap. I, §1.2, Def. 2]) von der Lie-Algebra $\mathfrak{g}$ nach $\mathfrak{g}$ wird als die Abbildung $h \mapsto [g, h]$ definiert, wobei $h, g \in \mathfrak{g}$. Wir definieren die adjungierte Darstellung ([Bou89b, Kap. I, §3.1, Def. 1]) der Lie-Algebra $\mathfrak{g}$ mit Hilfe dieser Notation: $g \mapsto \mathrm{ad}_{\mathfrak{g}}(g)$. Bezeichne $\mathrm{ad}_{\mathfrak{g}}(\mathfrak{h})$ die Menge $\{\mathrm{ad}_{\mathfrak{g}}(h) \colon h \in \mathfrak{h}\}$ bezüglich eines Unterraumes $\mathfrak{h}$ der Lie-Algebra $\mathfrak{g}$. Wir führen nun auf der Lie-Algebra $\mathfrak{g}$ eine symmetrische Bilinearform, die sogenannte Killing-Form $B_{\mathfrak{g}}(g, h) := \mathrm{Tr}_{\mathfrak{g}}(\mathrm{ad}_{\mathfrak{g}}(g) \circ \mathrm{ad}_{\mathfrak{g}}(h))$ ein ([Bou89b, Kap. I, §3.6, Def. 4]).

Wir bezeichnen eine Unteralgebra $\mathfrak{h}$ einer Lie-Algebra $\mathfrak{g}$ genau dann als Ideal, falls die Gleichung $[\mathfrak{h}, \mathfrak{g}] := \{[h, g] \colon h \in \mathfrak{h}, g \in \mathfrak{g}\} \subset \mathfrak{h}$ gilt (vgl. [Bou89b, Kap. I, §1.3] oder [Jac79, S. 23]). Seien im folgenden alle Lie-Algebren bzgl. einem Körper $\mathbb{K}$ definiert. Eine Unteralgebra $\mathfrak{h}$ einer Lie-Algebra nennen wir auflösbar, falls ein $n \in \mathbb{N} \cup \{0\}$ existiert, so daß $\mathcal{D}^n(\mathfrak{h}) = \{0\}$, wobei $\mathcal{D}^0(\mathfrak{h}) := \mathfrak{h}$ und $\mathcal{D}^{n+1}(\mathfrak{h}) := [\mathcal{D}^n(\mathfrak{h}), \mathcal{D}^n(\mathfrak{h})]$ gilt (siehe

[EOM02c] oder [Jac79, S. 24]). Wir erhalten, daß die Summe zweier auflösbarer Ideale wieder ein auflösbares Ideal ist (siehe [Jac79, S. 24]). Wir schränken uns nun auf den Fall von endlichdimensionalen Lie-Algebren ein. Eine Lie-Algebra gilt als halbeinfach, falls sie keine auflösbare Ideale $\mathfrak{h} \neq \{0\}$ besitzt (siehe [EOM02b] oder [Jac79, S. 24]). Wir führen den Begriff des (auflösbaren) Radikals $\mathfrak{rad}(\mathfrak{g})$ einer Lie-Algebra $\mathfrak{g}$ als das maximale auflösbare Ideal von $\mathfrak{g}$ ein (siehe [EOM02f], [Jac79, S. 24] oder [Bou89b, Kap. I, §5.2, Def. 2]). Die Definition einer halbeinfachen Lie-Algebra $\mathfrak{g}$ ist also äquivalent dazu, daß $\mathfrak{rad}(\mathfrak{g}) = \{0\}$ gilt (vgl. [Jac79, S. 24]). Sei nun im folgenden $\mathbb{K}$ ein Körper der Charakteristik 0 (siehe z. B. [Bou74, Kap. I, §9, Übungsaufgabe 4]), d. h., $\mathbb{K}$ besitzt einen Unterkörper, der isomorph zu $\mathbb{Q}$ ist. Dies ist insbesondere der Fall, wenn z. B. $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ gilt.

Faktum A.7 ([Bou89b, Kap. I, §6.1, Def. 1 und Thm. 1])**.** Sei $\mathfrak{g}$ eine endlichdimensionale Lie-Algebra über einem Körper $\mathbb{K}$ der Charakteristik 0. Die folgenden Bedingungen sind äquivalent:

1. $\mathfrak{g}$ ist halbeinfach
2. das einzige kommutative Ideal von $\mathfrak{g}$ ist $\{0\}$
3. $\mathfrak{rad}(\mathfrak{g}) = \{0\}$
4. die Killing-Form $B_{\mathfrak{g}}$ von $\mathfrak{g}$ ist nicht entartet
   (d. h. $\{ g \in \mathfrak{g} |\ B_{\mathfrak{g}}(g, h) = 0$ für alle $h \in \mathfrak{g}\} = \{0\}$ (siehe z. B. [TY05, S. 234]))

Eine Lie-Algebra $\mathfrak{g}$ wird genau dann als einfach bezeichnet, falls $\{0\}$ und $\mathfrak{g}$ die einzigen Ideale von $\mathfrak{g}$ sind und $\mathfrak{g}$ zusätzlich nicht kommutativ ist ([Bou89b, Kap. I, §6.2, Def. 2]). Es gilt, daß jede einfache Lie-Algebra auch halbeinfach ist (siehe [Jac79, S. 24–25] und [Bou89b, Kap. I, §6.2]).

Sei nun im folgenden $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$. Für eine reelle oder komplexe Lie-Gruppe, die endlichdimensional ist, definieren wir das Radikal Rad(G) von G als die größte zusammenhänge Lie-Gruppe, die zugleich normal in G und auflösbar ist ([Bou89b, Kap. III, §9.7, Def. 1]). Diese Definition ist wohldefiniert, und die Lie-Algebra von Rad(G) ist das Radikal $\mathfrak{rad}(\mathfrak{g})$ der Lie-Algebra $\mathfrak{g}$ von G (siehe [Bou89b, Kap. III, §9.7, Def. 1] und [OV93, Thm. 5.11, S. 57]). Eine reelle oder komplexe Lie-Gruppe, die zusammenhängend und endlichdimensional ist, ist genau dann halbeinfach, falls $\mathrm{Rad}(G) = \{\mathrm{Id}\}$ oder äquivalent, falls die Lie-Algebra von G halbeinfach ist (vgl. [Bou89b, Kap. III, §9.7-8] oder [OV93, S. 57]).

A.3. Beispiele

Wir geben nun einige Beispiele von Lie-Gruppen und ihren Lie-Algebren an (vgl. z. B. [Kna02, S. 1–5]). Dabei ist die Lie-Multiplikation jeweils durch den Lie-Kommutator $(x, y) \mapsto [x, y] = xy - yx$ gegeben. Die allgemeine (komplex) lineare Gruppe $\mathrm{GL}(n, \mathbb{C})$ ist die Lie-Gruppe der invertierbaren komplexen $n \times n$-Matrizen. Die zugehörige Lie-Algebra $\mathfrak{gl}(n, \mathbb{C})$ ist die Menge der komplexen $n \times n$-Matrizen. Entsprechend ist die reell lineare Gruppe $\mathrm{GL}(n, \mathbb{R})$ die Lie-Gruppe der invertierbaren reellen $n \times n$-Matrizen und

die zugehörige Lie-Algebra $\mathfrak{gl}(n,\mathbb{R})$ die Menge der reellen $n\times n$-Matrizen. Die speziell linearen Gruppen

$$\mathrm{SL}(n,\mathbb{K}) = \{G \in \mathrm{GL}(n,\mathbb{K})|\ \det(G)=1\}$$

haben als Lie-Algebren

$$\mathfrak{sl}(n,\mathbb{K}) = \{x \in \mathfrak{gl}(n,\mathbb{K})|\ \mathrm{Tr}(x)=0\}.$$

Wir bezeichnen die Lie-Gruppe $\mathrm{SL}(n,\mathbb{C})$ als die (eigentliche) speziell lineare Gruppe. Die (verallgemeinerte) Rotationsgruppe

$$\mathrm{SO}(n) = \{G \in \mathrm{GL}(n,\mathbb{R})|\ GG^T=1 \text{ und } \det(G)=1\}$$

hat die Lie-Algebra

$$\mathfrak{so}(n) = \{x \in \mathfrak{gl}(n,\mathbb{R})|\ x+x^T=0\}.$$

Wir bezeichnen mit $G^\dagger$ die transponierte und komplex konjugierte Matrix einer Matrix G. Die unitäre Gruppe

$$\mathrm{U}(n) = \{G \in \mathrm{GL}(n,\mathbb{C})|\ GG^\dagger=1\}$$

und die speziell unitäre Gruppe

$$\mathrm{SU}(n) = \{G \in \mathrm{U}(n)|\ \det(G)=1\}$$

spielen in dieser Arbeit eine besondere Rolle. Die entsprechenden Lie-Algebren sind

$$\mathfrak{u}(n) = \{x \in \mathfrak{gl}(n,\mathbb{C})|\ x+x^\dagger=0\}$$

und

$$\mathfrak{su}(n) = \{x \in \mathfrak{u}(n)|\ \mathrm{Tr}(x)=0\}.$$

Die Lie-Gruppe $\mathrm{SU}(n)$ ist kompakt, einfach und halbeinfach (vgl. [Bou02, Kap. IX, §3.4]). Wir definieren auf der unitären Gruppe und der speziell unitären Gruppe die Topologie [Bou89a, S. 17], die von der folgenden Operatornorm induziert wird (vgl. z. B. [Gaa73, S. 58]): Bezeichne $\||\alpha\rangle\| := \sqrt{\langle\alpha|\alpha\rangle}$ die euklidische Norm des Zustandes $|\alpha\rangle$ und

$$\|U\| := \sup_{|\alpha\rangle\neq 0} \frac{\|U|\alpha\rangle\|}{\||\alpha\rangle\|}$$

die Operatornorm des unitären Operators U (vgl. auch [KSV02, S. 71]).

Lebenslauf

Persönliche Daten:

Name:	Robert Michael Zeier
Geburtsdaten:	20. August 1975 in Großau

Schulausbildung:

August 1982 – Juli 1986	Hans-Thoma-Grundschule in Karlsruhe
August 1986 – Juli 1993	Ludwig-Marum-Gymnasium in Pfinztal
August 1993 – Juni 1995	Fichte-Gymnasium in Karlsruhe
Juni 1995	Abitur

Studium:

September 1995 – Juli 2000	Studium der Informatik an der Universität Karlsruhe (TH)
Juli 1997	Vordiplom
Juli 2000	Diplom

Beruf:

seit September 2000	Wissenschaftlicher Mitarbeiter am Institut für Algorithmen und Kognitive Systeme an der Universität Karlsruhe (TH)

Eigene Veröffentlichungen

[1] Zeier, Robert: *Modellierung von Situationsfolgen.* 1999. – Universität Karlsruhe, Informatik, Studienarbeit

[2] Zeier, Robert: *Zum fehlertoleranten Rechnen mit Quantenzuständen.* 2000. – Universität Karlsruhe, Informatik, Diplomarbeit

[3] Janzing, D.; Wocjan, P.; Zeier, R.; Geiss, R.; Beth, Th.: Thermodynamic Cost of Reliability and Low Temperatures: Tightening Landauer's Principle and the Second Law. In: *International Journal of Theoretical Physics* 39 (2000), Nr. 12, S. 2717–2753

[4] Janzing, D.; Armknecht, F.; Zeier, R.; Beth, Th.: Quantum control without access to the controlling interaction. In: *Physical Review A* 65 (2002), Nr. 2, S. 022104

[5] Beth, Th.; Grassl, M.; Janzing, D.; Rötteler, M.; Wocjan, P.; Zeier, R.: Algorithms for Quantum Systems — Quantum Algorithms. In: Leuchs, Gerd (Hrsg.); Beth, Thomas (Hrsg.): *Quantum Information Processing.* Weinheim: Wiley-VCH, 2003, Kapitel 1, S. 1–13

[6] Zeier, Robert; Grassl, Markus; Beth, Thomas: Gate simulation and lower bounds on the simulation time. In: *Physical Review A* 70 (2004), Nr. 3, S. 032319

[7] Beth, Th.; Grassl, M.; Janzing, D.; Rötteler, M.; Wocjan, P.; Zeier, R.: Algorithms for Quantum Systems — Quantum Algorithms. In: Beth, Thomas (Hrsg.); Leuchs, Gerd (Hrsg.): *Quantum Information Processing.* 2. Auflage. Weinheim: Wiley-VCH, 2005, Kapitel 1, S. 1–13

Literaturverzeichnis

[ABO99] Aharonov, D.; Ben-Or, M.: *Fault-tolerant quantum computation with constant error rate*. 1999. – http://arxiv.org/quant-ph/9906129

[Abr67] Abraham, Ralph: *Foundations of mechanics*. New York: W. A. Benjamin, 1967

[AD04] Albertini, Francesca; D'Alessandro, Domenico: Control of the evolution of Heisenberg spin systems. *Math. Control Signal Systems* 10 (2004), Nr. 5, S. 497–504

[AF01] Albeverio, Sergio; Fei, Shao-Ming: A note on invariants and entanglements. *J. Opt. B* 3 (2001), S. 223–227

[Aha99] Aharonov, D.: *Noisy quantum computation*. Jerusalem, The Hebrew University, Diss., 1999

[Aha03] Aharonov, Dorit: *A simple proof that Toffoli and Hadamard are quantum universal*. 2003. – http://arxiv.org/quant-ph/0301040

[AI95] de Azcárraga, José A.; Izquierdo, José M.: *Lie groups, Lie algebras, cohomology and some applications in physics*. Cambridge: Cambridge University Press, 1995

[Alt89] Altmann, Simon L.: Hamilton, Rodrigues, and the quaternion scandal. *Math. Mag.* 62 (1989), Nr. 5, S. 291–308

[Alt02] Altafini, Claudio: Controllability of quantum mechanical systems by root space decomposition of $\mathfrak{su}(N)$. *J. Math. Phys.* 43 (2002), Nr. 5, S. 2051–2062

[Alt05] Altmann, Simon L.: *Rotations, quaternions, and double groups*. Korrigierte Auflage. Mineola: Dover, 2005

[AMR88] Abraham, R.; Marsden, J. E.; Ratiu, T.: *Manifolds, tensor analysis and applications*. Zweite Auflage. New York: Springer, 1988 (Applied mathematical sciences 75)

[And62] André, Michel: Cohomologie des algèbre différentielles oú opère une algèbre de Lie. *Tohoku Math. J., II. Ser.* 14 (1962), S. 263–311

[And89a] Ando, T.: Majorization, doubly stochastic matrices, and comparison of eigenvalues. *Linear Algebra Appl.* 118 (1989), S. 163–248

[And89b] Ando, T.: Majorizations and inequalities in matrix theory. *Linear Algebra Appl.* 199 (1989), S. 17–67

[Apo90] Apostol, T. M.: *Modular functions and Dirichlet series in number theory.* Zweite Auflage. New York: Springer, 1990

[Arv03] Arvanitoyeorgos, Andreas: *An introduction to Lie groups and the geometry of homogeneous spaces.* Providence: American Mathematical Society, 2003 (Student mathematical library 22)

[AS03] Aho, Alfred V.; Svore, Krysta M.: *Compiling quantum circuits using the palindrome transform.* 2003. – `http://arxiv.org/quant-ph/0311008`

[AS04] Agrachev, Andrei A. (Hrsg.); Sachkov, Yuri L. (Hrsg.): *Control theory from the geometric viewpoint.* Berlin: Springer, 2004 (Encyclopaedia of mathematical sciences 87)

[AU82] Alberti, Peter M.; Uhlmann, Armin: *Stochasticity and partial order.* Berlin: VEB Deutscher Verlag der Wissenschaften, 1982

[AVD01] Audenaert, Koenraad; Verstraete, Frank; De Moor, Bart: Variational characterizations of separability and entanglement of formation. *Phys. Rev. A* 64 (2001), Nr. 5, S. 052304

[Bab92] Babai, László: Deciding finiteness of matrix groups in Las Vegas polynomial time. In: *Proc. of the third annual ACM-SIAM symposium on discrete algorithms*, 1992, S. 33–40

[Bar95] Barenco, A.: A universal two-bit gate for quantum computation. *Proc. R. Soc. London, Ser. A* 449 (1995), S. 679–683

[BB02a] Brylinski, Jean-Luc; Brylinski, Ranee: Invariant polynomial functions on k qudits. In: [BC02], S. 277–286

[BB02b] Brylinski, Jean-Luc; Brylinski, Ranee: Universal quantum gates. In: [BC02], S. 101–116

[BB04] Bullock, Stephen S.; Brennen, Gavin K.: Canonical decompositions of n-qubit quantum computations and concurrence. *J. Math. Phys.* 45 (2004), Nr. 6, S. 2447–2467

[BBC+93] Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* 70 (1993), Nr. 13, S. 1895–1899

[BBC+95] Barenco, A.; Bennett, C. H.; Cleve, R.; DiVincenzo, D. P.; Margolus, N.; Shor, P.; Sleator, T.; Smolin, J. A.; Weinfurter, H.: Elementary gates for quantum computation. *Phys. Rev. A* 52 (1995), Nr. 5, S. 3457–3467

[BBPS96] Bennett, Charles H.; Bernstein, Herbert J.; Popescu, Sandu; Schumacher, Benjamin: Concentrating partial entanglement by local operations. *Phys. Rev. A* 53 (1996), Nr. 4, S. 2046–2052

[BBR93] Babai, L.; Beals, R.; Rockmore, D.: Deciding finiteness of matrix groups in deterministic polynomial time. In: Bronstein, M. (Hrsg.): *Proceedings of the 1993 international symposium on symbolic and algebraic computation*, ACM Press, 1993, S. 117–126

[BC02] Brylinski, Ranee K. (Hrsg.); Chen, Goong (Hrsg.): *Mathematics of quantum computation*. Bocata Raton: Chapman & Hall/CRC, 2002

[BC05] Boscain, Ugo; Chitour, Yacine: Time-optimal synthesis for left-invariant control systems on SO(3). *SIAM J. Control. Optim.* 44 (2005), Nr. 1, S. 111–139

[BCL+02] Bennett, C. H.; Cirac, J. I.; Leifer, M. S.; Leung, D. W.; Linden, N.; Popescu, S.; Vidal, G.: Optimal simulation of two-qubit Hamiltonians using general local operations. *Phys. Rev. A* 66 (2002), Nr. 1, S. 012305

[BCP97] Bosma, Wieb; Cannon, John J.; Playoust, Catherine: The Magma algebra system I: the user language. *J. Symbolic Comput.* 24 (1997), Nr. 3–4, S. 235–265

[BD85] Bröcker, Theodor; tom Dieck, Tammo: *Representations of compact Lie groups*. New York: Springer, 1985

[BDD+02] Bremner, M. J.; Dawson, C. M.; Dodd, J. L.; Gilchrist, A.; Harrow, A. W.; Mortimer, D.; Nielsen, M. A.; Osborne, T. J.: Practical scheme for quantum computation with any two-qubit entangling gate. *Phys. Rev. Lett.* 89 (2002), Nr. 24, S. 247902

[BDH+02] Badziag, Piotr; Deuar, Piotr; Horodecki, Michał; Horodecki, Paweł; Horodecki, Ryszard: Concurrence in arbitrary dimensions. *J. Mod. Opt.* 49 (2002), Nr. 8, S. 1289–1297

[BDNB04] Bremner, Michael J.; Dodd, Jennifer L.; Nielsen, Michael A.; Bacon, Dave: Fungible dynamics: there are only two types of entangling multiple-qubit interactions. *Phys. Rev. A* 69 (2004), Nr. 1, S. 012313

[BDSW96] Bennett, Charles H.; DiVincenzo, David P.; Smolin, John A.; Wootters, William K.: Mixed-state entanglement and quantum error correction. *Phys. Rev. A* 54 (1996), Nr. 5, S. 3824–3851

[Bea97] Beals, Robert: Towards polynomial time algorithms for matrix groups. In: Finkelstein, Larry (Hrsg.); Kantor, William M. (Hrsg.): *Groups and computation II*. Providence: American Mathematical Society, 1997 (Series in discrete mathematics and theoretical computer science 28), S. 31–54

[Ben73] Bennett, C. H.: Logical reversibility of computation. *IBM J. Res. Develop.* 17 (1973), S. 525–532

[Ber87a] Berger, Marcel: *Geometry.* Bd. I. Berlin: Springer, 1987

[Ber87b] Berger, Marcel: *Geometry.* Bd. II. Berlin: Springer, 1987

[BGJ+03] Beth, Th.; Grassl, M.; Janzing, D.; Rötteler, M.; Wocjan, P.; Zeier, R.: Algorithms for quantum systems — quantum algorithms. In: Leuchs, Gerd (Hrsg.); Beth, Thomas (Hrsg.): *Quantum information processing.* Weinheim: Wiley-VCH, 2003, Kapitel 1, S. 1–13

[BGJ+05] Beth, Th.; Grassl, M.; Janzing, D.; Rötteler, M.; Wocjan, P.; Zeier, R.: Algorithms for quantum systems — Quantum algorithms. In: Beth, Thomas (Hrsg.); Leuchs, Gerd (Hrsg.): *Quantum information processing.* Zweite Auflage. Weinheim: Wiley-VCH, 2005, Kapitel 1, S. 1–13

[Bha97] Bhatia, Rajendra: *Matrix analysis.* New York: Springer-Verlag, 1997

[BIM90] Bar-Itzhack, Itzhack Y.; Markley, F. L.: Minimal parameter solution of the orthogonal matrix differential equation. *IEEE Trans. Automat. Control* 35 (1990), Nr. 3, S. 315–317

[BK00] Brockett, Roger; Khaneja, Navin: On the stochastic control of quantum ensembles. In: Djaferis, Theodore E. (Hrsg.); Schick, Irvin C. (Hrsg.): *System theory: modeling, analysis and control.* Boston: Kluwer, 2000 (The Kluwer international series in engineering and computer science 518), S. 75–96

[BK05] Bravyi, Sergey; Kitaev, Alexei: Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A* 71 (2005), Nr. 2, S. 022316

[BL01] Barnum, H.; Linden, N.: Monotones and invariants for multi-particle quantum states. *J. Phys. A* 34 (2001), Nr. 35, S. 6787–6805

[BLT03] Briand, Emmanuel; Luque, Jean-Gabriel; Thibon, Jean-Yves: A complete set of covariants of the four qubit system. *J. Phys. A* 36 (2003), Nr. 38, S. 9915–9927

[BLTV04] Briand, Emmanuel; Luque, Jean-Gabriel; Thibon, Jean-Yves; Verstaete, Frank: The moduli space of three-qutrit states. *J. Math. Phys.* 45 (2004), Nr. 12, S. 4855–4867

[BM03] Bullock, S. S.; Markov, I. L.: Arbitrary two-qubit computation in 23 elementary gates. *Phys. Rev. A* 68 (2003), Nr. 1, S. 012318

[BM04] Bullock, S. S.; Markov, I. L.: Asymptotically optimal circuits for arbitrary n-qubit diagonal computations. *Quantum Inf. Comput.* 4 (2004), Nr. 1, S. 27–47

[BM05] Boscain, Ugo; Mason, Paolo: Time minimal trajectories for two-level quantum systems with drift. In: *Proceedings of the 44th IEEE conference on decision and control*, 2005, S. 3188–3193

[BM06] Boscain, Ugo; Mason, Paolo: Time minimal trajectories for a spin 1/2 particle in a magnetic field. *J. Math. Phys.* 47 (2006), Nr. 6, S. 062101

[BMP+99] Boykin, P. O.; Mor, T.; Pulver, M.; Roychowdhury, V.; Vatan, F.: On universal and fault-tolerant quantum computing: a novel basis and a new constructive proof of universality for Shor's basis. In: *Proc. of the 40th annual symposium on foundations of computer science*, 1999, S. 486–494

[BMR92] Braunstein, Samuel L.; Mann, A.; Revzen, M.: Maximal violation of Bell inequalities for mixed states. *Phys. Rev. Lett.* 68 (1992), Nr. 22, S. 3259–3261

[Bor53] Borel, Armand: Sur la cohomologie des espaces fibres principaux et des espaces homogenes de groupes de Lie compacts. *Ann. of Math.* 57 (1953), Nr. 1, S. 115–207

[Bor55] Borel, Armand: Topology of Lie groups and characteristic classes. *Bull. Am. Math. Soc.* 61 (1955), S. 397–432

[Bor98] Borel, Armand: *Semisimple groups and Riemannian symmetric spaces.* Hindustan Book Agency, 1998

[Bos96] Bosch, Siegfried: *Algebra.* Zweite Auflage. Berlin: Springer, 1996

[Bou71a] Bourbaki, N.: *Variétés différentielles et analytiques, Fascicule de résultats, Paragraphes 8 à 15.* Paris: Hermann, 1971 (Éléments de mathématique 36)

[Bou71b] Bourbaki, N.: *Variétés différentielles et analytiques, Fascicule de résultats, Paragraphes 1 à 7.* Zweite Auflage. Paris: Hermann, 1971 (Éléments de mathématique 33)

[Bou71c] Bourbaki, Nicolas: *Elemente der Mathematikgeschichte.* Göttingen: Vandenhoeck & Ruprecht, 1971 (Studia mathematica 23)

[Bou74] Bourbaki, Nicolas: *Algebra I: chapters 1–3.* Paris: Hermann, 1974

[Bou80] Bourbaki, N.: *Algèbre, Chapitre 10, Algèbre homologique.* Neue Auflage. Paris: Masson, 1980

[Bou81] Bourbaki, N.: *Algèbre, Chapitres 4 à 7.* Paris: Masson, 1981

[Bou87] Bourbaki, N.: *Topological vector spaces.* Berlin: Springer, 1987

[Bou89a] Bourbaki, Nicolas: *General topology: chapters 1–4.* Berlin: Springer, 1989

[Bou89b] Bourbaki, Nicolas: *Lie groups and Lie algebras: chapters 1–3*. Berlin: Springer, 1989

[Bou02] Bourbaki, Nicolas: *Lie groups and Lie algebras: chapters 4–6*. Berlin: Springer, 2002

[Bou05] Bourbaki, Nicolas: *Lie groups and Lie algebras: chapters 7–9*. Berlin: Springer, 2005

[Bry02] Brylinski, Jean-Luc: Algebraic measures of entanglement. In: [BC02], S. 3–23

[BS80] Butkovskii, A. G.; Samoilenko, Yu. I.: Controllability of quantum objects. *Soviet Phys. Dokl.* 25 (1980), Nr. 1, S. 22–24

[BS05] Boya, Luis J.; Sudarshan, E. C. G.: Relation between rigid-body motion, isotropic cones, and spinors. *Found. Phys. Lett.* 18 (2005), Nr. 1, S. 53–63

[BT65] Borel, Armand; Tits, Jacques: Groupes réductifs. *Publ. Math. I.H.E.S.* 27 (1965), S. 55–151

[BW93] Becker, Thomas; Weispfenning, Volker: *Gröbner bases: a computational approach to commutative algebra*. New York: Springer, 1993 (Graduate texts in mathematics 141)

[BŻ06] Bengtsson, Ingemar; Życzkowski, Karol: *Geometry of quantum states: an introduction to quantum entanglement*. Cambridge: Cambridge University Press, 2006

[Cap02] Caparrini, Sandro: The discovery of the vector representation of moments and angular velocity. *Arch. Hist. Exact Sci.* 56 (2002), Nr. 2, S. 151–181

[Car28] Cartan, M. E.: Sur les numbres de Betti des espaces de groupes clos. *C. R. Acad. Sc.* 187 (1928), S. 196–198. – siehe auch [Car52, S. 999–1001]

[Car29] Cartan, Elie: Sur les invariants intégraux de certains espaces homogénes clos et les propriétés topologiques de ces espaces. *Ann. Soc. pol. Math.* 8 (1929), S. 181–225. – siehe auch [Car52, S. 1081–1125]

[Car36a] Cartan, Élie: La topologie des espaces représentatifs. *Enseign. Math.* 35 (1936), S. 177–200

[Car36b] Cartan, Élie: *La topologie des groupes de Lie*. Paris: Hermann, 1936 (Actualités scientifiques et industrielles 358). – siehe auch [Car36a] und [Car52, S. 1307–1330]

[Car37] Cartan, E.: La topologie des espaces homogènes clos. *Mém. Sémin. Anal. vect., Moscou* 4 (1937), S. 388–394. – siehe auch [Car52, 1331–1337]

[Car50a] Cartan, Henri: La transgression dans un groupe de Lie et dans un espace fibré principal. In: [Col50], S. 57–71. – siehe auch [GS99, S. 205–219]

[Car50b] Cartan, Henri: Notions d'algèbre différentielle; application aux groupes de Lie et aux variétés où opère un groupe de Lie. In: [Col50], S. 15–27. – siehe auch [GS99, S. 191–203]

[Car52] Cartan, Élie: *Œuvres complètes, Partie 1, Volume 2*. Paris: Gauthier-Villars, 1952

[Car58] Cartan, E.: *Leçons sur les invariants intégraux*. Paris: Hermann, 1958. – Nachdruck

[Cay45] Cayley, Arthur: On certain results relating to quaternions. *Philosphical Magazine, 3. Serie* 26 (1845), S. 141–145. – siehe auch [Cay89, S. 123-126]

[Cay89] Cayley, Arthur: *The collected mathematical papers of Arthur Cayley*. Bd. 1. Cambridge: Cambridge University Press, 1889

[CE48] Chevalley, Claude; Eilenberg, Samuel: Cohomology theory of Lie groups and Lie algebras. *Trans. Amer. Math. Soc.* 63 (1948), Nr. 1, S. 85–124

[CG89] Cheng, Hui; Gupta, K. C.: An historical note on finite rotations. *Trans. ASME J. Appl. Mech.* 56 (1989), Nr. 1, S. 139–145

[CH91] Collins, George E.; Hong, Hoon: Partial cylindrical algebraic decomposition for quantifier elimination. *J. Symbolic Comput.* 12 (1991), Nr. 3, S. 299–328

[Che51] Chevalley, Claude: *Théorie des groupes de Lie, tome II: Groupes algébriques*. Paris: Hermann, 1951 (Actualités scientifiques et industrielles 1152)

[Che52a] Chern, Shiing-shen: Differential geometry of fiber bundles. In: *Proc. Internat. Congr. Math.* Bd. 2, 1952, S. 397–411

[Che52b] Chevalley, C.: The Betti numbers of the exceptional simple Lie groups. In: *Proc. Internat. Congr. Math.* Bd. 2, 1952, S. 21–24

[Che55] Chevalley, Claude: *Théorie des groupes de Lie, tome III : Théorèmes généraux sur les algèbre de Lie*. Paris: Hermann, 1955 (Actualités scientifiques et industrielles 1226)

[Che72] Chern, Shiing-shen: Geometry of characteristic classes. In: *Proc. 13th Biennial Seminar, Canadian Math. Congress* Bd. 1, 1972. – siehe auch [Che79, S. 97–150], S. 1–40

[Che79] Chern, Shiing-shen: *Complex manifolds without potential theory*. Zweite Auflage. New York: Springer, 1979

[Che99] Chevalley, Claude: *Theory of Lie groups I*. Princeton University Press, 1999. – Nachdruck

[Che03] Chen, Hao: Necessary conditions for efficient simulation of Hamiltonians using local unitary operations. *Quantum Inf. Comput.* 3 (2003), Nr. 3, S. 249–257

[CHKO06] Carlini, Alberto; Hosoya, Akio; Koike, Tatsuhiko; Okudaira, Yosuke: Time-optimal quantum evolution. *Phys. Rev. Lett.* 96 (2006), Nr. 6, S. 060503

[CHN03] Childs, Andrew M.; Haselgrove, Henry L.; Nielsen, Michael A.: Lower bounds on the complexity of simulating quantum gates. *Phys. Rev. A* 68 (2003), Nr. 5, S. 052311

[Cho39] Chow, W.-L.: Über Systeme von linearen partiellen Differentialgleichungen erster Ordnung. *Math. Ann.* 117 (1939), S. 98–105

[CKW00] Coffman, Valerie; Kundu, Joydip; Wootters, William K.: Distributed entanglement. *Phys. Rev. A* 61 (2000), Nr. 5, S. 052306

[CLE85] Counsell, C.; Levitt, M. H.; Ernst, R. R.: Analytic theory of composite pulses. *J. Magn. Reson.* 63 (1985), Nr. 1, S. 133–141

[CLPS99] Carteret, H. A.; Linden, N.; Popescu, S.; Sudbery, A.: Multiparticle entanglement. *Found. Phys.* 29 (1999), Nr. 4, S. 527–552

[CLR90] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.: *Introduction to algorithms.* MIT Press and McGraw-Hill, 1990

[CLV04] Childs, A. M.; Leung, D. W.; Vidal, G.: Reversible simulation of bipartite product Hamiltonians. *IEEE Trans. Inf. Theory* 50 (2004), Nr. 6, S. 1189–1197

[Col50] *Colloque de topologie (espaces fibrés).* Liège: Georges Thone, 1950

[Col89] Colin de Verdière, Yves: Distribution de points sur une sphère (d'après Lubotzky, Phillips et Sarnak). *Séminaire Bourbaki* 41 (1989), Nr. 703, S. 83–93

[Cox89] Coxeter, H. S. M.: *Introduction to geometry.* Zweite Auflage. New York: John Wiley & Sons, 1989

[Cox98] Coxeter, H. S. M.: *Non-euclidean geometry.* Sechste Auflage. Washington, D.C.: Mathematical Association of America, 1998

[CS83] Crouch, P. E.; Silva Leite, F.: On the uniform finite generation of $SO(n, \mathbb{R})$. *Syst. Control Lett.* 2 (1983), S. 341–347

[CS00] Carteret, H. A.; Sudbery, A.: Local symmetry properties of pure three-qubit states. *J. Phys. A* 33 (2000), Nr. 28, S. 4981–5002

[CW95] Chau, H. F.; Wilczek, F.: Simple realization of the Fredkin gate using a series of two-body operators. *Phys. Rev. Lett.* 75 (1995), Nr. 4, S. 748–750

[Cyb01] Cybenko, Georg: Reducing quantum computations to elementary unitary operations. *Comput. Sci. Eng.* 3 (2001), Nr. 2, S. 27–32

[D'A00] D'Alessandro, D.: Algorithms for quantum control based on decompositions on Lie groups. In: *Proceedings of the 39th IEEE conference on decision and control*, 2000, S. 967–968

[D'A01] D'Alessandro, Domenico: Constructive controllability of one and two spin $\frac{1}{2}$ particles. In: *Proceedings of the American control conference*, 2001, S. 1715–1720

[D'A02] D'Alessandro, Domenico: Uniform finite generation of compact Lie groups. *Syst. Control Lett.* 47 (2002), S. 87–90

[D'A03] D'Alessandro, Domenico: Controllability of one spin and two intracting spins. *Math. Control Signal Systems* 16 (2003), Nr. 1, S. 1–25

[D'A04] D'Alessandro, Domenico: Optimal evaluation of generalized Euler angles with applications to control. *Automatica* 40 (2004), Nr. 11, S. 1997–2002

[Dav73] Davenport, Paul B.: Rotations about nonorthogonal axes. *AIAA J.* 11 (1973), Nr. 6, S. 853–857

[DBE95] Deutsch, D.; Barenco, A.; Ekert, A.: Universality in quantum computation. *Proc. R. Soc. London, Ser. A* 449 (1995), S. 669–677

[DC02] Dür, W.; Cirac, J. I.: Equivalence classes of non-local unitary operations. *Quantum Inf. Comput.* 2 (2002), Nr. 3

[DD00] D'Alessandro, Domenico; Dahleh, Mohammed: Optimal control of two-level quantum systems. In: *Proceedings of the American control conference*, 2000, S. 3893–3897

[DD01] D'Alessandro, Domenico; Dahleh, Mohammed: Optimal control of two-level quantum systems. *IEEE Trans. Automat. Control* 46 (2001), Nr. 6, S. 866–876

[Deu89] Deutsch, D.: Quantum computational networks. *Proc. R. Soc. London, Ser. A* 425 (1989), S. 73–90

[DFN85] Dubrovin, B. A.; Fomenko, A. T.; Novikov, S. P.: *Modern geometry — methods and applications II.* New York: Springer, 1985 (Graduate texts in mathematics 104)

[DFN90] Dubrovin, B. A.; Fomenko, A. T.; Novikov, S. P.: *Modern geometry — methods and applications III.* New York: Springer, 1990 (Graduate texts in mathematics 124)

[DHH+06] Dirr, G.; Helmke, U.; Hüper, K.; Kleinsteuber, M.; Liu, Y.: Spin dynamics: a paradigm for time optimal control on compact Lie groups. *J. Global Optim.* 35 (2006), Nr. 3, S. 443–474

[DHK04] Dirr, G.; Helmke, U.; Kleinsteuber, M.: Time optimal factorizations on compact Lie groups. *PAMM* 4 (2004), Nr. 1, S. 664–665

[DiV95] DiVincenzo, D. P.: Two-bit gates are universal for quantum computation. *Phys. Rev. A* 51 (1995), Nr. 2, S. 1015–1022

[DK00] Duistermaat, J. J.; Kolk, J. A. C.: *Lie groups.* Berlin: Springer, 2000

[DK02] Derksen, Harm; Kemper, Gregor: *Computational invariant theory.* Berlin: Springer, 2002 (Encyclopaedia of mathematical sciences 130)

[DN06] Dawson, Christopher M.; Nielsen, Michael A.: The Solovay-Kitaev algorithm. *Quantum Inf. Comput.* 6 (2006), Nr. 1, S. 81–95

[DNBT02] Dodd, Jennifer L.; Nielsen, Michael A.; Bremner, Michael J.; Thew, Robert T.: Universal quantum computation and simulation using any entangling Hamiltonian and local unitaries. *Phys. Rev. A* 65 (2002), Nr. 4, S. 040301(R)

[DS94] DiVincenzo, D. P.; Smolin, J.: Results on two-bit gate design for quantum computers. In: *Proc. of the workshop on physics and computation*, 1994, S. 14–23

[DST98] Day, Jane; So, Wasin; Thompson, Robert C.: The spectrum of a Hermitian matrix sum. *Linear Algebra Appl.* 280 (1998), S. 289–332

[Dup78] Dupont, Johan L.: *Curvature and characteristic classes.* Berlin: Springer, 1978 (Lecture notes in mathematics 640)

[Dup03] Dupont, Johan: *Fibre bundles and Chern-Weil theory.* Aarhus: University of Aarhus, Department of Mathematics, 2003 (Lecture Notes Series 69). – `http://www.imf.au.dk/publications/ln/2003/imf-ln-2003-69.pdf`

[DVC+01] Dür, W.; Vidal, G.; Cirac, J. I.; Linden, N.; Popescu, S.: Entanglement capabilities of nonlocal Hamiltonians. *Phys. Rev. Lett.* 87 (2001), Nr. 13, S. 137901

[Dyn57] Dynkin, E. B.: Topological characteristics of homomorphisms of compact Lie groups. *Am. Math. Soc., Transl., II. Ser.* 6 (1957), S. 301–342. – siehe auch [Dyn00, S. 317–358], für Kommentare siehe [Oni00]

[Dyn00] Dynkin, E. B.; Yushkevich, A. A. (Hrsg.); Seitz, G. M. (Hrsg.); Onishchik, A. L. (Hrsg.): *Selected papers of E. B. Dynkin with commentary.* Providence: American Mathematical Society, 2000

[EBW97] Ernst, Richard R.; Bodenhausen, Geoffrey; Wokaun, Alexander: *Principles of nuclear magnetic resonance in one and two dimensions.* Oxford: Clarendon Press, 1997. – Korrigierte Auflage

[Eis95] Eisenbud, David: *Commutative algebra with a view toward algebraic geometry.* New York: Springer, 1995 (Graduate texts in mathematics 150)

[EOM02a] Hazewinkel, Michiel (Hrsg.). *Encyclopaedia of mathematics*. `http://eom.springer.de`. 2002

[EOM02b] *Lie algebra, semi-simple*. Artikel in [EOM02a]. 2002

[EOM02c] *Lie algebra, solvable*. Artikel in [EOM02a]. 2002

[EOM02d] *Lie group, semisimple*. Artikel in [EOM02a]. 2002

[EOM02e] *Lie group, solvable*. Artikel in [EOM02a]. 2002

[EOM02f] *Radical of rings and algebras*. Artikel in [EOM02a]. 2002

[Eul71] Eulero, L.: Problema algebraicum ob affectiones prorsus singulares memorabile. *Novi commentarii academiae scientiarum Petropolitanae* 15 (1771), S. 75–106. – siehe auch [Eul21, S. 287–315]

[Eul76a] Eulero, L.: Formulae generales pro translatione quacunque corporum rigidorum. *Novi commentarii academiae scientiarum Petropolitanae* 20 (1776), S. 189–207. – siehe auch [Eul68, S. 84–98], deutsche Übersetzung in [Eul53, S. 557–570]

[Eul76b] Eulero, L.: Nova methodus motum corporum rigidorum determinandi. *Novi commentarii academiae scientiarum Petropolitanae* 20 (1776), S. 208–238. – siehe auch [Eul68, S. 99–125], deutsche Übersetzung in [Eul53, S. 571–595]

[Eul53] Euler, Leonhard; Wolfers, J. P. (Hrsg.): *Leonhards Euler's Mechanik oder analytische Darstellung der Wissenschaft von der Bewegung mit Anmerkungen und Erläuterungen*. Bd. 3. Greifswald: C. A. Koch's Verlagshandlung, 1853

[Eul62] Euler, Leonard: De motu corporum circa punctum fixum mobilium. In: [Eul68], S. 411–441. – Nachdruck des Orginals aus Opera postuma, Bd. 2, von 1862

[Eul21] Euleri, Leonhardi; Rudio, Ferdinand (Hrsg.); Krazer, Adolf (Hrsg.); Stäckel, Paul (Hrsg.): *Commentationes algebraicae ad theoriam aequationum pertinentes*. Leipzig und Berlin: B. G. Teubneri, 1921 (Opera Omnia, 1. Serie, Band 6)

[Eul45] Euleri, Leonhardi; Speiser, Andreas (Hrsg.): *Introductio in analysin infinitorum, tomus secondus*. Zürich und Leipzig: Orell Füssli, 1945 (Opera Omnia, 1. Serie, Band 9). – Nachdruck des Orginals von 1748, englische Übersetzung in [Eul90]

[Eul68] Euleri, Leonhardi; Blanc, Charles (Hrsg.): *Commentationes mechanicae ad theoriam corporum rigidorum pertinentes, volumen posterius*. Zürich: Orell Füssli, 1968 (Opera Omnia, 2. Serie, Band 9)

[Eul90] Euler: *Introduction to analysis of the infinite, book II.* New York: Springer, 1990

[Fan49] Fan, Ky: On a thoerem of Weyl concerning eigenvalues of linear transformations. I. *Proc. Natl. Acad. Sci. U.S.A.* 35 (1949), Nr. 11, S. 652–655

[Fey85] Feynman, R. P.: Quantum mechanical computers. *Opt. News* 11 (1985), Nr. 2, S. 11–20

[Fey86] Feynman, Richard P.: Quantum mechanical computers. *Found. Phys.* 16 (1986), Nr. 6, S. 507–531

[FKL03] Freedman, Michael H.; Kitaev, Alexei; Lurie, Jacob: Diameters of homogeneous spaces. *Math. Res. Lett.* 10 (2003), S. 11–20

[FLW02] Freedman, M. H.; Larsen, M. J.; Wang, Z.: Two-eigenvalue problem and density of Jones representation of braid groups. *Commun. Math. Phys.* 228 (2002), Nr. 1, S. 177–199

[FMI03] Fan, Heng; Matsumoto, Keiji; Imai, Hiroshi: Quantify entanglement by concurrence hierarchy. *J. Phys. A* 36 (2003), Nr. 14, S. 4151–4158

[For51] Ford, Lester R.: *Automorphic functions.* Zweite Auflage. New York: Chelsa, 1951

[Fra04] Frankel, Theodore: *The geometry of physics: an introduction.* Zweite Auflage. Cambridge: Cambridge University Press, 2004

[FT82] Fredkin, E.; Toffoli, T.: Conservative logic. *Int. J. Theor. Phys.* 21 (1982), Nr. 3/4, S. 219–253

[Ful00] Fulton, William: Eigenvalues, invariant factors, highest weights, and Schubert calculus. *Bull. Amer. Math. Soc.* 37 (2000), Nr. 3, S. 209–249

[Gaa73] Gaal, Steven A.: *Linear analysis and representation theory.* Berlin: Springer, 1973 (Die Grundlehren der mathematischen Wissenschaften 198)

[Gau00a] Gauss, Carl F.: Die Kugel. In: *Werke* [Gau00c], S. 351–356

[Gau00b] Gauss, Carl F.: Mutationen des Raumes. In: *Werke* [Gau00c], S. 357–362

[Gau00c] Gauss, Carl F.: *Werke.* Bd. 8. Leipzig: B. G. Teubner, 1900

[GC97] Gershenfeld, Neil A.; Chuang, Isaac L.: Bulk spin-resonance quantum computation. *Science* 275 (1997), Nr. 5298, S. 350–356

[Ger03] Gerjuoy, Edward: Lower bound on entanglement of formation for the qubit-qudit system. *Phys. Rev. A* 67 (2003), Nr. 5, S. 052308

[GHV72] Greub, Werner; Halperin, Stephen; Vanstone, Ray: *Connections, curvature, and cohomology.* Bd. I. New York: Academic Press, 1972

[GHV73] Greub, Werner; Halperin, Stephen; Vanstone, Ray: *Connections, curvature, and cohomology.* Bd. II. New York: Academic Press, 1973

[GHV76] Greub, Werner; Halperin, Stephen; Vanstone, Ray: *Connections, curvature, and cohomology.* Bd. III. New York: Academic Press, 1976

[Gil94] Gilmore, Robert: *Lie groups, Lie algebras, and some of their applications.* Malabar: Krieger Publishing, 1994. – Nachdruck

[GJS99] Gamburd, Alex; Jakobson, Dmitry; Sarnak, Peter: Spectra of elements in the group ring of SU(2). *J. Eur. Math. Soc.* 1 (1999), Nr. 1, S. 51–85

[GL53] Garnier, René (Hrsg.); Lévy, Jacques (Hrsg.): *Œuvres de Henri Poincaré.* Bd. VI. Paris: Gauthier-Villars, 1953

[Gol50] Goldstein, Herbert: *Classical mechanics.* Reading: Addison-Wesley, 1950

[Got69] Goto, Morikuni: On an arcwise connected subgroup of a Lie group. *Proc. Amer. Math. Soc.* 20 (1969), Nr. 1, S. 157–162

[Gra80] Gray, Jeremy J.: Olinde Rodrigues' paper of 1840 on transformation groups. *Arch. Hist. Exact Sci.* 21 (1979/1980), Nr. 4, S. 375–385

[Gra81] Graham, Alexander: *Kronecker products and matrix calculus: with applications.* Chichester: Ellis Horwood, 1981

[Gra01] Grassl, Markus: *Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen*, Universität Karlsruhe, Informatik, Diss., 2001

[Gra02] Grassl, Markus: *Entanglement and invariant theory.* 2002. – Quantum Computation and Information Seminar, UC Berkeley, `http://iaks-www.ira.uka.de/home/grassl/paper/MSRI_InvarTheory.pdf`

[GRB98] Grassl, Markus; Rötteler, Martin; Beth, Thomas: Computing local invariants of quantum-bit-systems. *Phys. Rev. A* 58 (1998), Nr. 3, S. 1833–1839

[Gru99] Gruska, Jozef: *Quantum computation.* London: McGraw-Hill, 1999

[GS99] Guillemin, Victor W.; Sternberg, Shlomo: *Supersymmetry and equivariant de Rham theory.* Berlin: Springer, 1999

[Gui80] Guichardet, A.: *Cohomologie des groupes topologiques et des algèbres de Lie.* Paris: Cedic/Fernand Nathan, 1980 (Textes mathématiques 2)

[Ham44] Hamilton, William R.: On quaternions; or on a new system of imaginaries in algebra. *Philosphical Magazine, 3. Serie* 25 (1844), S. 489–495

[Har01] Harrow, A.: *Quantum compiling.* 2001. – Bachelor Thesis, Massachusetts Insitute of Technology

[Hec80] Heckman, Gerrit J.: *Projections of orbits and asymptotic behaviour of multiplicities for compact Lie groups*, Leiden, Diss., 1980

[Hel01] Helgason, Sigurdur: *Differential geometry, Lie groups, and symmetric spaces*. Providence: American Mathematical Society, 2001. – Korrigierte Auflage

[HH02] Hughes, Richard (Hrsg.); Heinrichs, Todd (Hrsg.): *A quantum information science and technology roadmap*. Los Alamos National Laboratory. Technical report LA-UR-02-6900. 2002. – `http://qist.lanl.gov`

[HHL89] Hilgert, Joachim; Hofmann, Karl H.; Lawson, Jimmie D.: *Lie Groups, convex cones and semigroups*. Oxford: Clarendon, 1989

[Hil90] Hilbert, David: Ueber die Theorie der algebraischen Formen. *Math. Ann.* 26 (1890), S. 473–534

[Hir73] Hirschorn, Ronald: Topological semigroups, sets of generators, and controllability. *Duke Math. J.* 40 (1973), S. 937–947

[HM94] Helmke, U.; Moore, J. B.: *Optimization and dynamical systems*. London: Springer, 1994

[HN91] Hilgert, Joachim; Neeb, Karl-Hermann: *Lie-Gruppen und Lie-Algebren*. Braunschweig: Vieweg, 1991

[HN93] Hilgert, Joachim; Neeb, Karl-Hermann: *Lie semigroups and their applications*. Berlin: Springer, 1993 (Lecture notes in mathematics 1552)

[HNO03] Haselgrove, Henry L.; Nielsen, Michael A.; Osborne, Tobias J.: Practicality of time-optimal two-qubit Hamiltonian simulation. *Phys. Rev. A* 68 (2003), Nr. 4, S. 042303

[Hor62] Horn, Alfred: Eigenvalues of sums of hermitian matrices. *Pacific J. Math.* 12 (1962), S. 225–241

[HRC02] Harrow, A. W.; Recht, B.; Chuang, I. L.: Efficient discrete approximations of quantum gates. *J. Math. Phys.* 43 (2002), Nr. 9, S. 4445–4451

[HTC83] Huang, G. M.; Tarn, T. J.; Clark, J. W.: On the controllability of quantum-mechanical systems. *J. Math. Phys.* 24 (1983), Nr. 11, S. 2608–2618

[HVC02] Hammerer, K.; Vidal, G.; Cirac, J. I.: Charaterization of nonlocal gates. *Phys. Rev. A* 66 (2002), Nr. 6, S. 062321

[HW60] Hardy, G. H.; Wright, E. M.: *An introduction to the theory of numbers*. Vierte Auflage. Oxford: Clarendon Press, 1960

[HW68] Heberlen, U.; Waugh, J. S.: Coherent averaging effects in magnetic resonance. *Phys. Rev.* 175 (1968), Nr. 2, S. 453–467

[HW97] Hill, Scott; Wootters, William K.: Entanglement of a pair of quantum bits. *Phys. Rev. Lett.* 78 (1997), Nr. 26, S. 5022–5025

[Isi95] Isidori, A.: *Nonlinear control systems*. Dritte Auflage. Berlin: Springer, 1995

[Iva01] Ivanyos, Gábor: Deciding finiteness for matrix groups over function fields over finite fields. *Israel J. Math.* 124 (2001), S. 185–188

[Jac84a] Jacobi, C. G. J.: *Bemerkungen zu einer Abhandlung Euler's ueber die orthogonale Substitution*. 1884. – siehe [Jac84b, S. 601–609]

[Jac84b] Jacobi, C. G. J.; Weierstrass, K. (Hrsg.): *Gesammelte Werke*. Bd. 3. Berlin: Georg Reimer, 1884

[Jac79] Jacobson, Nathan: *Lie algebras*. Korrigierte Auflage. New York: Dover, 1979

[Jak02] Jakubczyk, Bronisław: Introduction to geometric nonlinear control; controllability and Lie bracket. In: Agrachev, A. A. (Hrsg.): *Mathematical control theory*. Trieste: The Abdus Salam International Centre for Theoretical Physics, 2002 (ICTP lecture notes series VIII). – `http://www.ictp.trieste.it/~pub_off/lectures/vol8.html`, S. 107–168

[Jän01] Jänich, Klaus: *Vector analysis*. Springer, 2001

[Jau68] Jauch, Josef M.: *Foundations of quantum mechanics*. Reading: Addison-Wesley, 1968

[JB01] Janzing, D.; Beth, Th.: Complexity measure for continuous time quantum algorithms. *Phys. Rev. A* 64 (2001), S. 022301

[Jea04] Jeandel, Emmanuel: Universality in quantum computation. In: Diaz, Josep (Hrsg.); Karhumäki, Juhani (Hrsg.); Lepistö, Arto (Hrsg.); Sannella, Donald (Hrsg.): *Proc. of the 31st international colloquium on automata, languages and programming*. Berlin: Springer, 2004 (Lecture notes in computer science 3142), S. 793–804

[Jea05] Jeandel, Emmanuel: *Techniques algébriques en calcul quantique*, ENS Lyon, Diss., 2005

[JK99] Jones, J. A.; Knill, E.: Efficient refocusing of one-spin and two-spin interactions for NMR quantum computation. *J. Magn. Reson.* 141 (1999), Nr. 2, S. 322–325

[JS72] Jurdjevic, Velmir; Sussmann, Héctor J.: Control systems on Lie groups. *J. Diff. Eq.* 12 (1972), S. 313–329

[JSST03] Jaeger, Gregg; Sergienko, Alexander V.; Saleh, Bahaa E.; Teich, Malvin C.: Entanglement, mixedness, and spin-flip symmetry in multiple-qubit systems. *Phys. Rev. A* 68 (2003), Nr. 2, S. 022318

[JTFS+03] Jaeger, Gregg; Teodorescu-Frumosu, Mihail; Sergienko, Alexander; Saleh, Bahaa E. A.; Teich, Malvin C.: Multiphoton Stokes-parameter invariant for entangled states. *Phys. Rev. A* 67 (2003), Nr. 3, S. 032307

[Jur97] Jurdjevic, V.: *Geometric control theory.* Cambridge: Cambridge University Press, 1997

[JWB02] Janzing, Dominik; Wocjan, Pawel; Beth, Thomas: Complexity of decoupling and time-reversal for n spins with pair-interactions: arrow of time in quantum control. *Phys. Rev. A* 66 (2002), Nr. 4, S. 042311

[KBG01] Khaneja, N.; Brockett, R.; Glaser, S.: Time optimal control in spin systems. *Phys. Rev. A* 63 (2001), Nr. 3, S. 032308

[KC01] Kraus, B.; Cirac, J. I.: Optimal creation of entanglement using a two-qubit gate. *Phys. Rev. A* 63 (2001), Nr. 6, S. 062309

[KG01] Khaneja, Navin; Glaser, Steffen J.: Cartan decomposition of $SU(2^n)$ and control of spin systems. *Chem. Phys.* 267 (2001), Nr. 1–3, S. 11–23

[KGB02] Khaneja, Navin; Glaser, Steffen J.; Brockett, Roger: Sub-Riemannian geometry and time optimal control of three spin systems: quantum gates and coherence transfer. *Phys. Rev. A* 65 (2002), Nr. 3, S. 032301

[Kha00] Khaneja, Navin: *Geometric control in classical and quantum systems*, Harvard University, Applied Mathematics, Diss., 2000

[Kit97] Kitaev, A. Y.: Quantum computations: algorithms and error correction. *Russian Math. Surveys* 52 (1997), Nr. 6, S. 1191–1249

[Kle79] Klein, Felix: *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert.* Berlin: Springer, 1979 (Grundlehren der mathematischen Wissenschaft 24/25). – Nachdruck

[Kle93] Klein, Felix; Slodowy, Peter (Hrsg.): *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade.* Basel: Birkhäuser, 1993. – Nachdruck

[Kly98] Klyachko, A. A.: Stable bundles representation theory and Hermitian matrices. *Selecta Math. (N.S.)* 4 (1998), S. 419–445

[KLZ96] Knill, E.; Laflamme, R.; Zurek, W.: *Accuracy threshold for quantum computation.* 1996. – `http://arxiv.org/quant-ph/9610011`

[KLZ98a] Knill, E.; Laflamme, R.; Zurek, W. H.: Resilient quantum computation. *Science* 273 (1998), Nr. 1, S. 342–345

[KLZ98b] Knill, E.; Laflammme, R.; Zurek, W. H.: Resilient quantum computation: error models and thresholds. *Proc. R. Soc. London, Ser. A* 454 (1998), S. 365–384

[KN91] Kobayashi, Shoshichi; Nomizu, Katsumi: *Foundations of differential geometry.* Bd. 1. New York: Wiley, 1991

[KN96] Kobayashi, Shoshichi; Nomizu, Katsumi: *Foundations of differential geometry.* Bd. 2. New York: Wiley, 1996

[Kna02] Knapp, Anthony W.: *Lie groups beyond an introduction.* Zweite Auflage. Boston: Birkhäuser, 2002

[Kni95] Knill, E.: *Approximation by quantum circuits.* 1995. – `http://arxiv.org/quant-ph/9508006`

[Knu00] Knutson, Allen: The symplectic and algebraic geometry of Horn's problem. *Linear Algebra Appl.* 319 (2000), S. 61–81

[Kos50a] Koszul, J. L.: Sur un type d'algèbre différentielles en rapport avec la transgression. In: [Col50], S. 73–81

[Kos50b] Koszul, Jean-Louis: Homologie et cohomologie des algèbres de Lie. *Bull. Soc. Math. Fr.* 78 (1950), S. 65–127

[Kos73] Kostant, Bertram: On convexity, the Weyl group and the Iwasawa decomposition. *Ann. Sci. École Norm. Sup.* 4 (1973), Nr. 6, S. 413–455

[KR01] Kaloshin, V.; Rodnianski, I.: Diophantine properties of elements of SO(3). *GAFA, Geom. funct. anal.* 11 (2001), Nr. 5, S. 953–970

[Kre74] Krener, Arthur J.: A generalization of Chow's theorem and the bang-bang theorem to nonlinear control problems. *SIAM J. Control* 12 (1974), Nr. 1, S. 43–52

[KSV02] Kitaev, A. Y.; Shen, A. H.; Vyalyi, M. N.: *Classical and quantum computation.* American Mathematical Society, 2002

[KT99] Knutson, Allen; Tao, Terence: The honeycomb model of $GL_n(\mathbb{C})$ tensor products I: proof of the saturation conjecture. *J. Amer. Math. Soc.* 12 (1999), Nr. 4, S. 1055–1090

[Kun01] Kung, Sidney H.: Proof without words: the Weierstrass substitution. *Mathematics Magazine* 74 (2001), Nr. 5, S. 393

[KW06] King, Roland C.; Welsh, Trevor A.: Qubits and invariant theory. *J. Phys.: Conf. Ser.* 30 (2006), S. 1–8

[LBŻW03] Loziński, A.; Buchleitner, A.; Życzkowski, K.; Wellens, T.: Entanglement of $2 \times K$ quantum systems. *Europhys. Lett.* 62 (2003), Nr. 2, S. 168–174

[LCYY00] Leung, Debbie W.; Chuang, Issac L.; Yamaguchi, Fumiko; Yamamoto, Yoshihisa: Efficient implementation of coupled logic gates for quantum computation. *Phys. Rev. A* 61 (2000), Nr. 4, S. 042310

[Leu02] Leung, Debbie W.: Simulation and reversal of n-qubit Hamiltonians using Hadamard matrices. *J. Mod. Opt.* 49 (2002), Nr. 8, S. 1199–1217

[Lév52] Lévy, Jacques (Hrsg.): *Œuvres de Henri Poincaré.* Bd. VII. Paris: Gauthier-Villars, 1952

[Lev86] Levitt, Malcom H.: Composite pulses. *Progr. Nucl. Magn. Reson. Spectrosc.* 18 (1986), Nr. 2, S. 61–122

[Lev96] Levitt, Malcolm H.: Composite pulses. In: Grant, David M. (Hrsg.); Harris, Robin K. (Hrsg.): *Encyclopedia of nuclear magnetic resonance* Bd. 2. Chichester: John Wiley & Sons, 1996, S. 1396–1411

[Lid82] Lidskii, B. V.: Spectral polyhedron of a sum of two hermitian matrices. *Funct. Anal. Appl.* 16 (1982), Nr. 2, S. 139–140

[LKC+02] Laflamme, Raymond; Knill, Emanuel; Cory, David G.; Fortunato, Evan M.; Havel, Timothy F.; Miquel, Cesar; Martinez, Rudy; Negrevergne, Camille J.; Ortiz, Gerardo; Pravia, Marco A.; Sharf, Yehuda; Sinha, Suddhasattwa; Somma, Rolando; Viola, Lorenza: NMR and quantum information processing. *Los Alamos Science* (2002), Nr. 27, S. 227–259

[Llo95] Lloyd, S.: Almost any quantum logic gate is universal. *Phys. Rev. Lett.* 75 (1995), Nr. 2, S. 346–349

[Llo96] Lloyd, S.: Universal quantum simulators. *Science* 273 (1996), S. 1073–1078

[Loo69a] Loos, Ottmar: *Symmetric spaces I: general theory.* New York: W. A. Benjamin, 1969

[Loo69b] Loos, Ottmar: *Symmetric spaces II: compact spaces and classification.* New York: W. A. Benjamin, 1969

[Low71] Lowenthal, F.: Uniform finite generation of the rotation group. *Rocky Mountain J. Math.* 1 (1971), Nr. 4, S. 575–586

[LP98] Linden, N.; Popescu, S.: On multi-particle entanglement. *Fortschr. Phys.* 46 (1998), Nr. 4–5, S. 567–578

[LPS86] Lubotzky, A.; Phillips, R.; Sarnak, P.: Hecke operators and distributing points on the sphere I. *Commun. Pure App. Math.* 39 (1986), S. S149–S186

[LPS87] Lubotzky, A.; Phillips, R.; Sarnak, P.: Hecke operators and distributing points on S^2 II. *Commun. Pure App. Math.* 40 (1987), Nr. 4, S. 401–420

[LPS99] Linden, N.; Popescu, S.; Sudbery, A.: Nonlocal parameters for multiparticle density matrices. *Phys. Rev. Lett.* 83 (1999), Nr. 2, S. 243–247

[LT03] Luque, Jean-Gabriel; Thibon, Jean-Yves: Polynomial invariants of four qubits. *Phys. Rev. A* 67 (2003), Nr. 4, S. 042303

[LT06] Luque, Jean-Gabriel; Thibon, Jean-Yves: Algebraic invariants of five qubits. *J. Phys. A* 39 (2006), Nr. 2, S. 371–377

[Lub94] Lubotzky, Alexander: *Discrete groups, expanding graphs and invariant measures*. Basel: Birkhäuser, 1994 (Progress in mathematics 125)

[Mak03] Makhlin, Yuriy: Nonlocal properties of two-qubit gates and mixed states, and the optimization of quantum computations. *Quant. Inf. Proc.* 1 (2003), Nr. 4, S. 243–252

[Mal00] Maltese, Giulio: On the relativity of motion in Leonhard Euler's science. *Arch. Hist. Exact Sci.* 54 (2000), Nr. 4, S. 319–348

[Map05] Maplesoft. *Maple 10*. 2005

[May60] Mayer, Arthur: Rotations and their algebra. *SIAM Rev.* 2 (1960), Nr. 2, S. 77–122

[MCB05] Mandilara, A.; Clark, J. W.; Byrd, M. S.: Elliptical orbits in the Bloch sphere. *J. Opt. B* 7 (2005), Nr. 10, S. S277–S282

[Mes61] Messiah, Albert: *Quantum mechanics*. Bd. I. Amsterdam: North-Holland, 1961

[MO79] Marshall, Albert W.; Olkin, Ingram: *Inequalities: theory of majorization and its applications*. New York: Academic Press, 1979

[Mos57] Mostow, G. D.: On the fundamental group of a homogeneous space. *Ann. of Math.* 66 (1957), Nr. 2, S. 249–255

[MT97] Madsen, Ib; Tornehave, Jørgen: *Form calculus to cohomology: de Rham cohomology and characteristic classes*. Cambridge: Cambridge University Press, 1997

[MVBS04] Möttönen, Mikko; Vartiainen, Juha J.; Bergholm, Ville; Salomaa, Martti M.: Quantum circuits for general multiqubit gates. *Phys. Rev. Lett.* 93 (2004), Nr. 13, S. 130502

[MVL02] Masanes, Ll.; Vidal, G.; Latorre, J. I.: Time-optimal Hamiltonian simulation and gate synthesis using homogeneous local unitaries. *Quantum Inf. Comput.* 2 (2002), Nr. 4, S. 285–296

[MW02] Meyer, David A.; Wallach, Noland: Invariants for multiple qubits: the case of 3 qubits. In: [BC02], S. 77–97

[Nak90] Nakahara, Mikio: *Geometry, topology and physics.* London: Institute of Physics, 1990

[NBD+02] Nielsen, Michael A.; Bremner, Michael J.; Dodd, Jennifer L.; Childs, Andrew M.; Dawson, Christopher M.: Universal simulation of Hamiltonian dynamics for quantum systems with finite-dimensional state spaces. *Phys. Rev. A* 66 (2002), Nr. 2, S. 022317

[NC00] Nielsen, M. A.; Chuang, I. L.: *Quantum computation and quantum information.* Cambridge: Cambridge University Press, 2000

[NDGD06a] Nielsen, Michael A.; Dowling, Mark R.; Gu, Mile; Doherty, Andrew C.: Optimal control, geometry, and quantum computing. *Phys. Rev. A* 73 (2006), Nr. 6, S. 062323

[NDGD06b] Nielsen, Michael A.; Dowling, Mark R.; Gu, Mile; Doherty, Andrew C.: Quantum computation as geometry. *Science* 311 (2006), Nr. 5764, S. 1133–1135

[Neu69] Neudecker, H.: Some theorems on matrix differentiation with special reference to Kronecker matrix products. *J. Amer. Statist. Assoc.* 64 (1969), Nr. 327, S. 953–963

[Nie06] Nielsen, Michael A.: A geometric approach to quantum circuit lower bounds. *Quantum Inf. Comput.* 6 (2006), Nr. 3, S. 213–262

[NV01] Nielsen, Michael A.; Vidal, Guifré: Majorization and the interconversion of bipartite states. *Quantum Inf. Comput.* 1 (2001), Nr. 1, S. 76–93

[Ogi90] Ogilvy, C. S.: *Excursions in geometry.* Korrigierte Auflage. New York: Dover, 1990

[Olv99] Olver, Peter J.: *Classical invariant theory.* Cambridge: Cambridge University Press, 1999 (London mathematical society student texts 44)

[Oni93] Onishchik, A. L. (Hrsg.): *Lie groups and Lie algebras I.* New York: Springer, 1993 (Encyclopaedia of mathematical sciences 20)

[Oni94] Onishchik, Arkadi L.: *Topology of transitive transformation groups.* Leipzig: Johann Ambrosius Barth, 1994

[Oni00] Onishchik, A. L.: Comments on the paper "Topological characteristics of homomorphisms of compact Lie groups". In: [Dyn00], S. 359–361

[OV90] Onishchik, A. L.; Vinberg, E. B.: *Lie groups and algebraic groups.* Berlin: Springer, 1990

[OV93] Onishchik, A. L.; Vinberg, E. B.: Foundations of Lie theory. In: [Oni93], S. 1–94

[OV94] Onishchik, A. L. (Hrsg.); Vinberg, E. B. (Hrsg.): *Lie groups and Lie algebras III.* New York: Springer, 1994 (Encyclopaedia of mathematical sciences 41)

[PHG01] Philips, W. F.; Hailey, C. E.; Gebert, G. A.: *The effects of orthogonality error in aircraft flight simulation.* 2001. – 39th AIAA Aerospace Sciences Meeting & Exhibit

[Pio66] Pio, Richard L.: Euler angle transformations. *IEEE Trans. Automat. Control* AC11 (1966), Nr. 4, S. 707–715

[Poi90] Poincaré, Henri: Sur le problème des trois corps et les équations de la dynamique. *Acta Math.* 13 (1890), S. 1–270. – siehe auch [Lév52, S. 262–479]

[Poi95] Poincaré, Henri: Analysis situs. *J. Éc. Polyt.* 1 (1895), S. 1–121. – siehe auch [GL53, S. 193–288]

[PR97] Popescu, Sandu; Rohrlich, Daniel: Thermodynamics and the measure of entanglement. *Phys. Rev. A* 56 (1997), Nr. 5, S. 3319(R)–3321(R)

[PV94] Popov, V. L.; Vinberg, E. B.: Invariant theory. In: Parshin, A. N. (Hrsg.); Shafarevich, I. R. (Hrsg.): *Algebraic geometry IV.* Berlin: Springer, 1994 (Encyclopaedia of mathematical sciences 55), Kapitel II, S. 123–278

[QEP03] *QEPCAD Version B 1.21.* 2003. – `http://www.cs.usna.edu/~qepcad/B/QEPCAD.html`

[Rad52] Rado, R.: An inequality. *J. London Math. Soc.* 27 (1952), Nr. 105, S. 1–6

[Ram01a] Ramakrishna, V.: *Comments on quantum control by decomposition of* SU(2). 2001. – `http://arxiv.org/quant-ph/0106147`

[Ram01b] Ramakrishna, V.: Control of molecular systems with very few phases. *Chem. Phys.* 267 (2001), S. 25–32

[Rao96] Rao, K. N. S.: *Linear algebra and group theory for physicists.* New York: Wiley, 1996

[Ras69] Rashevskii, P. K.: The real cohomology of homogeneous spaces. *Russ. Math. Surv.* 24 (1969), Nr. 3, S. 23–95

[RBC+01] Rungta, Pranaw; Bužek, V.; Caves, Carlton M.; Hillery, M.; Milburn, G. J.: Universal state inversion and concurrence in arbitrary dimensions. *Phys. Rev. A* 64 (2001), Nr. 4, S. 042315

[RFRO00] Ramakrishna, V.; Flores, K. L.; Rabitz, H.; Ober, R.: Quantum control by decompositions of SU(2). *Phys. Rev. A* 62 (2000), Nr. 5, S. 053409

[Rha29] de Rham, M. G.: Intégrales multiples et analysis situs. *C. R. Acad. Sc.* 188 (1929), S. 1651–1652

[Rha31] de Rham, Georges: Sur l'analysis situs des vartiétés á n dimensions. *J. Math. Pures Appl., Série 9,* 10 (1931), S. 115–200

[Rob68] Roberson, Robert E.: Kinematical equations for bodies whose rotation is described by the Euler-Rodrigues parameter. *AIAA J.* 6 (1968), Nr. 5, S. 916–917

[Rod40] Rodrigues, M. O.: Des lois géométriques qui régissent les déplacements d'un système solide dans l'espace, et de la variation des coordonnées provenant de ces déplacements consideérés indépendamment des causes qui peuvent les produire. *J. de mathématiques pures et appliquées* 5 (1840), S. 380–440

[ROFR01] Ramakrishna, V.; Ober, R. J.; Flores, K. L.; Rabitz, H.: Constructive control of a spin system via periodic control. In: *Proceedings of the 40th IEEE conference on decision and control*, 2001, S. 292–297

[ROS+00] Ramakrishna, V.; Ober, R.; Sund, X.; Steuernagel, O.; Botina, J.; Rabitz, H.: Explicit generation of unitary transformations in a single atom or molecule. *Phys. Rev. A* 61 (2000), Nr. 3, S. 032106

[Ros02] Rossmann, Wulf: *Lie groups: an introduction through linear groups.* Oxford: Oxford University Press, 2002 (Oxford graduate texts in mathematics 5)

[Röt01] Rötteler, Martin: *Schnelle Signaltransformationen für Quantenrechner*, Universität Karlsruhe, Informatik, Diss., 2001

[Röt04] Rötteler, Martin: *Efficient decoupling schemes based on Hamilton cycles.* 2004. – `http://arxiv.org/quant-ph/0408078`

[Roz67] Rozenknop, I. Z.: Some problems and applications of homology theory of polynomial ideals. *Trans. Moscow math. Soc.* 13 (1967), S. 273–358

[RR96] Ramakrishna, V.; Rabitz, H.: Relation between quantum computing and quantum controllability. *Phys. Rev. A* 54 (1996), Nr. 2, S. 1715–1716

[RSD+95] Ramakrishna, V.; Salapaka, M. V.; Dahleh, M.; Rabitz, H.; Peirce, A.: Controllability of molecular systems. *Phys. Rev. A* 51 (1995), Nr. 2, S. 960–966

[RTB99] Rockmore, Daniel N.; Tan, Ki-Seng; Beals, Robert: Deciding finiteness for matrix groups over function fields. *Israel J. Math.* 109 (1999), S. 93–116

[RW06] Rötteler, Martin; Wocjan, Pawel: Equivalence of decoupling schemes and orthogonal arrays. *IEEE Trans. Inf. Theory* 52 (2006), Nr. 9, S. 4171–4181

[Sak94] Sakurai, J. J.: *Modern quantum mechanics*. Rev. Auflage. Reading: Addison-Wesley, 1994

[Sam52] Samelson, Hans: Topology of Lie groups. *Bull. Am. Math. Soc.* 58 (1952), S. 2–37

[Sam99] Samelson, Hans: *Notes on Lie algebras*. Zweite Auflage. New York: Springer, 1999

[Sar90] Sarnak, Peter: *Some applications of modular forms*. Cambridge: Cambridge University Press, 1990 (Cambridge tracts in mathematics 99)

[Sas99] Sastry, S.: *Nonlinear systems: analysis, stability, and control*. New York: Springer, 1999 (Interdisciplinary applied mathematics 10)

[SBM04] Shende, Vivek V.; Bullock, Stephen S.; Markov, Igor L.: Recognizing small-circuit structure in two-qubit operators. *Phys. Rev. A* 70 (2004), Nr. 1, S. 012310

[Sch79] Schwerdtfeger, Hans: *Geometry of complex numbers*. Korrigierte Auflage. New York: Dover, 1979

[Sch95] Schumacher, B.: Quantum coding. *Phys. Rev. A* 51 (1995), S. 2738–2747

[SD96] Smolin, J. A.; DiVincenzo, D. P.: Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate. *Phys. Rev. A* 53 (1996), Nr. 4, S. 2855–2856

[SH98] Schulte-Herbrüggen, T.: *Aspects and prospects of high-resolution NMR*, Eidgenössische Technische Hochschule Zürich, Diss., 1998

[Shi03] Shi, Y.: Both Toffoli and controlled-NOT need little help to do universal quantum computation. *Quantum Inf. Comput.* 3 (2003), Nr. 1, S. 84–92

[Sho96] Shor, P.: Fault-tolerant quantum computation. In: *Proc. of the 37th annual symposium on foundations of computer science*, 1996, S. 56–65

[SHSKG05] Schulte-Herbrüggen, T.; Spörl, A.; Khaneja, N.; Glaser, S. J.: Optimal control-based efficient synthesis of building blocks of quantum algorithms: a perspective from network complexity towards time complexity. *Phys. Rev. A* 72 (2005), Nr. 4, S. 042331

[Shu93] Shuster, Malcolm D.: A survey of attitude representations. *J. Astronaut. Sci.* 41 (1993), Nr. 4, S. 439–517

[Shu02] Shuster, Malcom D.: The kinematic equation for the rotation vector. *IEEE Trans. Aero. Elec. Sys.* 29 (2002), Nr. 1, S. 263–267

[Sil85a] Silva Leite, M. F.: On the uniform controllability of systems evolving on Lie groups. In: Jakubczyk, Bronislaw (Hrsg.); Respondek, Witold (Hrsg.); Tchon, Krzysztof (Hrsg.): *Geometric theory of nonlinear control systems*. Wroclaw: Technical University of Wroclaw, 1985, S. 207–218

[Sil85b] Silva Leite, M. F.: The uniform finite generation problem of Lie groups and its application to control systems. In: Brualdi, Richard A. (Hrsg.); Carlson, David H. (Hrsg.); Datta, Biswa N. (Hrsg.); Johnson, Charles R. (Hrsg.); Plemmons, Robert J. (Hrsg.): *Linear algebra and its role in systems theory*. Providence: American Mathematical Society, 1985 (Contemporary mathematics 47), S. 273–285

[Sil86] Silva Leite, F.: Uniform controllable sets of left-invariant vector fields on compact Lie groups. *Syst. Control Lett.* 6 (1986), S. 329–335

[Sil91a] Silva Leite, F.: Bounds on the order of generation of $SO(n, \mathbb{R})$ by one-parameter subgroups. *Rocky Mountain J. Math.* 21 (1991), Nr. 2, S. 879–911

[Sil91b] Silva Leite, F.: Corrections to: "Bounds on the order of generation of $SO(n, \mathbb{R})$ by one-parameter subgroups". *Rocky Mountain J. Math.* 21 (1991), Nr. 3, S. 1183–1188

[SJ72] Sussmann, Héctor J.; Jurdjevic, Velmir: Controllability of nonlinear systems. *J. Diff. Eq.* 12 (1972), S. 95–116

[SK03] Song, G.; Klappenecker, A.: Optimal realizations of controlled unitary gates. *Quantum Inf. Comput.* 3 (2003), Nr. 2, S. 139–156

[SM95] Schlienz, J.; Mahler, G.: Description of entanglement. *Phys. Rev. A* 52 (1995), Nr. 6, S. 4396–4404

[SM96] Schlienz, J.; Mahler, G.: The maximal entangled three-particle state is unique. *Phys. Lett. A* 224 (1996), Nr. 1–2, S. 39–44

[SM01] Stollsteimer, Marcus; Mahler, Günter: Suppression of arbitrary internal coupling in a quantum register. *Phys. Rev. A* 64 (2001), Nr. 5, S. 052301

[SM05] Shende, Vivek V.; Markov, Igor L.: Quantum circuits for incompletely specified two-qubit operations. *Quantum Inf. Comput.* 5 (2005), Nr. 1, S. 48–56

[SMB04] Shende, Vivek V.; Markov, Igor L.; Bullock, Stephen S.: Minimal universal two-qubit controlled-NOT-based circuits. *Phys. Rev. A* 69 (2004), Nr. 6, S. 062321

[Spi99a] Spivak, Michael: *A comprehensive introduction to differential geometry*. Bd. 1. Dritte Auflage. Houston: Publish or perish, 1999

[Spi99b] Spivak, Michael: *A comprehensive introduction to differential geometry.* Bd. 5. Dritte Auflage. Houston: Publish or perish, 1999

[SS03] Schuch, N.; Siewert, J.: Programmable networks for quantum algorithms. *Phys. Rev. Lett.* 91 (2003), Nr. 2, S. 027902

[Stu93] Sturmfels, Bernd: *Algorithms in invariant theory.* Wien: Springer, 1993

[Sud01] Sudbery, Anthony: On local invariants of pure three-qubit states. *J. Phys. A* 34 (2001), Nr. 3, S. 643–652

[Sus79] Sussmann, Héctor: A bang-bang theorem with bounds on the number of switchings. *SIAM J. Control Opt.* 17 (1979), Nr. 5, S. 629–651

[Sus83] Sussmann, Hector J.: Lie brackets, real analyticity and geometric control. In: Brockett, Roger W. (Hrsg.); Millman, Richard S. (Hrsg.); Sussmann, Hector J. (Hrsg.): *Differential geometric control theory.* Boston: Birkhäuser, 1983 (Progress in mathematics 27), S. 1–116

[Sus85] Sussmann, Héctor: Lie brackets and real analyticity in control theory. In: Olech, Czesław (Hrsg.); Jakubczyk, Bronisław (Hrsg.); Zabczyk, Jerry (Hrsg.): *Mathematical control theory.* Warszawa: Polish Scientific Publishers, 1985 (Banach center publications 14), S. 515–542

[SW86] Sattinger, D. H.; Weaver, O. L.: *Lie groups and algebras with applications to physics, geometry, and mechanics.* New York: Springer, 1986 (Applied mathematical sciences 61)

[SW95a] Sleator, T.; Weinfurter, H.: Quantum teleportation and quantum computation based on cavity QED. *Ann. New York Acad. Sci.* 755 (1995), S. 715–725

[SW95b] Sleator, T.; Weinfurter, H.: Realizable universal quantum logic gates. *Phys. Rev. Lett.* 74 (1995), Nr. 20, S. 4087–4090

[Swo06] Swoboda, Jan: *Time-optimal control of spin systems.* 2006. – `http://arxiv.org/quant-ph/0601131`

[SWS93] Sarti, Augusto; Walsh, Gregory; Sastry, Shankar: Steering left-invariant control systems on matrix Lie groups. In: *Proc. of the 32nd conference on decision and control*, 1993, S. 3117–3121

[Tam04] Tamvakis, Harry: The connection between representation theory and Schubert calculus. *Enseign. Math., II. Sér.* 50 (2004), Nr. 3–4, S. 267–286

[TFJ03] Teodorescu-Frumosu, Mihail; Jaeger, Gregg: Quantum Lorentz-group invariants of n-qubit systems. *Phys. Rev. A* 67 (2003), Nr. 5, S. 052305

[Tho86] Thompson, Robert C.: Proof of a conjectured exponential formula. *Linear Multilinear Algebra* 19 (1986), Nr. 2, S. 187–197

[Tof80] Toffoli, T.: Reversible computing. In: de Baker, J. W. (Hrsg.); van Leeuwen, J. (Hrsg.): *Seventh colloquium on automata, languages and programming*. Berlin: Springer, 1980 (Lecture notes in computer science 85), S. 632–644

[Tof81] Toffoli, Tommaso: Bicontinuous extensions of invertible combinatorial functions. *Math. Systems Theory* 14 (1981), S. 13–23

[TY05] Tauvel, Patrice; Yu, Ruppert W. T.: *Lie algebras and algebraic groups*. Berlin: Springer, 2005

[Uhl71] Uhlmann, A.: Sätze über Dichtematrizen. *Wiss. Z. Karl-Marx-Univ. Leipzig, Math.-Naturwiss.* 20 (1971), Nr. 4/5, S. 633–637

[Uhl00] Uhlmann, Armin: Fidelity and concurrence of conjugated states. *Phys. Rev. A* 62 (2000), Nr. 3, S. 032307

[Vak98] Vakhrameev, S. A.: Bang-bang theorems and related topics. *Proc. Steklov Inst. Math.* 220 (1998), Nr. 1, S. 45–108

[Var84] Varadarajan, V. S.: *Lie groups, Lie algebras, and their representations*. New York: Springer, 1984

[Vas98] Vasconcelos, Wolmer V.: *Computational methods in commutative algebra and algebraic geometry*. Berlin: Springer, 1998 (Algorithms and computation in mathematics 2)

[VC02a] Vidal, G.; Cirac, J. I.: Catalysis in nonlocal quantum operations. *Phys. Rev. Lett.* 88 (2002), Nr. 16, S. 167903

[VC02b] Vidal, G.; Cirac, J. I.: Nonlocal Hamiltonian simulation assisted by local operations and classical communication. *Phys. Rev. A* 66 (2002), Nr. 2, S. 022315

[VC04] Vandersypen, L. M. L.; Chuang, I. L.: NMR techniques for quantum control and computation. *Rev. Mod. Phys.* 76 (2004), Nr. 4, S. 1037–1069

[VD04] Vidal, G.; Dawson, C. M.: Universal quantum circuit for two-qubit transformations with three controlled-NOT gates. *Phys. Rev. A* 69 (2004), Nr. 1, S. 010301(R)

[VDD03] Verstraete, Frank; Dehaene, Jeroen; De Moor, Bart: Normal forms and entanglement measures for multipartite quantum states. *Phys. Rev. A* 68 (2003), Nr. 1, S. 012103

[Ver03] Verdun, Andreas: Leonhard Eulers Einführung und Anwendung von Bezugssystemen in Mechanik und Astronomie. *Elem. Math.* 58 (2003), Nr. 4, S. 169–176

[VHC02] Vidal, G.; Hammerer, K.; Cirac, J. I.: Interaction cost of nonlocal gates. *Phys. Rev. Lett.* 88 (2002), Nr. 23, S. 237902

[Vin89] Vinberg, Ernest B.: *Linear representations of groups.* Basel: Birkhäuser, 1989 (Basler Lehrbücher 2)

[VLK99] Viola, Lorenza; Lloyd, Seth; Knill, Emanuel: Universal control of decoupled quantum systems. *Phys. Rev. Lett.* 83 (1999), Nr. 23, S. 4888–4891

[VMS04] Vartiainen, Juha J.; Möttönen, Mikko; Salomaa, Martti M.: Efficient decomposition of quantum gates. *Phys. Rev. Lett.* 92 (2004), Nr. 17, S. 177902

[VW00] Vollbrecht, K. G. H.; Werner, R. F.: Why two qubits are special. *J. Math. Phys.* 41 (2000), Nr. 10, S. 6772–6782

[VW04] Vatan, Farrokh; Williams, Colin: Optimal quantum circuits for general two-qubit gates. *Phys. Rev. A* 69 (2004), Nr. 3, S. 032315

[Wal90] Walter, Wolfgang: *Analysis II.* Berlin: Springer, 1990 (Grundwissen Mathematik 4)

[Wal05] Wallach, Nolan R.: The Hilbert series of measures of entanglement for 4 qubits. *Acta Appl. Math.* 86 (2005), Nr. 1–2, S. 203–220

[WC01] Wong, Alexander; Christensen, Nelson: Potential multiparticle entanglement measure. *Phys. Rev. A* 63 (2001), Nr. 4, S. 044301

[Wea00a] Weaver, N.: Comment on "On the universality of almost every quantum logic gate". *J. Math. Phys.* 41 (2000), Nr. 5, S. 3300

[Wea00b] Weaver, N.: On the universality of almost every quantum logic gate. *J. Math. Phys.* 41 (2000), Nr. 1, S. 240–243

[Wei23] Weitzenböck, Roland: *Invariantentheorie.* Groningen: P. Noordhoff, 1923

[Wei79] Weil, A.: Géométrie différentielledes espaces fibrés. In: *Œuvres scientifiques. Collected papers* Bd. I. New York: Springer, 1979, S. 422–436

[Whi57] Whitney, Hassler: Elementary structure of real algebraic varieties. *Ann. of Math.* 66 (1957), Nr. 3, S. 545–556

[Whi64] Whittaker, E. T.: *A treatise on the analytical dynamics of particles and rigid bodies.* Vierte Auflage. Cambridge Uinversity Press, 1964. – Nachdruck

[WJB02] Wocjan, Pawel; Janzing, Dominik; Beth, Thomas: Simulating arbitrary pair-interactions by a given Hamiltonian: graph-theoretical bounds on the time complexity. *Quantum Inf. Comput.* 2 (2002), Nr. 2, S. 117–132

[WMS94] Walsh, Gregory C.; Montgomery, Richard; Sastry, S. S.: Optimal path planning on matrix Lie groups. In: *Proc. of the 33nd conference on decision and control*, 1994, S. 1258–1263

[Woc03] Wocjan, Pawel: *Computational power of Hamiltonians in quantum computing*, Universität Karlsruhe, Informatik, Diss., 2003

[Woc06] Wocjan, Pawel: Efficient decoupling schemes with bounded controls on Eulerian orthogonal arrays. *Phys. Rev. A* 73 (2006), Nr. 6, S. 062317

[Wol84] Wolf, Joseph A.: *Spaces of constant curvature*. Fünfte Auflage. Wilmington: Publish or Perish, 1984

[Woo98a] Wootters, William K.: Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.* 80 (1998), Nr. 10, S. 2245–2248

[Woo98b] Wootters, William K.: Quantum entanglement as a quantifiable resource. *Phil. Trans. R. Soc. Lond. A* 356 (1998), S. 1717–1731

[Woo01] Wootters, William K.: Entanglement of formation and concurrence. *Quantum Inf. Comput.* 1 (2001), Nr. 1, S. 27–44

[WRJB02a] Wocjan, Pawel; Rötteler, Martin; Janzing, Dominik; Beth, Thomas: Simulating Hamiltonians in quantum networks: efficient schemes and complexity bounds. *Phys. Rev. A* 65 (2002), Nr. 4, S. 042309

[WRJB02b] Wocjan, Pawel; Rötteler, Martin; Janzing, Dominik; Beth, Thomas: Universal simulation of Hamiltonians using a finite set of control operations. *Quantum Inf. Comput.* 2 (2002), Nr. 2, S. 133–150

[Yam50] Yamabe, Hidehiko: On an arcwise connected subgroup of a Lie group. *Osaka Math. J.* 2 (1950), Nr. 1, S. 13–14

[YK05] Yuan, Haidong; Khaneja, Navin: Time optimal control of coupled qubits under nonstationary interactions. *Phys. Rev. A* 72 (2005), Nr. 4, S. 040301(R)

[Zei96] Zeidler, E. (Hrsg.): *Teubner-Taschenbuch der Mathematik*. Bd. 1. Stuttgart und Leipzig: Teubner, 1996

[Zei00] Zeier, Robert: *Zum fehlertoleranten Rechnen mit Quantenzuständen*, Universität Karlsruhe, Informatik, Diplomarbeit, 2000

[ZGB04] Zeier, Robert; Grassl, Markus; Beth, Thomas: Gate simulation and lower bounds on the simulation time. *Physical Review A* 70 (2004), Nr. 3, S. 032319

[ZVSW03] Zhang, J.; Vala, J.; Sastry, S; Whaley, K. B.: Exact two-qubit universal quantum circuit. *Phys. Rev. Lett.* 91 (2003), Nr. 2, S. 027903

[ZVSW04a] Zhang, Jun; Vala, Jiri; Sastry, Shankar; Whaley, K. B.: Minimum construction of two-qubit quantum operations. *Phys. Rev. Lett.* 93 (2004), Nr. 2, S. 020502

[ZVSW04b] Zhang, Jun; Vala, Jiri; Sastry, Shankar; Whaley, K. B.: Optimal quantum circuit synthesis from controlled-unitary gates. *Phys. Rev. A* 69 (2004), Nr. 4, S. 042309

[ZW05] Zhang, Jun; Whaley, K. B.: Generation of quantum logic operations from physical Hamiltonians. *Phys. Rev. A* 71 (2005), Nr. 5, S. 052317

[ZW06] Zhang, Jun; Whaley, K. B.: Optimal generation of single-qubit operation from an always-on interaction by algebraic decoupling. *Phys. Rev. A* 73 (2006), Nr. 2, S. 022306

Im Kontext der Informationsverarbeitung mit Quantenrechnern untersucht diese Arbeit effiziente Methoden zur Erzeugung unitärer Transformationen unter Verwendung einer gegebenen Menge von Grundoperationen. Nach den Gesetzen der Quantenmechanik bilden dabei die unitären Transformationen die durchführbaren Operationen und zugleich eine Beschreibungssprache für Algorithmen auf einem Quantenrechner. Wir verwenden Methoden der Lie-Theorie zur Strukturanalyse der auftretenden Kontrollprobleme.

ISBN-13: 978-3-86644-081-4
ISBN-10: 3-86644-081-2

www.uvka.de