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

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 • eMail: info@shaker.de

Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen

Dr. Markus Grassl, IAKS, Universität Karlsruhe

Die vorliegende Abhandlung leistet einen Beitrag zur Entwicklung konstruktiver Methoden, Fehler bei der Übertragung und Verarbeitung von Information, die in quantenmechanisch modellierten Systemen gespeichert ist, zu erkennen und zu korrigieren. Die Lösung dieser Aufgabe stellt einen wichtigen Schritt dar auf dem Weg zur Realisierung von Quantenrechnern.

Die Informationsverarbeitung mittels quantenmechanischer Systeme eröffnet im Vergleich zu klassischen Berechnungsmodellen, seien sie abstrakt oder konkret gegeben, neue Aspekte. So impliziert das quantenmechanische Superpositionsprinzip einen hohen Grad von Parallelität. Zustände von Systemen können verschränkt werden, was die Möglichkeit zur Entwicklung neuartiger Kommunikationsprinzipien eröffnet. Prominente Beispiele sind der von Shor entwickelte Algorithmus zur Faktorisierung ganzer Zahlen auf einem Quantenrechner in polynomialer Zeit sowie der Algorithmus von Grover zur Urbildsuche.

Da aber quantenmechanische Systeme keine isolierten Systeme sind, sondern stets in Wechselwirkung mit der Umgebung stehen, müssen Quantenrechner gegen Fehler geschützt werden, die durch diese Wechselwirkung hervorgerufen werden. Anders als bei *klassischen* Systemen kann die dafür erforderliche Redundanz nicht durch Kopieren der Information erzeugt werden; die Gesetze der Quantenmechanik schließen das Kopieren von unbekannten Quantenzuständen aus. Gleichwohl ist es möglich, Information so in einem geeignet gewählten Teilraum eines größeren Systems zu speichern, daß die durch das jeweilige Kanalmodell beschriebenen Fehler korrigiert werden können.

In der Literatur finden sich zwar verschiedene Untersuchungen zur Charakterisierung dieser *Quantencodes* und ihres Bezugs zur klassischen Codierungstheorie, die Ergebnisse sind jedoch meist nicht konstruktiv. In der vorliegenden Abhandlung werden daher Methoden entwickelt, mit Hilfe derer Quantencodes sowie die zur Codierung verwendeten *Quantenschaltkreise* direkt aus der Beschreibung von geeignet gewählten klassischen Codes abgeleitet werden können. Des weiteren werden verschiedene effiziente Algorithmen zur Decodierung von klassischen Codes in Verfahren zur Decodierung von Quantencodes überführt. Ferner wird gezeigt, wie Information über die Position von Fehlern bei der Decodierung genutzt werden kann. Ausgehend von einigen klassischen Codier- und Decodierverfahren für zyklische Codes werden Quantenschaltkreise für zyklische Quantencodes entwickelt.

Im ersten Kapitel werden die Grundlagen für ein abstraktes Modell der Quanteninformationsverarbeitung entwickelt. Dem interdisziplinären Charakter der Thematik entsprechend, werden zuerst Grundlagen aus der Quantenmechanik in einer axiomatischen Weise eingeführt, um anschließend darauf aufbauend ein Modell der Quantenalgorithmen zu entwickeln.

Die abstrakte Modellierung der durch Wechselwirkung eines quantenmechanischen Systems mit seiner Umgebung entstehenden Fehler ist Hauptthema des zweiten Kapitels. Neben verschiedenen anderen Kanalmodellen wird das aus meinen Untersuchungen hervorgegangene Konzept von Quantenkanälen mit klassischer Zusatzinformation eingeführt. Die Frage nach der Simulierbarkeit von Quantenkanälen stellt eine Verbindung zu Quantenalgorithmen her.

Im dritten Kapitel wird die Theorie der fehlerkorrigierenden Codes für Quantensysteme in konstruktiver Weise dargestellt. Aus den abstrakten Voraussetzungen für die Korrigierbarkeit von Fehlern werden Prinzipien zur Codekonstruktion abgeleitet. Damit einhergehend werden die Grundalgorithmen für die Codierung und Decodierung der Codes entwickelt. Mit Blick auf die experimentelle Realisierbarkeit werden die Grenzen für die Parameter von kleinen Codes untersucht; die einzelnen Resultate sind im Anhang zusammengefaßt.

Neuartige Konstruktionsverfahren für fehlerkorrigierende Quantencodes werden im vierten Kapitel beschrieben. Ferner werden Quantenalgorithmen zur Berechnung von linearen Transformationen über endlichen Körpern vorgestellt, die eine effiziente Codierung und Decodierung der neuen Codes erlauben.