

Studentisches Projekt **[QBit]**

Universität Bremen, Fachbereich 3 — Mathematik und Informatik

Bastian Blachetta
Maxime Djao Mola
Olga Hetke
Christoph Hilken
Christian Otterstedt
Nils Przigoda
Abirami Puvanendran
Matthias Schilmann
Eleonora Schönborn
Julia Seiter
Karl Trzebiatowski

Technische Informatik

**Rolf Drechsler,
Mathias Soeken,
Robert Wille
(Hrsg.)**

Auf dem Weg zum Quantencomputer

Entwurf reversibler Logik

Shaker Verlag
Aachen 2012

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Copyright Shaker Verlag 2012

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

Printed in Germany.

ISBN 978-3-8440-1199-9

ISSN 1436-882X

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen

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

Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort

Mit rasanter Geschwindigkeit werden Rechnersysteme heute schneller, kleiner und besser. Computer, die wir heute kaufen, sind bereits nach wenigen Monaten überholt. Ermöglicht wird dies durch die stetig steigende Miniaturisierung, wie sie bereits in den 60er Jahren durch Gordon Moore voraus gesagt wurde: Alle 18 Monate verdoppelt sich die Anzahl der Komponenten auf einem Computerchip. Doch diese Entwicklung wird in absehbarer Zukunft an ihre Grenzen stoßen. Spätestens wenn einzelne Komponenten die atomare Ebene erreichen, wird man heutzutage verwendete Rechnersysteme nicht mehr weiter verbessern können. Schon jetzt zeigt sich, dass mehr Performanz oft nur noch durch die Verwendung von mehreren Cores auf einem Chip erreicht wird. Daher braucht man Alternativen, welche grundsätzlich anders funktionieren als die derzeit eingesetzten Rechenmaschinen.

Eine vielversprechende Alternative stellen Quantencomputer dar. Sie ermöglichen es beispielsweise, viele relevante Probleme in deutlich kürzerer Laufzeit als konventionelle Methoden zu lösen. Quantencomputer arbeiten dabei auf Basis so genannter reversibler Logik. Das heißt, mit Hilfe der Ausgaben eines Systems lassen sich stets die Eingaben berechnen. Dies steht im Gegensatz zu den meisten klassischen Systemen, wie sie heute verwendet werden: Ein Wert 1 am Ausgang eines ODER-Gatters lässt zum Beispiel nicht auf die Eingabe schließen. Entsprechend ergeben sich beim Entwurf von Quantencomputern neue Fragestellungen. So müssen wie bei heutigen Technologien Schaltungen synthetisiert, optimiert und anschließend auf Korrektheit überprüft (d.h. verifiziert) werden. Konventionelle Methoden lassen sich aber nicht alle 1:1 für Quantencomputer umsetzen. Außerdem werden besonders hilfreiche Eigenschaften reversibler Logik durch sie nicht ausgenutzt. Daher müssen Verfahren zum Entwurf solcher Schaltungen neu entwickelt werden.

Dieser Aufgabe hat sich eine Gruppe von elf Studierenden der Informatik an der Universität Bremen im zweijährigen studentischen Projekt *QBit* gewidmet. Ziel des Projektes war die Entwicklung und Zusammenführung von Entwurfsverfahren für den Bau von Quantenschaltungen aus Sicht der Informatik. Dies beinhaltete unter anderem die Synthe-

se, Optimierung, Technologieabbildung, Simulation und die Verifikation entsprechender Systeme sowie die Integration der resultierenden Methoden in einen zusammenhängenden Entwurfsablauf. Neben der dafür nötigen Erarbeitung der Grundlagen sowie des existierenden Stands der Forschung haben die Studierenden dabei auch wissenschaftliche Fragestellungen adressiert und erfolgreich gelöst. So ist besonders hervorzuheben, dass Ergebnisse des Projektes bereits auf internationalen Tagungen veröffentlicht und auch teilweise durch die Studierenden selbst vorgestellt wurden.

Das vorliegende Buch ist eine Zusammenfassung der im Rahmen des Projektes erzielten Ergebnisse. Es führt in die wesentlichen Grundlagen dieses spannenden Gebietes ein und stellt anschließend die im Projekt entwickelten Beiträge vor. Das Buch ist dabei mehr als nur ein Arbeitsbericht eines studentischen Projektes. Es stellt Innovationen sowie bisher unveröffentlichte, wissenschaftlich sehr interessante Ergebnisse vor und bietet damit auch für Wissenschaftlerinnen und Wissenschaftler aus dem Gebiet neue Einblicke und interessante Ideen.

Als Betreuer des *QBit*-Projektes möchten wir uns bei den Teilnehmenden für die spannende und interessante Zusammenarbeit bedanken. Die gemeinsame Projektarbeit haben wir sowohl fachlich als auch außerfachlich stets als sehr inspirierend und bereichernd empfunden. Allen Teilnehmenden wünschen wir alles Gute und einen erfolgreichen Start in das Berufsleben.

Bremen,
Juli 2012

Rolf Drechsler
Mathias Soeken
Robert Wille

Inhaltsverzeichnis

1. Einleitung	1
2. Grundlagen	5
2.1. Reversible Funktionen	5
2.2. Reversible Schaltkreise	7
2.2.1. Quantenschaltkreise	10
2.2.2. Kostenmaße	11
2.2.3. Kombinatorische und sequentielle Schaltkreise	13
2.2.4. Waveforms	13
2.3. Boolesche Datenstrukturen und Algorithmen	14
2.3.1. Binäre Entscheidungsdiagramme	14
2.3.2. Boolesche Erfüllbarkeit	16
I. Synthese	19
3. Synthese kleiner Funktionen	21
3.1. Transpositionsbasierte Synthese	21
3.1.1. Generelle Idee und Algorithmus	23
3.1.2. Theoretische Ergebnisse	30
3.1.3. Experimentelle Ergebnisse	36
3.2. Optimierung exakter Synthese	40
3.2.1. Exakte Synthese	41
3.2.2. Erweiterung des bisherigen Verfahrens	46
3.2.3. Erweiterung um Redundanzprüfung	49
3.2.4. Experimentelle Ergebnisse	53
3.3. Zusammenfassung	55

4. Synthese großer Funktionen	57
4.1. KFDD-basierte Synthese	57
4.1.1. Kronecker Functional Decision Diagramms	57
4.1.2. Algorithmus	58
4.1.3. Optimierung	60
4.1.4. Experimentelle Ergebnisse	64
4.2. QMDD-basierte Synthese	67
4.2.1. Grundlagen	67
4.2.2. Generelle Idee	70
4.2.3. Algorithmus	73
4.2.4. Experimentelle Ergebnisse	75
4.3. Zusammenfassung	78
5. Synthese sequentieller Funktionen	81
5.1. Sequentialität in reversiblen Schaltungen	81
5.2. DEA-basierte Synthese	84
5.2.1. Zustandsautomaten	84
5.2.2. Algorithmus	85
5.2.3. Optimierung	88
5.2.4. Experimentelle Ergebnisse	94
5.3. Zusammenfassung	101
6. Synthese mit Hardwarebeschreibungssprachen	103
6.1. SyReC - Eine reversible Hardwarebeschreibungssprache	103
6.2. Erweiterungen von SyReC	106
6.3. Zusammenfassung	108
7. Synthese von Quantenschaltkreisen	111
7.1. Dekomposition	111
7.1.1. Generelle Idee	111
7.1.2. Algorithmus	113
7.2. Optimierung	117
7.2.1. Generelle Idee	117
7.2.2. Algorithmus	118
7.3. Experimentelle Ergebnisse	120
7.4. Zusammenfassung	121

II. Verifikation 125

8. Simulation 127

8.1. Simulation auf Gatterebene 127

8.2. Simulation mit SystemC 130

 8.2.1. Generelle Idee 130

 8.2.2. Übersetzung 131

8.3. Experimentelle Ergebnisse 138

8.4. Zusammenfassung 139

9. Eigenschaftsprüfung 141

9.1. Theorembeweisen 141

 9.1.1. Grundlagen 142

 9.1.2. Generelle Idee 144

 9.1.3. Modellierung von Schaltkreisen in HOL 145

 9.1.4. Formulierung von Eigenschaften 150

 9.1.5. Formulierung des Beweisziels 151

 9.1.6. Beweisführung 152

 9.1.7. Besondere Aspekte 153

 9.1.8. Diskussion 157

9.2. Modellprüfung 158

 9.2.1. Grundlagen 159

 9.2.2. Vorgehen 164

9.3. Zusammenfassung 167

10. Simulativer Äquivalenzvergleich 171

10.1. Motivation 171

10.2. Generelle Idee 173

10.3. Experimentelle Ergebnisse 174

10.4. Zusammenfassung 176

III. Anwendung 177

11. Fallstudien 179

11.1. Prozessor 179

 11.1.1. Spezifikation 179

 11.1.2. Realisierung 182

11.1.3. Modellprüfung	186
11.1.4. Programmausführung	195
11.2. Bildkonverter	197
11.2.1. Spezifikation	197
11.2.2. Realisierung	198
11.2.3. Programmausführung	200
11.3. Zusammenfassung	201
12. Integration in eine Entwurfsumgebung	203
13. Zusammenfassung	207
Literaturverzeichnis	209