

# **Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen**

Zur Erlangung des akademischen Grades eines  
Doktors der Naturwissenschaften  
von der Fakultät für Informatik der Universität Karlsruhe  
genehmigte

Dissertation

von

Markus Grassl

aus Trossingen

Tag der mündlichen Prüfung: 14. Februar 2001

Erster Gutachter: Prof. Dr. Thomas Beth

Zweiter Gutachter: Prof. Dr. Rainer Blatt



Berichte aus der Informatik

**Markus Grassl**

**Fehlerkorrigierende Codes für Quantensysteme:  
Konstruktionen und Algorithmen**

Shaker Verlag  
Aachen 2002

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

*Grassl, Markus:*

Fehlerkorrigierende Codes für Quantensysteme:  
Konstruktionen und Algorithmen / Markus Grassl.

Aachen : Shaker, 2002

(Berichte aus der Informatik)

Zugl.: Karlsruhe, Univ., Diss., 2001

ISBN 3-8322-0492-X

Copyright Shaker Verlag 2002

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten.

Printed in Germany.

ISBN 3-8322-0492-X

ISSN 0945-0807

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9

Internet: [www.shaker.de](http://www.shaker.de) • eMail: [info@shaker.de](mailto:info@shaker.de)

## Dank

An erster Stelle möchte ich meinem Doktorvater Herrn Prof. Dr. Thomas Beth danken, der meinen akademischen Werdegang von Anfang an begleitet hat. Schon im Grundstudium der Informatik hat er mein Interesse an Forschungsfragen geweckt. Er hat mir als Diplomanden den Weg in die Wissenschaft geebnet, indem er es mir ermöglichte, die eigenen Untersuchungsergebnisse auf Konferenzen zu präsentieren, und hat mich als Doktorand bei der aktiven Teilnahme an der aktuellen wissenschaftlichen Diskussion unterstützt.

Mein Dank an Herrn Prof. Dr. Rainer Blatt für die Übernahme des Korreferats ist mit der Hoffnung verbunden, daß die theoretischen Ergebnisse dieser Arbeit in nicht allzu ferner Zukunft in den Innsbrucker Forschungslabors seiner Gruppe experimentell umgesetzt werden können.

Bei allen Kollegen und Studierenden, die mich während meiner Zeit als Student und Doktorand am IAKS begleitet haben, sowie bei allen Koautoren meiner wissenschaftlichen Beiträge möchte ich mich für ihre stete Bereitschaft zur Diskussion bedanken. Ausdrücklich erwähnen möchte ich Rainer Steinwandt, dessen konstruktiv kritischen Kommentare ich sehr schätze.

Meine Schwester Roswitha hatte stets ein offenes Ohr für mich. Sie mühte sich durch das technische Sprachwirrwarr eines Informatikers, der sich zudem auf dem Terrain der Mathematiker und Physiker bewegt.

Die größte Unterstützung habe ich durch meine Eltern erfahren. Sie haben mich in meinen Entscheidungen bestärkt und mir während meiner gesamten Zeit in Karlsruhe sehr viel Rückhalt geboten.



# Inhaltsverzeichnis

<b>Einleitung</b>	<b>1</b>
<b>1 Grundlagen</b>	<b>3</b>
1.1 Grundlagen aus der Quantenmechanik . . . . .	3
1.1.1 Bra-Ket-Notation . . . . .	3
1.1.2 Einzelne Quantensysteme . . . . .	6
1.1.3 Ensembles von Quantenzuständen . . . . .	13
1.1.4 Zusammengesetzte Quantensysteme . . . . .	18
1.1.5 Teilsysteme . . . . .	22
1.2 Quantenalgorithmen . . . . .	25
1.2.1 Berechnungsmodelle . . . . .	25
1.2.2 Modellierung von Quantenalgorithmen . . . . .	26
1.2.3 Quantenschaltkreise . . . . .	31
1.2.4 Beispielalgorithmen . . . . .	36
<b>2 Quantenkanäle</b>	<b>43</b>
2.1 Allgemeine Kanalmodellierung . . . . .	43
2.1.1 Allgemeine Quantentransformationen . . . . .	43
2.1.2 Kanaleigenschaften . . . . .	48
2.2 Beispiele . . . . .	53
2.2.1 Einfache Quantenkanäle . . . . .	53
2.2.2 Auslöschungskanal . . . . .	57
2.2.3 Korrelierte Quantenkanäle . . . . .	59
2.2.4 Quantensprünge . . . . .	60
2.3 Simulation von Quantenkanälen . . . . .	62

<b>3</b>	<b>Quantencodes</b>	<b>67</b>
3.1	Allgemeine Quantencodes . . . . .	67
3.1.1	Wiederholungscode . . . . .	68
3.1.2	Bedingungen für die Korrigierbarkeit von Fehlern . . . . .	70
3.1.3	Minimale Codes . . . . .	78
3.2	Quantencodes und klassische Codes . . . . .	83
3.2.1	Pauli-Fehler . . . . .	84
3.2.2	Binärcodes . . . . .	86
3.2.3	Additive Quantencodes . . . . .	94
3.3	Schranken für CSS-Codes . . . . .	103
<b>4</b>	<b>Konstruktion von Quantencodes</b>	<b>109</b>
4.1	Binäre Expansion von Codes . . . . .	109
4.1.1	Endliche Körper . . . . .	109
4.1.2	Expansion von linearen Codes . . . . .	110
4.2	Quanten-BCH-Codes . . . . .	112
4.3	Quantenschaltkreise für $\mathbb{F}_{2^k}$ -lineare Transformationen . . . . .	115
4.4	Quanten-Reed-Solomon-Codes . . . . .	119
4.4.1	Definition der Quanten-Reed-Solomon-Codes . . . . .	119
4.4.2	Codierung von Quanten-Reed-Solomon-Codes . . . . .	121
4.4.3	Decodierung von Quanten-Reed-Solomon-Codes . . . . .	122
<b>5</b>	<b>Ausblick</b>	<b>127</b>
<b>A</b>	<b>Tabellen</b>	<b>129</b>
A.1	Schranken für Quantencodes . . . . .	129
A.1.1	Additive Quantencodes . . . . .	129
A.1.2	CSS-Codes . . . . .	130
A.2	Parameter von <i>Q BCH</i> -Codes . . . . .	135
A.3	Neue additive Quantencodes . . . . .	137
	<b>Literaturverzeichnis</b>	<b>139</b>
	<b>Eigene Veröffentlichungen</b>	<b>155</b>
	<b>Index</b>	<b>161</b>