Über Reversibilität, Nicht-Determiniertheit und Quantenrechnen in Zellularautomaten

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

Dissertation

von Kathrin Paschen
aus Hamburg

Tag der mündlichen Prüfung: 21. Juni 2002
Erster Gutachter: Prof. Dr.-Ing. Roland Vollmar
Zweiter Gutachter: Prof. Dr. Jozef Gruska DrSc

If we knew what we were doing,
it wouldn't be called research, would it?

Albert Einstein

INHALTSVERZEICHNIS

Danksagung

An dieser Stelle möchte ich mich bei all denen bedanken, die mich bei der Anfertigung dieser Arbeit unterstützt haben. Dazu gehört Herr Professor Vollmar, der mir viel Freiheit gelassen hat, meinen wissenschaftlichen Interessen nachzugehen. Besonders möchte ich Herrn Professor Gruska für die Übernahme des Korreferates danken; ohne ihn hätte ich mich nie mit Quantenzellularautomaten beschäftigt. Außerdem danke ich Thomas Worsch für viele anregende Diskussionen.

Einleitung

Quantenrechner sind ein neuartiges Modell. Sie nutzen quantenmechanisches Verhalten, um im Vergleich mit klassischen Rechnern bessere Laufzeiten zu erzielen. Verschiedene Architekturen für Quantenrechner sind im Gespräch; einige von ihnen ähneln Zellularautomaten. Dies ist eine attraktive Architektur, weil Zellularautomaten aus vielen einfachen (daher vergleichsweise leicht herstellbaren) Rechenelementen bestehen und trotz ihrer gleichförmigen und streng lokalen Interaktion Berechnungsuniversalität erreichen.

Quantenzellularautomaten sind schon relativ früh in der Geschichte der Quantenrechner vorgeschlagen worden (zum Beispiel 1988 von Grössing und Zeilinger [33]). Dennoch ist bis jetzt wenig über sie bekannt. Es gibt nur eine Hand voll Aufsätze zu dem Thema, und diese beschäftigen sich vorwiegend mit der Vorstellung einer Definition und dem Nachweis der Berechnungsuniversalität. Deshalb sind eine ganze Reihe von Fragen bis jetzt offen geblieben.

Erstens sind die existierenden Definitionen nicht zufriedenstellend, weil sie keine lückenlose Übertragung klassischer Zellularautomaten zulassen. Sie bauen ihre Sicht auf Zustände und die Anwendung von Zellularautomaten auf globale Konfigurationen auf und es gelingt ihnen nicht, einen sinnvollen Begriff von lokalen Konfigurationen entwickeln. Lokalität ist eine der definierenden Eigenschaften von Zellularautomaten – und darüber

hinaus eine, die diese Architektur für Quantenrechner attraktiv macht. Die existierenden Begriffe aber können gerade diese Lokalität nicht widerspiegeln, und so geht ein Teil des Bezugs zum klassischen Modell verloren.

Zweitens muss man fragen, ob es sich hier um ein sinnvolles Berechnungsmodell handelt. Quantenzellularautomaten sind auf unitäre (insbesondere reversible) Operationen beschränkt. Die bekannten klassischen Berechnungsmodelle müssen bei reversibler Operation grundsätzlich Effizienzeinbußen hinnehmen, wie Frank in seiner Dissertation gezeigt hat [31]. Vom Einsatz von Quantensystemen erhofft man sich einen Effizienzgewinn, doch man erkauft ihn eventuell mit zusätzlichen Ressourcen für die Reversibilität und muss auch für Quantenzellularautomaten abwägen, ob der Nutzen die Kosten aufwiegt.

Drittens sind Quantenrechner nicht deterministisch; sie weisen verschiedenen Zuständen Amplituden zu. Im Laufe der Zeit können auch weit auseinanderliegende Zellen miteinander verschränkt werden; die Beschreibung der Konfigurationen muss dem Rechnung tragen.

Viertens stellt sich die Frage, welchen Effekt geringe Abweichungen von der Überführungsfunktion eines Quantenzellularautomaten auf seine Entwicklung haben. Dies führt auf die allgemeinere Frage, wie man globale Konfigurationen von Quantenzellularautomaten vergleicht.

Das zentrale Ergebnis dieser Arbeit ist ein aussagekräftiges Modell von Quantenzellularautomaten, das es uns insbesondere erlaubt, die hier gestellten Fragen zu beantworten. Die Zielsetzung ist damit strukturell und nicht algorithmisch: Neue Quantenalgorithmen oder neue Nachweise der Überlegenheit von Quantenzellularautomaten über ihre klassischen Gegenstücke würden den Rahmen der Arbeit sprengen.

In der Arbeit kommen in erster Linie algebraische Methoden zum Einsatz. Für unsere Definition von Quantenzellularautomaten setzen wir reduzierte Dichteoperatoren ein, um das begrenzte Wissen jeder einzelnen Zelle über ihre Nachbarschaft abzubilden. Dies erlaubt uns, lokale und globale Konfigurationen (auch unendliche) über Elemente von C^*-Algebren definieren und Quantenzellularautomaten als eine spezielle Klasse von Automorphismen solcher Algebren einzuführen. Dadurch erhalten wir ein Modell

mit der gewünschten Lokalität und ermöglichen darüber hinaus den Einsatz einer reichen mathematischen Theorie.

Unser Modell enthält klassische reversible Zellularautomaten als Spezialfälle von Quantenzellularautomaten. Daher können wir die Frage nach dem Preis der Reversibilität zumindest teilweise durch Ergebnisse aus der Literatur zur reversiblen Simulation irreversibler Zellularautomaten beantworten. Daneben diskutieren wir detailliert die Auswirkungen von Reversibilität auf das Verhalten deterministischer Zellularautomaten.

Für Antworten zum dritten Fragenkomplex beschäftigen wir uns auch mit stochastischen Zellularautomaten. Sie sind natürliche Kandidaten für einen Vergleich mit Quantenzellularautomaten; man kann hoffen, dass sich Ergebnisse übertragen lassen oder dass ein Scheitern der Übertragung Einblicke in die Unterschiede zwischen den beiden Modellen erlaubt.

Wir stellen eine Metrik für stochastische Zellularautomaten vor und setzen sie ein, um nachzuweisen, dass kleine Abweichungen von der Überführungsfunktion im Allgemeinen große Auswirkungen haben können (auch wenn sie dies üblicherweise nicht tun). Aus der Metrik für stochastische Zellularautomaten gewinnen wir eine Pseudometrik für Quantenzellularautomaten. Der C^*-algebraische Ansatz gestattet jedoch eine elegantere Metrik. Allerdings ist es sehr schwierig, gute Abschätzungen für den Abstand nach mehreren Iterationen zu erhalten.

Die Arbeit ist folgendermaßen aufgebaut: Klassische reversible Zellularautomaten werden in Kapitel 1 behandelt. Kapitel 2 beschäftigt sich mit stochastischen Zellularautomaten. Nach einer kurzen Einführung in Quantenrechnen in Kapitel 3 behandelt Kapitel 4 Quantenzellularautomaten. Ein Überblick über die Ergebnisse sowie offen gebliebene Fragen schließt die Arbeit ab.

KAPITEL 1

Deterministische reversible Zellularautomaten

1.1 Einleitung

Zellularautomaten sind ein universelles Modell paralleler Rechnung, dessen Ursprünge auf John v. Neumann zurückgehen [10]. Sie bestehen aus einer Vielzahl gleichartiger Rechenelemente, die jedes für sich genommen relativ einfach sind. Diese Einfachheit und Gleichartigkeit sind ein Grund, Zellularautomaten als Architektur eines Quantencomputers zu erwägen; tatsächlich ähneln einige der physikalischen Realisierungen von Quantenrechnern Zellularautomaten.

Quantenrechnen ist reversibles Rechnen; jede Definition von Quantenzellularautomaten baut auf reversiblen Zellularautomaten auf. Wie schwer wiegt die Forderung nach Reversibilität – wie stark beeinträchtigt sie Mächtigkeit und Effizienz von Zellularautomaten? Mit dieser Frage beschäftigt sich das folgende Kapitel.

Reversible Zellularautomaten müssen insbesondere injektiv sein. Hierbei macht es einen Unterschied, ob man die Zellularautomaten auf sogenannte endliche Konfigurationen einschränkt oder nicht. Die übliche Definition von Reversibilität geht von unendlichen Konfigurationen aus.

Wir untersuchen die strukturellen Besonderheiten reversibler Zellular-

automaten und geben Ursachen dafür an, dass sie nicht nur selten, sondern meist auch trivial sind. Außerdem führen wir verschiedene Konstruktionsverfahren ein.

Da reversible ZA selten sind, stellt sich die Frage, ob sie ein sinnvolles Berechnungsmodell darstellen. Diese Frage beantworten wir positiv, indem wir verschiedene bekannte Verfahren zur reversiblen Simulation beliebiger Zellularautomaten (und damit zur reversiblen Simulation von Turingmaschinen) vorstellen.

Schließlich untersuchen wir den Zusammenhang zwischen Reversibilität und verschiedenen Begriffen von Informationserhalt.

1.2 Definitionen

Zellularautomaten bestehen aus einer endlichen oder unendlichen Menge gleichartiger Rechenelemente, den sogenannten *Zellen*. Diese sind regelmäßig angeordnet und so miteinander verknüpft, dass jede Zelle über die gleiche Menge an direkten Nachbarn verfügt. Jede Zelle befindet sich zu jedem Zeitpunkt in einem aus einer endlichen Menge von Zuständen.

Rechnung erfolgt in zeitdiskreten Schritten; in jedem Schritt wendet jede Zelle die gleiche Funktion auf ihren eigenen Zustand und die ihrer Nachbarn an, um ihren neuen Zustand zu ermitteln.

In dieser Arbeit beschränken wir uns auf eindimensionale Zellularautomaten und indizieren die Zellen mit den Elementen von $\mathbb{Z}$. Wenn wir von „der Zelle k“ sprechen, meinen wir die Zelle mit dem Index k.

Definition 1.1 (Deterministischer Zellularautomat)
Ein deterministischer eindimensionaler Zellularautomat *ist ein 3-Tupel* (S, N, φ), *wobei* S *für ein endliches Alphabet steht,* $N \in \mathbb{N}$ *für die* Nachbarschaftsgröße *und* $\varphi : S^N \to S$ *für die* lokale Überführungsfunktion.

Wir gehen ohne Beschränkung der Allgemeinheit davon aus, dass S isomorph zu $\{0, \ldots, |S|-1\} \subset \mathbb{N}$ ist. Die *Nachbarschaft* der Zelle k besteht für ungerade N aus den Zellen $k-(N-1)/2, \ldots, k+(N-1)/2$, für gerade N aus den Zellen $k-(N-2)/2, \ldots, k+N/2$. Wenn nichts anderes gesagt

ist, ist N im Folgenden immer ungerade. Gelegentlich verwenden wir den *Radius* $R = (N-1)/2$ anstelle von N.

Von nun an kürzen wir Zellularautomaten als ZA ab.

Als *lokale Konfiguration* an der Stelle k bezeichnet man die Zustände der Zellen in der Nachbarschaft der Zelle k; sie entspricht einem Wort aus S^N. Eine *globale Konfiguration* beschreibt die Zustände aller Zellen des ZA. Formal schreiben wir globale Konfigurationen als Funktionen $c : \mathbb{Z} \to S$ und verwenden $c_i = c(i)$, um den Zustand der Zelle mit dem Index i zu bezeichnen.

Gelegentlich versteht man unter einer globalen Konfiguration ein beidseitig unendliches Wort, also die Äquivalenzklasse modulo Verschiebung einer globalen Konfiguration gemäß unserer Schreibweise. Dies werden wir hier nicht tun.

Die lokale Überführungsfunktion φ ist eine Abbildung von S^N in S. Wir können sie mittels

$$\begin{aligned} &\varphi(w_1 w_2 \dots w_{N+k}) \\ &:= \varphi(w_1 w_2 \dots w_N)\varphi(w_2 w_3 \dots w_{N+1}) \dots \varphi(w_{k+1} w_{k+2} \dots w_{k+N}) \end{aligned} \tag{1.1}$$

zu einer Funktion $S^N \cdot S^* \to S^+$ fortsetzen. In ähnlicher Weise erhalten wir die von φ induzierte *globale Überführungsfunktion* Φ, eine Selbstabbildung von $S^{\mathbb{Z}}$: Für alle $i \in \mathbb{Z}$ ist $(\Phi(c))_i = \varphi(c_{i-R}, \dots, c_{i+R})$.

Abbildung 1.1 zeigt, wie Φ aus φ hervorgeht.

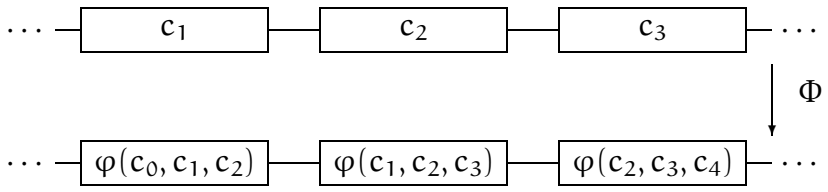

Abbildung 1.1: Globale und lokale Überführungsfunktion

Wir schreiben gelegentlich $A(c)$ statt $\Phi(c)$ für das Ergebnis der Anwendung von Φ auf $c \in S^{\mathbb{Z}}$, wenn Φ die globale Überführungsfunktion

eines ZA A ist. Unter einem *Berechnungsschritt* eines ZA verstehen wir die einmalige Anwendung seiner globalen Überführungsfunktion.

Die lokale Überführungsfunktion eines ZA (S, N, φ) ist durch Angabe einer Tabelle mit $|S|^N$ Einträgen eindeutig festgelegt. Indem man die Elemente von S^N mit Zahlen zur Basis $|S|$ identifiziert, erhält man eine Ordnung von S^N. Schreibt man die Funktionswerte von φ in der Reihenfolge dieser Ordnung, so erhält man ein Wort aus $S^{|S^N|}$. Dieses entspricht wiederum einer Zahl, der *Wolfram-Kodierung* von φ. Sie ist eine nützliche und kompakte Spezifikation der lokalen Überführungsfunktion.

Sei zum Beispiel A der ZA $(\{0,1\}, 3, \sigma)$ mit

$$\begin{aligned}
&\sigma(0,0,0) = 0, \quad && \sigma(0,0,1) = 0, \quad && \sigma(0,1,0) = 0,\\
&\sigma(0,1,1) = 0, \quad && \sigma(1,0,0) = 1, \quad && \sigma(1,0,1) = 1,\\
&\sigma(1,1,0) = 1, \quad && \sigma(1,1,1) = 1.
\end{aligned}$$

A heißt auch *(elementare) Verschiebung (nach rechts)*. Die Wolfram–Kodierung von A ist binär 00001111, dezimal 240. Wenn wir im Folgenden einen ZA mit der lokalen Überführungsfunktion σ verwenden, ist immer eine Verschiebung gemeint.

Man kann jeden ZA (S, N, φ) in einen ZA $(S, N+2, \psi)$ so einbetten, dass die globalen Überführungsfunktionen gleich sind, indem man $\psi(s_0, w, s_{N+1})$ für $s_0, s_{N+1} \in S$ und $w \in S^N$ durch $\varphi(w)$ definiert. Verallgemeinernd kann man jeden ZA in einen ZA mit größerer Nachbarschaft einbetten.

Andererseits kann man die Nachbarschaft immer auf die Größe drei reduzieren: Sei $A = (S, N, \varphi)$ ein ZA mit $N > 3$. Ohne Einschränkung sei $N = 3k$ für ein $k \in \mathbb{N}$ (für $N \neq 3k$, bettet man A in einen ZA mit entsprechend größerer Nachbarschaft ein). Wir wählen ein Alphabet T, das zu S^k isomorph ist, und definieren

$$\begin{aligned}
&\psi((s_1, \ldots, s_k), (s_{k+1}, \ldots, s_{2k}), (s_{2k+1}, \ldots, s_{3k}))\\
&= \varphi(s_1, \ldots, s_{3k}).
\end{aligned}$$

Dann haben (S, N, φ) und $(T, 3, \psi)$ die gleiche globale Überführungsfunktion.

Weitergehende Einführungen in ZA findet man in den Büchern *Cellular Automata Machines* von Toffoli und Margolus [81] oder *Algorithmen in Zellularautomaten* von Vollmar [84].

Wir kommen zur Surjektivität und Injektivität von ZA. Hier macht es einen Unterschied, ob man sich auf sogenannte endliche Konfigurationen einschränkt oder nicht.

Viele ZA besitzen einen *stillen* Zustand: Ihre Überführungsfunktion bildet lokale Konfigurationen, die nur aus stillen Zuständen bestehen, wieder auf einen stillen Zustand ab. Ein ZA kann immer so erweitert werden, dass er einen stillen Zustand besitzt. Wenn sich alle bis auf endlich viele Zellen einer globalen Konfiguration in dem gleichen stillen Zustand befinden, wird dies auch nach endlich vielen Rechenschritten noch der Fall sein. Solche globalen Konfigurationen nennt man *endlich*, . Ein Spezialfall von unendlichen Konfigurationen sind *periodische* Konfigurationen; das sind solche, für die ein $k \in \mathbb{N}$ existiert, so dass für alle $i \in \mathbb{Z}$ gilt: Die Zelle i ist im gleichen Zustand wie die Zelle $i + k$. Eine äquivalente Definition besagt, dass eine Konfiguration (mit Periode k) periodisch ist, wenn sie unter k-facher Verschiebung auf sich selbst abgebildet wird.

Wir nennen einen ZA *reversibel*, wenn seine globale Überführungsfunktion auf unendlichen Konfigurationen bijektiv ist. Das folgende Lemma besagt unter anderem, dass dies genau dann der Fall ist, wenn die globale Überführungsfunktionen auf unendlichen Konfigurationen injektiv ist.

Lemma 1.1 (Durand [19])
Ein ZA ist auf unendlichen Konfigurationen genau dann bijektiv, wenn seine globale Überführungsfunktion dort injektiv ist. Injektivität auf unendlichen Konfigurationen ist gleichbedeutend mit Injektivität auf periodischen Konfigurationen.

Eingeschränkt auf endliche Konfigurationen ist ein ZA genau dann injektiv, wenn er auf unendlichen Konfigurationen surjektiv ist.

Wir bezeichnen ZA als surjektiv beziehungsweise injektiv, wenn sie auf unendlichen Konfigurationen surjektiv beziehungsweise injektiv sind.

Ein surjektiver und nicht injektiver ZA ist zum Beispiel

$$A_{\text{xor}} = (\{0, 1\}, 2, \varphi)$$

mit $\varphi(x, y) = x + y \bmod 2$: Mit dem im folgenden Abschnitt eingeführten Verfahren ist leicht zu sehen, dass A_{xor} surjektiv ist. Die unendlichen Konfigurationen $\ldots 01010101 \ldots$ und $\ldots 10101010 \ldots$ haben unter A_{xor} das gleiche Bild, nämlich $\ldots 111111 \ldots$; demnach ist A_{xor} auf unendlichen Konfigurationen nicht injektiv.

Man kann Reversibilität von ZA durch Injektivität auf endlichen Konfigurationen definieren. Das hat allerdings den Nachteil, dass dann die Inverse eines reversiblen ZA nicht immer ein ZA ist.

Wir verstehen unter Reversibilität im Folgenden Injektivität auf unendlichen Konfigurationen. Damit besitzt jeder reversible ZA einen inversen ZA:

Lemma 1.2 (Hedlund [37])
Ist ein ZA auf unendlichen Konfigurationen injektiv, so ist die Inverse seiner globalen Überführungsfunktion ihrerseits die globale Überführungsfunktion eines ZA.

Schließlich bemerken wir noch, dass die Einschränkung eines surjektiven ZA auf endliche Konfigurationen nicht surjektiv sein muss. Als Beispiel dient wieder A_{xor}: Die endliche Konfiguration $\ldots 0001000 \ldots$, bei der nur eine Zelle im Zustand 1 ist und alle anderen im Zustand 0 sind, besitzt zwei Urbilder, nämlich $\ldots 111000 \ldots$ und $\ldots 000111 \ldots$ und keines der beiden ist endlich, weil 1 kein stiller Zustand von A_{xor} ist. Folglich ist A_{xor} *eingeschränkt auf endliche Konfigurationen* nicht surjektiv.

Von nun an kürzen wir reversible Zellularautomaten mit RZA ab und verstehen darunter solche ZA, deren globale Überführungsfunktion auf unendlichen Konfigurationen bijektiv ist.

1.3 Eigenschaften reversibler ZA

1.3.1 Reversibilität erkennen

Für eindimensionale ZA haben Amoroso und Patt Algorithmen angegeben, die Injektivität und Surjektivität entscheiden [3]. Für höhere Dimensionen

hat Kari nachgewiesen, dass Injektivität und Surjektivität unentscheidbar sind [43]. Wir beschäftigen uns hier nur mit eindimensionalen ZA.

Surjektivität ist einfach zu entscheiden. Zu $w \in S^n$ und einem ZA $A = (S, N, \varphi)$ sei $\varphi^{-1}(w) = \{v \in S^{n+N-1} : \varphi(v) = w\}$. Es gilt nach Hedlund [37]:

Lemma 1.3
Sei $A = (S, N, \varphi)$ ein ZA. Die folgenden Aussagen sind äquivalent:

1. *A ist surjektiv.*
2. *Für alle $w \in S^+$ ist $|\varphi^{-1}(w)| > 0$.*
3. *Für alle $w \in S^k$ ist $|\varphi^{-1}(w)| = |S|^{N-1}$.*

Surjektivität läßt sich daher folgendermaßen entscheiden. Zu A bilden wir einen nichtdeterministischen endlichen Automaten mit dem Eingabealphabet S und der Zustandsänderungsfunktion δ. Die Zustandsmenge Z enthält die Zustände s_w für $w \in S^{N-1}$ sowie einen nichtakzeptierenden Zustand s_F. Die Menge der Anfangszustände ist gleich der Menge der akzeptierenden Zustände $Z \setminus \{s_F\}$. Die Funktion $\delta : Z \times S \to Z$ ist definiert durch $\delta(s_F, x) = s_F$ für alle $x \in S$ und

$$\delta(s_{x \cdot v}, y) = \begin{cases} s_{v \cdot z} & \text{falls } \exists z \in S : \varphi(x \cdot v \cdot z) = y \\ s_F & \text{sonst} \end{cases}$$

für $v \in S^{N-2}, x, y, z \in S$.

Dieser Automat (auch bekannt als deBruijn–Graph von A [86]) erkennt die Wörter über S, die als endliche Teilwörter in Elementen von $A(S^{\mathbb{Z}})$ vorkommen. Der Automat erkennt genau dann S^*, wenn A surjektiv ist. Einen effizienteren (Polynomialzeit-) Algorithmus hat Sutner [79] angegeben.

Außerdem folgt aus Lemma 1.3, dass alle surjektiven ZA *balanciert* sind; das heißt, für alle $s \in S$ existiert die gleiche Anzahl von $w \in S^N$ mit $\varphi(w) = s$ (man setze $k = 1$ in der dritten Aussage). Insbesondere sind daher auch alle reversiblen ZA balanciert, weil sie eine echte Teilmenge der surjektiven ZA bilden.

Injektivität ist schwieriger zu erkennen. Der Algorithmus von Amoroso und Patt [3] nutzt aus, dass es ausreicht, Injektivität auf periodischen

Konfigurationen nachzuweisen. Er sucht systematisch nach verschiedenen Konfigurationen, die unter der globalen Überführungsfunktion das gleiche Bild haben. Die Laufzeit ist in

$$O\left(|S| \cdot \binom{|S|^{N-1}}{2}\right).$$

Dies lässt sich nicht wesentlich verbessern, da jeder äquivalente Algorithmus zumindest die $|S|^N$ Einträge umfassende Spezifikation der lokalen Überführungsfunktion durchgehen muss.

Hat man mit diesem oder einem anderen Algorithmus sichergestellt, dass ein ZA A reversibel ist, stellt sich die Frage, wie man die Inverse A^{-1} bestimmt. Dazu kann man Algorithmus 1.1 einsetzen.

Er erhält als Eingabe die Spezifikation (S, N, φ) eines RZA A sowie eine natürliche Zahl n und ermittelt einen eindimensionalen RZA $B = (S, n, \psi)$ mit der Eigenschaft, dass für alle globalen Konfigurationen c gilt: $(A \circ B)(c) = (B \circ A)(c) = c$, falls ein solcher RZA B existiert. Es stehe $w[i]$ für das i-te Symbol von w.

Algorithmus 1.1 (Invertierung eines ZA)

```
für alle Wörter v der Länge n über S
   ψ(v) := unbekannt
für alle Wörter w der Länge N − 1 + n über S
   falls ψ(φ(w)) = w[(N − 1 + n)/2] oder ψ(φ(w)) = unbekannt
      ψ(φ(w)) := w[(N − 1 + n)/2]
   sonst
      beende die Suche hier
falls alle Wörter w abgearbeitet wurden
   gib B als Inverse von A aus
```

Diesen Algorithmus wendet man zuerst für $n = 1$ an. Jedes Mal, wenn der Algorithmus sich vorzeitig beendet, erhöht man n um zwei und ruft den Algorithmus erneut auf. Da A laut Voraussetzung reversibel ist, existiert eine Inverse und das Verfahren terminiert.

Die Iteration über verschiedene n ist nötig, weil die Größe der Nachbarschaft von A^{-1} von der für A abweichen kann.

1.3.2 Konstruktion von RZA

Einleitung

Es ist nicht leicht, reversible ZA zu finden. Der Algorithmus von Amoroso und Patt entscheidet zwar in vertretbarer Zeit, ob ein gegebener ZA reversibel ist, aber wie wir weiter unten noch sehen werden, sind RZA so selten, dass man sie schon gezielt erzeugen muss, um brauchbare Beispiele zu finden.

Eine Möglichkeit dafür sind partitionierte ZA, eine spezielle Darstellungsform von ZA, die Reversibilität leicht erkennen lässt. Von der Definition her ähnlich sind Block-ZA, die wir ebenfalls kurz einführen. Schließlich erwähnen wir noch eine effiziente algebraische Methode zur Aufzählung sämtlicher reversibler ZA.

Partitionierte Zellularautomaten

Bei partitionierten ZA (PZA) ist Reversibilität einfach festzustellen. Der Preis hierfür ist eine Vergrößerung der Zustandsmenge. Für die reversible Implementierung von Algorithmen werden bevorzugt partitionierte ZA angegeben; ein Beispiel ist die Lösung des Firing Squad Synchronization Problems von Imai und Morita [40]. Diese arbeitet in der auch für nicht reversible ZA optimalen Zeit, benötigt aber 99 Zustände. Dagegen gibt eine irreversible zeitoptimale Lösung mit sechs Zuständen von Mazoyer [51] (ob es eine zeitoptimale Lösung mit fünf Zuständen gibt, ist unbekannt).

Definition 1.2 (Partitionierter ZA)
Ein partitionierter ZA ist ein 3-Tupel (S, N, φ) *aus einem Alphabet* S *der Form* $S_1 \times S_2 \times \cdots \times S_N$, *einer Nachbarschaftsgröße* $N \in \mathbb{N}$ *und einer lokalen Überführungsfunktion* $\varphi : S \to S$.

Ein Berechnungsschritt eines PZA erfolgt folgendermaßen: Der Zustand c_i der i-ten Zelle ist ein N-Tupel $(s_i(1), \ldots, s_i(N))$. Die Nachbarschaft der i-ten Zelle besteht aus den Zellen mit den Indizes $i-(N-1)/2$ bis $i+(N-1)/2$. Als Eingabe für φ verwenden wir das N-Tupel

$$(s_{i-(N-1)/2}(1), s_{i-(N-1)/2+1}(2), \ldots, s_{i+(N-1)/2}(N)).$$

Man verwendet also von der k-ten Zelle der Nachbarschaft nur die k-te Komponente des Zustandes. Die Ausgabe von φ ist der neue Zustand der i-ten Zelle. Abbildung 1.2 illustriert die Arbeitsweise von PZA.

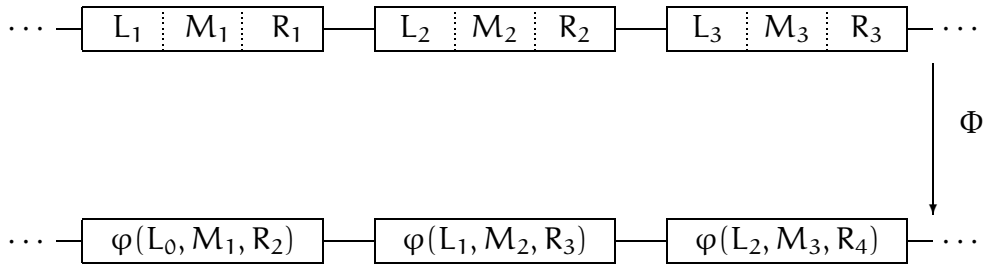

Abbildung 1.2: Arbeitsweise eines PZA mit drei Partitionen

PZA und ZA sind insofern gleichmächtig, als sie sich gegenseitig ohne Zeitverlust simulieren können. Sei dazu $A = (S, N, \varphi)$ ein PZA mit $S = S_1 \times \ldots \times S_N$. Wir definieren den ZA $B = (S, N, \psi)$ mit

$$\begin{aligned}&\psi(s_1, s_2, \ldots, s_N)\\ &= \varphi(s_1, s_2, \ldots, s_N).\end{aligned}$$

Dann ist die globale Überführungsfunktion von B gleich der von A.

Ist umgekehrt $B = (S, N, \psi)$ ein nichtpartitionierter ZA, so konstruieren wir den partitionierten ZA $A = (S^N, N, \varphi)$ mit $\varphi = \psi$ und erhalten ebenfalls gleiche globale Überführungsfunktionen.

Bei partitionierten ZA ist Reversibilität lokal entscheidbar:

Lemma 1.4 (Morita)
Ein PZA (S, N, φ) ist genau dann reversibel, wenn φ eine Bijektion von S ist.

Morita und Harao haben einen detaillierten Beweis gegeben [61]; wir heben hervor, dass für reversible PZA (S, N, φ) der inverse PZA immer durch (S, N, φ^{-1}) gegeben ist.

Bei der Transformation eines partitionierten in einen nicht-partitionierten ZA oder umgekehrt bleibt Reversibilität im Allgemeinen nicht erhalten. Es gibt jedoch eine Linearzeitsimulation von reversiblen ZA mit reversiblen PZA von Durand-Lose [26].

Block-Zellularautomaten

Bei PZA ist Reversibilität deshalb so einfach zu entscheiden, weil Definitions- und Wertebereich von φ gleich groß sind. Block-Zellularautomaten, auch bekannt als ZA mit Margolus–Nachbarschaft, erreichen diese Eigenschaft auf einem etwas anderen Weg; bei ihnen ist φ als *Blockfunktion*, das heißt als Selbstabbildung von S^N, definiert.

Definition 1.3 (Block-ZA)
Ein Block-ZA (BZA) ist ein 4-Tupel (S, N, φ, P) *mit Zustandsmenge* S, *Blockgröße* N, *lokaler Überführungsfunktion* $\varphi : S^N \to S^N$ *und einer endlichen Folge* P *von natürlichen Zahlen.*

Ein BZA wendet seine lokale Überführungsfunktion jeweils relativ zu einer Partitionierung der Menge aller Zellen an. Jede Partitionierung ist durch N und ein Element p von P bestimmt und teilt die Zellen in Blöcke der Länge N ein. Bestimmt p die aktuelle Partitionierung, so sind jeweils die Zellen $k \cdot N + p$ bis $(k+1) \cdot N + p - 1$ in einem Block relativ zum *Ursprung* p zusammengefasst. Anwendung von φ relativ zur Partitonierung p bedeutet, dass φ auf diese Blöcke angewandt wird.

Ein Rechenschritt eines BZA besteht darin, dass nacheinander für alle Elemente p von P die lokale Überführungsfunktion relativ zu p angewandt wird. Offenbar sind Partitionierungen p und p' mit $p \cong p \bmod N$ äquivalent; es reicht aus, p zwischen 0 und $N-1$ zu wählen. Informationsaustausch ist in BZA nur durch den Wechsel der Partitionierung möglich.

Abbildung 1.3 zeigt die Arbeitsweise eines BZA mit Blockgröße zwei. Die waagerechten Linien geben die aktuelle Partitionierung an. Zu Beginn sind die ersten zwei Zellen in einem Block zusammengefasst und die dritte Zelle bildet einen weiteren Block zusammen mit der (nicht abgebildeten) vierten Zelle. Auf diese Blöcke wird die Funktion φ angewandt und liefert die Zustände der Zellen in der zweiten Zeile. Für die beiden Zellen links

erhält man $\varphi(s_1, s_2)$; dies ist der Zustand eines Blocks, aus dem man die Zustände der einzelnen Zellen $s'_1 = \varphi(s_1, s_2)[1]$ und $s'_2 = \varphi(s_1, s_2)[2]$ erhält.

Im folgenden Schritt gehören die zweite und die dritte Zelle zu einem Block; die erste Zelle bildet einen Block zusammen mit der nicht abgebildeten Zelle mit dem Index Null. Auf die Zustände der neu eingeteilten Blöcke wird φ angewandt; damit erhält man $\varphi(s'_1, s'_2)][1]$ für den neuen Zustand der zweiten Zelle. Falls damit alle Partitionierungen abgearbeitet sind, ist ein Berechnungsschritt des BZA vollzogen und für den nächsten fängt man wieder von vorne mit den Partitionierungen an.

Für die globale Überführungsfunktion Φ des BZA aus Abbildung 1.3 gilt damit:

$$\Phi(c)_i = \begin{cases} \varphi(\varphi(c_{i-1}, c_i)[2], \varphi(c_{i+1}, c_{i+2})[1])[1] & \text{oder} \\ \varphi(\varphi(c_{i-2}, c_{i-1})[2], \varphi(c_i, c_{i+1})[1])[2] & \end{cases},$$

je nachdem, ob c_i die linke oder rechte Zelle in einem Block der ersten Partitionierung ist.

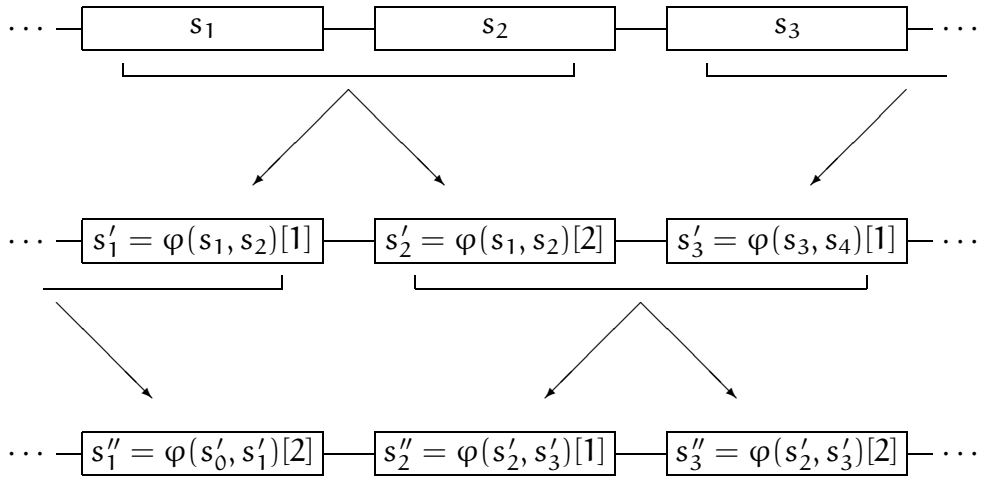

Abbildung 1.3: Arbeitsweise eines BZA mit Blockgröße zwei

BZA unterscheiden sich von anderen ZA dadurch, dass der neue Zustand einer Zelle nicht nur von ihrer Nachbarschaft abhängt, sondern auch

von ihrer Lage relativ zu den Partitionierungen. Dennoch sind BZA und ZA gleich mächtig. BZA mit ZA zu simulieren ist sogar relativ einfach, wenn man die Blöcke aus der ersten Partitionierung als Zellen auffasst. Betrachten wir dazu wieder das Beispiel aus Abbildung 1.3. Wir fassen entsprechend der Abbildung je zwei Zellen zu einem Block zusammen und erhalten „große" Zellen mit den Zuständen $t_1 = [s_1, s_2]$, $t_2 = [s_3, s_4]$ und so weiter. Wir setzen $t_1' = \varphi(s_1, s_2)$, $t_2' = \varphi(s_3, s_4)$ und entsprechend für die übrigen t_i'. Dann gilt nach der zweiten Anwendung von φ

$$t_1'' = [s_1'', s_2''] = [\varphi(t_0'[2], t_1'[1]), \varphi(t_1'[2], t_2'[1])$$

und wir können einen ZA $(S^2, 3, \psi)$ durch

$$\psi([a, b], [c, d], [e, f]) = [\varphi(\varphi(a, b)[2], \varphi(c, d)[1]), \varphi(\varphi(c, d)[2], \varphi(e, f)[1])]$$

definieren, dessen globale Überführungsfunktion gleich der des BZA ist. Da man jeden ZA durch einen ZA mit Nachbarschaftsgröße drei simulieren kann, ist damit gezeigt, dass BZA von ZA ohne Zeitverlust simuliert werden können.

Eine Simulation von ZA mit BZA ist ebenfalls möglich, aber komplizierter. Durand-Lose hat ein Verfahren angegeben, bei dem die Blockgröße des simulierenden BZA der vierfache Radius des simulierten ZA ist [25].

Wie bei PZA ist auch bei BZA Reversibilität leicht zu erkennen:

Lemma 1.5 (Margolus)
Ein BZA (S, N, φ, P) ist genau dann reversibel, wenn φ eine bijektive Selbstabbildung von S^N ist.

Ist (S, N, φ, P) ein reversibler BZA, so ist (S, N, φ^{-1}, P') seine Inverse, wobei P' die gleichen Partitionierungen enthält wie P, aber in umgekehrter Reihenfolge. Durand-Lose hat gezeigt, dass reversible PZA in Linearzeit reversible BZA und reversible ZA simulieren können [26].

Ähnlich wie PZA empfehlen sich BZA durch die Leichtigkeit, mit der sie reversible Konstruktionen erlauben. Es gibt jedoch noch einen tieferen Zusammenhang mit RZA zumindest im ein- und zweidimensionalen Fall. Kari hat gezeigt, dass sich alle ein- und zweidimensionalen RZA bis auf

partielle Verschiebung durch Blockbijektionen darstellen lassen [44]. Eindimensionale ZA kommen mit zwei Blockbijektionen aus, zweidimensionale benötigen vier. Da wir dieses Verfahren später noch verwenden, skizzieren wir hier die wichtigsten Überlegungen.

Definition 1.4 (Partielle Verschiebung)
Sei (S, N, φ) *ein ZA. Weiter seien* U *und* T *zwei endliche Mengen, so dass* $U \times T$ *isomorph zu* S *ist. Jeder Zustand ist damit äquivalent zu einem Paar* (u, t). *Der ZA ist eine* partielle Verschiebung, *wenn es ein* j *zwischen* 1 *und* N *gibt, so dass für alle lokalen Konfigurationen* $((u_1, t_1), \ldots, (u_N, t_N))$ *gilt:*

$$\varphi((u_1, t_1), \ldots, (u_N, t_N)) = (u_{(N-1)/2}, t_j).$$

Sei $A = (S, N, \varphi)$ ein RZA. Wir nehmen an, dass N gross genug ist, dass auch A^{-1} mit der Nachbarschaft N auskommt. Außerdem sei N ungerade und $R = (N-1)/2$. Wir betrachten die Mengen

$$\begin{aligned} R_\varphi &= \{(c_0, \ldots, c_{2R-1}, \varphi(c)_{-R}, \ldots, \varphi(c)_{R-1}\} \\ L_\varphi &= \{(\varphi(c)_0, \ldots, \varphi(c)_{2R-1}, c_{-R}, \ldots, c_{R-1})\} \end{aligned}$$

für $c \in S^{\mathbb{Z}}$. Für reversible ZA gilt

$$|R_\varphi| \cdot |L_\varphi| = |S|^{6R}, \tag{1.2}$$

denn für reversible ZA ist die Abbildung $f_\varphi : S^{6R} \to L_\varphi \times R_\varphi$ mit

$$\begin{aligned} &f_\varphi(c_0, \ldots, c_{6R-1}) \\ &\quad = [(\varphi(c)_R, \ldots, \varphi(c)_{3R-1}, c_0, \ldots, c_{2R-1}), \\ &\qquad (c_{4R}, \ldots, c_{6R-1}, \varphi(c)_{3R}, \ldots, \varphi(c)_{5R-1})] \end{aligned} \tag{1.3}$$

bijektiv.

Nur für einige RZA aber ist $|R_\varphi| = |L_\varphi| = |S|^{3R}$. Letztere sind gerade die, die sich mit Blockbijektionen darstellen lassen. Alle übrigen RZA entstehen aus diesen mittels partieller Verschiebungen. Hat man einen RZA mit $|R_\varphi| = |S|^{3R}$, so erhält man die Blockbijektionen wie folgt.

Da R_φ und S^{3R} die gleiche endliche Zahl von Elementen enthalten, existiert zwischen ihnen eine Bijektion h. Weiter folgt aus $|R_\varphi| = |S|^{3R}$, dass

$|L_\varphi| = |S|^{3R}$ und wir erhalten eine weitere Bijektion k. Aus einem Eingabeblock $(c_0, \ldots, c_{6R-1})$ erhalten wir gemäß Gleichung 1.3 ein Paar (l, r) aus $L_\varphi \times R_\varphi$, nämlich $f_\varphi(c_0, \ldots, c_{6R-1})$. Daraus erhalten wir $(k(l), h(r)) \in S^{3R} \times S^{3R} \equiv S^{6R}$ und definieren $(k(l)h(r))$ als das Ergebnis der ersten Blockbijektion π_1.

Da φ invertierbar ist, können wir entsprechende Betrachtungen auch für φ^{-1} anstellen (φ^{-1} sei die lokale Überführungsfunktion des zu A inversen ZA A^{-1}). Laut Voraussetzung ist die Nachbarschaft groß genug für A^{-1} und A; folglich gilt $|R_\varphi| = |S|^{3R} \Leftrightarrow |R_{\varphi^{-1}}| = |S|^{3R}$) und mit dem gleichen Verfahren wie oben erhalten wir eine zweite Blockbijektion π_2. Bezeichnet nun Π_i für $i = 1, 2$ die globale Funktion, die durch Anwendung von π_i auf jeden Block induziert wird, so gilt:

Lemma 1.6 (Kari)
Aus $|R_\varphi| = |S|^{3R}$ *folgt* $\Phi(c) = (\sigma_L^{3R} \circ \Pi_2^{-1} \circ \sigma_R^{3R} \circ \Pi_1)(c)$.

Dabei steht σ_L^{3R} für die Verschiebung um $3R$ Stellen nach links und σ_R^{3R} für die entsprechende Verschiebung nach rechts.

Man kann dieses Lemma zur Erzeugung reversibler ZA einsetzen: zu gegebenem Alphabet und Radius R wähle man Paare von Blockbijektionen und prüfe jeweils nach, ob die gemäß Lemma 1.6 entstehende globale Überführungsfunktion zu einem ZA mit Radius R gehört. Da liegt nun das Problem: Es gibt $(|S|^{6R})!$ Bijektionen von S^{6R}, also $(|S|^{6R})!^2$ mögliche Paare. Dem stehen $|S|^{|S^{2R+1}|}$ ZA mit Radius R gegenüber, von denen der bei weitem größere Teil nicht reversibel ist. In der Tat gehören einige Paare von Bijektionen zu ZA mit größerem Radius und einige Paare kodieren den gleichen ZA. Insbesondere gibt es $(|S|^{3R})!^2$ verschiedene Kodierungen der Identität mit Radius R: Seien τ_L und τ_R beliebige Bijektionen von S^{3R}. Wir definieren $\pi_1(c_0, \ldots, c_{6R-1})$ durch $(\tau_L(c_0, \ldots, c_{3R-1}), \tau_R(c_{3R}, \ldots, c_{6R-1}))$ und $\pi_2^{-1}(c_0, \ldots, c_{6R-1})$ durch $(\tau_R^{-1}(c_0, \ldots, c_{3R-1}), \tau_L^{-1}(c_{3R}, \ldots, c_{6R-1}))$. Dann sind π_1 und π_2 Blockbijektionen im Sinne von Lemma 1.6 und ihre Kombination ergibt gerade den identischen ZA Φ_{id} mit $\Phi_{id}(c) = c$ für alle $c \in S^{\mathbb{Z}}$. Da τ_L und τ_R beliebige Bijektionen von S^{3R} sein können, folgt die Behauptung.

Für eine effiziente Aufzählung aller RZA eignet sich eher der im folgenden Abschnitt beschriebene algebraische Ansatz.

Halbzentrale Bigruppoide

ZA sind unter anderem algebraische Strukturen. Statt sie über Überführungsfunktionen definieren, könnten wir die Zustandsübergänge auch als das Ergebnis einer Multiplikation von Zustandsvariablen betrachten. Damit erhalten wir RZA als Spezialfälle gewisser Algebren und dies wiederum ermöglicht eine effiziente Aufzählung aller eindimensionalen RZA.

Sei $\varphi : S^N \to S$ die lokale Überführungsfunktion eines ZA. Die globale Funktion Φ ergibt sich dann durch $(\Phi(c))_i = \varphi(c_{i-(N-1)/2}, \ldots, c_{i+(N-1)/2})$ für alle globalen Konfigurationen c. An der Reversibilität ändert sich nichts, wenn wir statt dessen $(\Phi'(c))_i = \varphi(c_i, \ldots, c_{i+|N|})$ verwenden, denn dies entspricht einer Konjugation von Φ mit der $(N-1)/2$-ten Potenz der Verschiebung.

Es ändert sich auch nichts an der Reversibilität, wenn wir statt φ die lokale Funktion $\varphi' : S^{2N-2} \to S^{N-1}$ betrachten, die durch Erweiterung von φ auf Eingaben der Länge $2N-2$ entsteht.

So können wir unseren ZA durch einen ersetzen, dessen lokale Überführungsfunktion sich auch als $\psi : S^{N-1} \times S^{N-1} \to S^{N-1}$ schreiben läßt, also als eine binäre Operation. Ist der ZA reversibel, so erhalten wir aus seiner Inversen mit der gleichen Überlegung eine binäre Operation ψ^{-1} und es gilt:

$$\psi(\psi^{-1}(t,s),\psi^{-1}(s,u)) = s$$
$$\psi^{-1}(\psi(t,s),\psi(s,u)) = s$$

für $s,t,u \in S^{N-1}$. Damit erfüllt (S^{N-1},ψ,ψ^{-1}) die folgende Definition eines halbzentralen Bigruppoides.

Definition 1.5 (Halbzentrales Bigruppoid)
Ein halbzentrales Bigruppoid *ist eine Algebra* $(A,\bullet,\circ)$ *mit*

$$(a \bullet b) \circ (b \bullet c) = b \text{ } \textit{und} \tag{1.4}$$
$$(a \circ b) \bullet (b \circ c) = b. \tag{1.5}$$

Jeder eindimensionale RZA entspricht einem halbzentralen Bigruppoid und umgekehrt. Wer effizient alle halbzentralen Bigruppoide einer gewissen

Größe aufzählen kann, hat auch ein effizientes Verfahren, um eindimensionale RZA zu finden. T. Boykett hat dies implementiert. Wir skizzieren das Verfahren und verweisen für Details auf seinen Aufsatz [8].

Ein halbzentrales Bigruppoid ist in einer der beiden Operationen genau dann idempotent, wenn es auch in der anderen Operation idempotent ist. Die idempotenten halbzentralen Bigruppoide dienen als Repräsentanten von Klassen.

Definition 1.6 (Anhebung)
Ist $(A, \bullet, \circ)$ *ein halbzentrales Bigruppoid und* $\pi : A \to A$ *eine Permutation, so heißt die Algebra* $(A, *, +)$ *mit*

$$a * b = \pi^{-1}(a \bullet b) \text{ und} \tag{1.6}$$

$$a + b = \pi(a) \circ \pi(b) \tag{1.7}$$

die Anhebung *von* $(A, \bullet, \circ)$ *mit* π.

Die Anhebung ist selbst ein halbzentrales Bigruppoid. Es gilt:

Lemma 1.7 (Boykett)
Jedes halbzentrale Bigruppoid $(A, \bullet, \circ)$ *besitzt eine eindeutige Darstellung aus einem idempotenten halbzentralen Bigruppoid und einer Permutation aus der symmetrischen Gruppe von* A.

Um die Isomorphie von halbzentralen Bigruppoiden zu entscheiden, reicht es aus, sich auf ihre idempotenten Repräsentanten zu konzentrieren.

Lemma 1.8 (Boykett)
Halbzentrale Bigruppoide $(A, \bullet, \circ)$ *und* $(B, *, +)$ *sind genau dann isomorph, wenn es einen Isomorphismus* $\beta : A \to B$ *gibt, so dass ihre idempotenten Repräsentanten modulo* β *isomorph sind und* $\beta(A \bullet A) = (B * B)\beta$ *gilt.*

Wir müssen also nur noch die Isomorphie idempotenter halbzentraler Bigruppoide entscheiden, und dies erfolgt mittels *Rechteckstrukturen*:

Definition 1.7 (Rechteckstruktur)
Sei A *eine Menge. Ein* Rechteck *über* A *ist ein geordnetes Paar von Teilmengen von* A. *Eine Ansammlung* $\mathcal{R}$ *solcher Rechtecke heißt eine* Recht-

eckstruktur *von* A, *wenn*

$$\forall (a,b) \in A^2 \; \exists! \; R \in \mathcal{R} \textit{ mit } (a,b) \in R \textit{ und} \tag{1.8}$$

$$\forall R, Q \in \mathcal{R} \textit{ gilt } |R_1 \cap Q_2| = 1, \tag{1.9}$$

wobei R *für* $R_1 \times R_2$ *steht.*

Zwei Rechteckstrukturen sind isomorph, wenn es zwischen ihren zugrundeliegenden Mengen eine Bijektion gibt, die Rechtecke erhält. Zu jedem idempotenten halbzentralen Bigruppoid existiert eine Rechteckstruktur, die unter Anhebung erhalten bleibt, nämlich

$$\mathcal{R}^\bullet = \{R_x^\bullet = \{(a,b) | a \bullet b = x\} | x \in A\}. \tag{1.10}$$

Diese betrachten wir als die kanonische mit diesem halbzentralen Bigruppoid assoziierte Rechteckstruktur. Zwei idempotente halbzentrale Bigruppoide sind genau dann isomorph, wenn ihre zugehörigen Rechteckstrukturen isomorph sind. Boykett gibt einen Algorithmus an, der effizient Isomorphieklassen von Rechteckstrukturen aufzählt und kann so RZA erzeugen.

Der Vorteil an dieser Methode ist ihre Geschwindigkeit. Andererseits ist es ein weiter Weg von einer Rechteckstruktur zu einer Klasse von RZA. Es ist schwierig, hier äquivalente oder triviale ZA zu eliminieren. Außerdem läßt sich das Verfahren im Gegensatz zu der Methode nach Kari nicht auf höhere Dimensionen übertragen.

1.3.3 Häufigkeit und Struktur von RZA

Einleitung

RZA sind selten. Das ist nicht überraschend, denn Reversibilität ist für die meisten Berechnungsmodelle eine erhebliche Einschränkung. Man weiß, dass RZA bezüglich einer punktweisen Topologie eine spärliche Untermenge aller ZA bilden [76] und dass alle eindimensionalen RZA mit Alphabetgröße zwei und Nachbarschaftsgröße zwei oder drei kongruent zur Identität sind [3, 39].

Daher stellt sich die Frage, ob RZA überhaupt ein sinnvolles Modell sind – gestatten sie nichttriviales Verhalten, sind sie als Berechnungsmodell universell? Die Antwort ist beide Male „ja“, wenn auch mit Einschränkungen.

Bevor wir dazu kommen, wollen wir aber begründen, warum RZA so selten sind. Offenbar hat Reversibilität Folgen für die Gestalt der Überführungsfunktion; diese Vermutung werden wir präzisieren.

Zu diesem Zweck betrachten wir beispielhaft ZA mit $|S| = 2$ und $N \leq 5$ sowie mit $|S| = 3$ und $N \leq 3$. Wir ermitteln, wie viele RZA mit diesen Parametern es gibt, teilen sie in Äquivalenzklassen ein und unterscheiden triviale von nichttrivialen RZA. Dabei nennen wir einen ZA *trivial*, wenn er sich nur durch die elementaren Operationen Verschiebung und Alphabetpermutation von der identischen Abbildung unterscheidet.

Wir beginnen mit der Definition der Äquivalenzklassen, weil diese auch beim Berechnen der RZA hilfreich sind.

Äquivalente ZA

Wir haben bis jetzt implizit zwei ZA als äquivalent betrachtet, wenn sie die gleiche globale Überführungsfunktion besitzen. Nun führen wir zwei etwas weiter gefasste Äquivalenzbegriffe ein, die ZA auch dann als äquivalent betrachten, wenn ihre globalen Überführungsfunktionen sich nur durch Alphabetpermutation beziehungsweise Verschiebung unterscheiden.

Definition 1.8 (Äquivalenz modulo Alphabetpermutation)
RZA $A = (S, N, \varphi)$ *und* $B = (S, N, \psi)$ *sind* äquivalent modulo einer Alphabetpermutation, *wenn es eine Bijektion* π *von* S *gibt, so dass* $\varphi(w) = \psi(\pi(w))$ *für alle* $w \in S^N$ *gilt, wenn man für* $w = w_1 w_2 \dots w_N$ *(mit* $w_j \in S$*)* $\pi(w)$ *durch* $\pi(w_1)\pi(w_2)\dots\pi(w_N)$ *definiert.*

Definition 1.9 (Äquivalenz modulo Verschiebung)
RZA A *und* B *wie eben heißen* äquivalent modulo Verschiebung, *wenn es ein* $k \in \mathbb{Z}$ *gibt, so dass für alle* $c \in S^{\mathbb{Z}}$ $A(c) = \sigma^k(B(c))$ *ist, wobei* σ *die elementare Verschiebung bezeichnet.*

Ein RZA heißt *trivial*, wenn er modulo Verschiebung oder Alphabetpermutation äquivalent zur identischen Abbildung ist.

Wir teilen nun RZA in Äquivalenzklassen bezüglich Alphabetpermutation ein. Als kanonischen Vertreter einer Klasse legen wir dabei den RZA fest, der für alle $s \in S$ auf s^N den Wert s annimmt. Damit erhalten wir für jede Klasse genau einen Vertreter:

Lemma 1.9
Ist $A = (S, N, \varphi)$ ein RZA, so gilt für alle $s \neq t \in S$: $\varphi(s^N) \neq \varphi(t^N)$.

Beweis: Angenommen, es gäbe $s \neq t$ mit $\varphi(s^N) = \varphi(t^N)$. Sei c die globale Konfiguration mit $c_i = s$ und d diejenige mit $d_i = t$ für alle $i \in \mathbb{Z}$. Dann ist $A(c) = A(d)$, folglich ist A nicht injektiv.

Außerdem ist A modulo einer Alphabetpermutation π äquivalent zu einem RZA $B = (S, N, \psi)$ mit $\psi(s^N) = s$ für alle $s \in S$: für $\varphi(s^N) = t$ setzen wir $\pi(s) = t$. □

Eine weitere reversibilitätserhaltende Transformation auf RZA ist die *Spiegelung*. Das Spiegelbild von Wörtern aus S^* ist durch

$$\varepsilon^R = \varepsilon \text{ und } (xw)^R = (w^R x)$$

mit dem leeren Wort ε, $x \in S$ und $w \in S^*$ definiert. Zu einem ZA $A = (S, N, \varphi)$ ist das Spiegelbild $A^R = (S, N, \varphi^R)$ durch $\varphi^R(w) = \varphi(w^R)$ für alle $w \in S^N$ gegeben. A und A^R verhalten sich auch global spiegelbildlich und deshalb betrachten wir sie als ähnlich.

Lemma 1.10
Ist A ein RZA, so ist auch A^R ein RZA.

Beweis: Angenommen, φ wäre injektiv und φ^R nicht. Dann gibt es Wörter $u \neq v$ gleicher Länge k über S, so dass φ^R auf den periodischen Wörtern $\ldots vvv \ldots$ und $\ldots uuu \ldots$ den gleichen Wert annimmt. Dies impliziert für alle $1 \leq i \leq k$

$$\begin{aligned}&\varphi^R(u_{i-(N-1)/2 \bmod k}, \ldots, u_{i+(N-1)/2 \bmod k})\\ &= \varphi^R(v_{i-(N-1)/2 \bmod k}, \ldots, v_{i+(N-1)/2 \bmod k}).\end{aligned}$$

Das ist äquivalent zu

$$\begin{aligned}&\varphi(u_{i+(N-1)/2 \bmod k}, \ldots, u_{i-(N-1)/2 \bmod k})\\ &= \varphi(v_{i+(N-1)/2 \bmod k}, \ldots, v_{i-(N-1)/2 \bmod k}),\end{aligned}$$

damit nimmt φ auf den verschiedenen periodischen Wörtern $\ldots v^R v^R v^R \ldots$ und $\ldots u^R u^R u^R \ldots$ die gleichen Werte an, ist also ebenfalls nicht injektiv. □

ZA A und B wie oben heißen *komplementär*, wenn für alle Wörter $w = w_1 \ldots w_N$ aus S^N gilt:

$$\varphi(w) = |S| - \psi(\overline{w}) \bmod |S|,$$

mit $\overline{w} = \overline{w_1 w_2} \ldots \overline{w_N}$ und $\overline{w_i} = |S| - w_i \bmod S$. Wir schreiben $\overline{A}$ für den zu A komplementären ZA.

A und $\overline{A}$ verhalten sich ähnlich; dies kann man zum Beispiel dadurch sehen, dass $\overline{A}$ sich auch als $h \circ A \circ h$ schreiben lässt, wobei h gerade die Alphabetpermutation von S mit $h(s) = |S| - s$ ist. Wieder gilt daher: ist A reversibel, so auch $\overline{A}$. Komplement und Spiegelbild ändern auch nichts an der Trivialität:

Lemma 1.11
Mit A sind auch A^R und $\overline{A}$ trivial.

Beweis: Sind A und B äquivalent modulo Alphabetpermutation oder Verschiebung, so gilt dies auch für A^R und B^R beziehungsweise $\overline{A}$ und $\overline{B}$. Ist aber B der identische ZA, so ist B^R eine Verschiebung und $\overline{B} = B$. □

Da wir am Verhaltensspektrum von RZA interessiert sind, reicht es aus, wenn wir aus jeder Äquivalenzklasse modulo Verschiebung, Alphabetpermutation, Spiegelung und Komplement genau einen Vertreter betrachten. Um systematisch alle RZA mit den gewählten Größen $|S|$ und N zu erzeugen, könnte man zum Beispiel halbzentrale Bigruppoide einsetzen; für relativ kleine Parameter reicht es jedoch aus, alle in Frage kommenden Regeln von ZA zu erzeugen und jede auf Reversibilität zu prüfen. Dabei kann man die Balanciertheit und Lemma 1.9 ausnutzen, um den Suchraum zu verkleinern.

Tabelle 1.1 zeigt den Anteil der RZA an allen ZA für einige Werte von $|S|$ und N. Die dritte Spalte enthält die Anzahl möglicher Regeln (das ist $|S|^{|S^N|}$), die vierte gibt an, wie viele davon reversibel sind. In der fünften

Spalte steht die Anzahl Äquivalenzklassen reversibler ZA modulo Alphabetpermutation, Verschiebung, Spiegelbild und Komplement.

$\|S\|$	N	insgesamt	reversibel	reduziert
2	2	16	4	1
2	3	256	6	1
2	4	65536	16	2
2	5	$4.29 \cdot 10^9$	62	7
3	2	19683	48	3
3	3	$7.63 \cdot 10^{12}$	1776	101
4	2	$4.29 \cdot 10^9$	5184	ca. 60

Tabelle 1.1: Totale und reduzierte Anzahl von RZA im Vergleich zur Gesamtmenge der ZA für die angegebenen Werte von $|S|$ und N. Die Angaben in der dritten Spalte sind auf die zweite Nachkommastelle gerundet.

Modulo Alphabetpermutation reduziert sich die Anzahl reversibler ZA um $|S|!$, modulo Verschiebung um N. Spiegelbild und Komplement halbieren die Zahl nochmals. Dass die Zahlen in der fünften Spalte nicht genau das $(|S|! \cdot N \cdot 4)^{-1}$-fache der Zahlen aus der vierten Spalte sind, liegt daran, dass einige ZA ihr eigenes Spiegelbild beziehungsweise Komplement sind und dass gelegentlich das Spiegelbild mit Komplement oder einer Verschiebung übereinstimmt.

An Tabelle 1.1 kann man unter anderem folgendes ablesen. Wie seit längerem bekannt sind alle RZA mit $|S| = 2$ und $N \leq 3$ trivial. Für größere Werte von $|S|$ und N gibt es jedoch RZA, die zumindest nicht in dem strengen Sinn einer Äquivalenz zur Identität trivial sind. Der Anteil reversibler ZA an der Gesamtmenge aller ZA ist verschwindend gering; die absoluten Zahlen wachsen zwar mit N und vor allem mit $|S|$, der prozentuale Anteil nimmt aber eher ab.

Sieht man die Vertreter der Äquivalenzklassen von RZA genauer an, so stellt man fest, dass viele von ihnen sich zeitperiodisch verhalten; das heißt, zu jeder Konfiguration $c \in S^{\mathbb{Z}}$ gibt es ein $k \in \mathbb{N}$, so dass $A^k(c) = c$ oder $A^k(c) = \sigma^t(c)$ für ein $t \in \mathbb{N}$. In der Tat reicht für viele der kleineren RZA

$\|S\|$	N	RZA	davon zu sich selbst invers
2	2	4	4
2	3	6	6
2	4	16	16
2	5	62	54
3	2	48	48
3	3	1776	648
4	2	5184	704

Tabelle 1.2: Anzahl zu sich selbst inverser RZA

sogar gleichmäßig $k = 1$: Sie sind zu sich selber invers. Tabelle 1.2 zeigt, für wie viele der untersuchten RZA dies der Fall ist. Dabei wurde auf die Reduktion modulo Äquivalenzrelationen verzichtet, weil zum Beispiel die Verschiebung nicht selbstinvers ist.

Sollen zu sich selbst inverse ZA als trivial gelten, so reduziert sich damit die Anzahl potentiell interessanter RZA weiter. Von den verbleibenden sind einige mit größerer Periode als Eins zeitperiodisch. Für größere Zeitperioden haben wir die Anzahlen nicht berechnet, denn man müsste dann entscheiden, ab welcher Periodenlänge man einen ZA nicht mehr als trivial einstuft. Darüber hinaus ist Zeitperiodizität im Allgemeinen nicht algorithmisch entscheidbar [15].

Zur Struktur von RZA

Genauere Untersuchung der Überführungsfunktionen von RZA zeigt, dass RZA nicht nur selten, sondern auch im Raum aller möglichen Überführungsfunktionen ungleichmäßig verteilt sind: Es gibt Gruppen von RZA, deren Überführungsfunktionen sich nur durch den Austausch weniger Werte unterscheiden, während andererseits Überführungsfunktionen mit bestimmten Kombinationen von Werten überhaupt nicht vorkommen.

Letzteres ist einfach zu erklären. Lemma 1.9 behandelt einen Spezialfall – keine Überführungsfunktion φ mit $\varphi(s^N) = \varphi(t^N)$ für $s \neq t \in S$ ist rever-

sibel. Ein weiteres Beispiel erhält man aus periodischen Konfigurationen der Form $\ldots ststst \ldots$. Sei c eine solche Konfiguration und $\sigma(c)$ die Konfiguration, die entsteht, wenn man c um eine Stelle verschiebt. Ein reversibler ZA muss auf c und $\sigma(c)$ verschiedene Werte annehmen; dies kann er nur tun, wenn für seine lokale Überführungsfunktion gilt: $\varphi((sts)^N) \neq \varphi((tst)^N)$.

Diese Idee kann man verallgemeinern: Sei T eine Teilmenge von S^N der Art, dass es mindestens zwei verschiedene periodische Konfigurationen gibt, in denen nur Elemente von T als Teilwörter der Länge N vorkommen. Ein ZA ist bereits dann nicht reversibel, wenn er eingeschränkt auf diese aus T konstruierten Konfigurationen nicht injektiv ist. Konsequent weiterverfolgt führt dieser Ansatz auf den Algorithmus von Amoroso und Patt. Da es Wörter in S^N gibt, aus denen sich sehr kleine Mengen T bilden lassen (Wörter der Form s^N sind ein Beispiel), folgt für die Überführungsfunktionen reversibler ZA, dass durch Wahl einiger weniger Werte schon eine ganze Reihe weiterer Stellen eingeschränkt sind. Eine statistische Untersuchung bestätigt dies [36].

Mit Hilfe des Darstellungssatzes von Kari kann man diese Beobachtungen weiter präzisieren. Dazu legen wir nach und nach die Werte von φ fest und prüfen nach jedem Schritt, ob $|L_\varphi|$ und $|R_\varphi|$ noch nicht größer als $|S|^{3R}$ sind.

Wir beginnen mit dem Beispiel $|S| = 2, N = 3$. Für R_φ ermitteln wir für jedes Paar $(a, b) \in S^2$ die Menge $R_\varphi^{a,b} := \{(x, y) : \exists (c, d) \in S^2 : \varphi(cdab) = xy\}$. Entsprechend definieren wir $L_\varphi^{a,b} := \{(x, y) : \exists (c, d) : \varphi(abcd) = xy\}$. Es gilt $R_\varphi = \cup_{a,b \in S} R_\varphi^{a,b}$ und entsprechend für L_φ.

Wie oben legen wir (modulo Äquivalenz ohne Beschränkung der Allgemeinheit) fest, dass $\varphi(000) = 0$ und $\varphi(111) = 1$ gilt. Für die übrigen Werte von φ verwenden wir zunächst Variable: $\varphi(001) = a, \ldots, \varphi(110) = f$. Tabelle 1.3 zeigt, was wir bis jetzt über φ wissen.

Jede Belegung der Variablen a bis f entspricht einem ZA. In Zeile j stehen die Elemente von L_φ^j, in Spalte i die Elemente von R_φ^i. Da wir wissen, dass alle RZA balanciert sind und dass $\varphi(010) \neq \varphi(101)$, also $b \neq e$, gelten muss, bleiben von den 64 Möglichkeiten für φ elf übrig.

Wir zählen in jeder Spalte, wie viele verschiedene Werte sie enthält; die Summe dieser Zahlen ist gerade $|R_\varphi|$. Von den elf Überführungsfunktionen

	00	01	10	11
00	00	0a	ab	ac
01	bd	be	cf	c1
10	d0	da	eb	ec
11	fd	fe	1f	11

Tabelle 1.3: Es ist jeweils $\varphi(xy)$ angegeben, wobei x der Zeilen- und y der Spaltenindex ist.

erfüllt nur eine die Bedingung $|R_\varphi| = 8$. Die übrigen RZA mit $|S| = 2, N = 3$ sind zu dieser einen Lösung über Verschiebung oder Permutation äquivalent – die Äquivalenzklasse modulo Permutation haben wir mittels $\varphi(000)$ und $\varphi(111)$ festgelegt, diejenige modulo Verschiebung ist im Ansatz von Kari implizit. Für L_φ zählt man statt der Spalten die Zeilen.

Um diesen Ansatz auf ZA mit größerem Alphabet und größerer Nachbarschaft zu verallgemeinern, müsste man Tabellen mit $|S|^{2R}$ Zeilen und Spalten aufstellen und für jede mögliche Belegung die Elemente von R_φ zählen; das ist nicht praktisch. Eine stärkere Aussage als Gleichung 1.2 erleichtert das Verfahren:

Lemma 1.12
Zu einem ZA (S, N, φ), $R = (N-1)/2$ *und* $w \in S^{2R}$ *sei*

$$R_\varphi^w = \{v \in S^{2R} | \exists u \in S^{2R} \textit{ mit } \varphi(uw) = v\},$$
$$L_\varphi^w = \{v \in S^{2R} | \exists u \in S^{2R} \textit{ mit } \varphi(wu) = v\}.$$

Dann ist

$$|R_\varphi| = |S|^{3R} \Leftrightarrow |R_\varphi^w| = |S|^R \forall w \in S^{2R}$$

und

$$|L_\varphi| = |S|^{3R} \Leftrightarrow |L_\varphi^w| = |S|^R \forall w \in S^{2R}$$

Beweis: Wir zeigen als Erstes, dass aus $|R_\varphi| \cdot |L_\varphi| = |S|^{6R}$ folgt:

$$|R_\varphi^w| \cdot |L_\varphi^v| = |S|^{2R} \tag{1.11}$$

für alle $v, w \in S^{2R}$. Laut dem Beweis von Kari existiert eine Bijektion f_φ zwischen S^{6R} und $L_\varphi \times R_\varphi$. Wenn wir nun v und w aus S^{2R} beliebig aber fest wählen, gibt es $|S|^{2R}$ Wörter in $v \cdot S^{2R} \cdot w$; f_φ weist jedem von ihnen genau ein Element von $L_\varphi \times R_\varphi$ zu. Um zu sehen, welches das ist, sei c eine globale Konfiguration, die uvw als Teilwort enthält, so dass $c_{0\ldots2R-1} = v$, $c_{2R\ldots4R-1} = u$ und $c_{5R\ldots6R-1} = w$. Dann gilt nach Gleichung 1.3

$$\begin{aligned} f_\varphi(v\,u\,w) &= f_\varphi(v_0, \ldots, v_{2R-1}, u_0, \ldots, u_{2R-1}, w_0, \ldots, w_{2R-1}) \\ &= [(\varphi(c)_R, \ldots, \varphi(c)_{3R-1}, v), (w, \varphi(c)_{3R}, \ldots, \varphi(c)_{5R-1})]. \end{aligned} \tag{1.12}$$

Demnach muss man für verschiedene u und gleichbleibende v und w jeweils unterschiedliche Werte für $\varphi(c)_R, \ldots, \varphi(c)_{5R-1}$ erhalten; daraus folgt Gleichung 1.11. Sei nun (S, N, φ) ein RZA mit $|R_\varphi| = |S|^{3R}$; weil dann auch $|L_\varphi| = |S|^{3R}$ ist, gilt Gleichung 1.11.

Angenommen, es gäbe ein $w \in S^{2R}$ mit $|R_\varphi^w| < |S|^R$. Dann gibt es wegen Gleichung 1.11 ein $k \in \mathbb{N}$, $k > 1$ mit $|R_\varphi^w| = |S|^R/k$ und für alle $v \in S^{2R}$ gilt $|L_\varphi^v| = k|S|^R$.

Andererseits ist

$$L_\varphi = \bigcup_{v \in S^{2R}} L_\varphi^v,$$

also

$$|L_\varphi| = \sum_{v \in S^{2R}} |L_\varphi^v| = \sum_{v \in S^{2R}} k|S|^R = k|S|^{3R},$$

was nur für $k = 1$ wahr sein kann.

Angenommen, es gäbe ein $w \in S^{2R}$ mit $|R_\varphi^w| > |S|^R$. Dann gibt es wegen $\sum_{w \in S^{2R}} |R_\varphi^w| = |S|^{3R}$ auch ein u mit $|R_\varphi^u| < |S|^R$. Damit ist die Behauptung für R_φ bewiesen; der Beweis für L_φ erfolgt analog. □

Aus Lemma 1.12 folgt, dass ein ZA (S, N, φ) nur genau dann reversibel ist, wenn er

1. für alle $w \in S^{2R}$ die Bedingung $|R_\varphi^w| = |S|^R$ erfüllt oder

2. äquivalent zu einem ZA mit größerem Radius ist, der die Bedingung erfüllt (wobei Äquivalenz bedeutet, dass beide ZA die gleiche globale Überführungsfunktion haben) oder

3. durch partielle Verschiebung aus einem ZA hervorgeht, der die Bedingung erfüllt.

Der zweite Fall tritt dann auf, wenn der ZA zwar reversibel ist, aber seine Inverse eine größere Nachbarschaft benötigt.

In Tabelle 1.3 und in den entsprechenden Tabellen für größere $|S|$ und R reicht es also aus, zu zählen, ob in jeder Zeile oder Spalte genau $|S|^R$ verschiedene Elemente vorkommen. Daraus folgt in der Tat eine erhebliche Einschränkung der möglichen Überführungsfunktionen.

Nach diesen Überlegungen stellt sich die Frage, ob es überhaupt interessante RZA gibt – sind sie vielleicht alle zeitperiodisch? Das ist nicht der Fall. Zunächst ein nichtkonstruktives algebraisches Argument:

Die RZA bilden eine Gruppe $\mathcal{A}$, nämlich die Homöomorphismengruppe von $S^{\mathbb{Z}}$ bezüglich der Cantor-Topologie (das ist die Produkttopologie, die von der diskreten Topologie auf den einzelnen Zellen erzeugt wird). Ein Satz von Curtis, Hedlund und Lyndon [37] besagt, dass jede endliche Gruppe zu einer Untergruppe von $\mathcal{A}$ isomorph ist. Daraus folgt, dass es zumindest RZA mit beliebig langen Zeitperioden gibt.

Darüber hinaus werden wir im folgenden Abschnitt sehen, dass RZA beliebige Turingmaschinen simulieren können. Daraus folgt insbesondere die Existenz nicht zeitperiodischer RZA.

1.4 Simulation von ZA mit RZA

1.4.1 Einleitung

Unsere Motivation für das Studium von RZA sind Quantenzellularautomaten; die Motivation hinter der Entwicklung von Quantenrechnern ist die erhoffte Leistungssteigerung im Vergleich mit klassischen Computern. Von

daher liegt es nahe, nach dem Preis der Reversibilität zu fragen – wieviel zusätzliche Ressourcen benötigt ein RZA, um einen ZA zu simulieren?

Hierauf gibt es verschiedene Antworten je nachdem, was genau man unter Simulation versteht und ob man bereit ist, die zu simulierenden ZA einzuschränken. Wir zeigen zunächst, dass eine strenge Definition keine Simulation zulässt und gehen dann auf verschiedene bekannte Verfahren ein. Diese ermöglichen meist nur die Simulation von ZA auf endlichen Konfigurationen; wir skizzieren jedoch abschließend eines, das auf beliebigen Konfigurationen funktioniert.

1.4.2 Simulation im strengen Sinn

Wir beginnen mit einer strengen Definition von Simulation. Unter dem Gesichtspunkt eines Einsatzes von ZA als universelle Rechner könnte man *ergebnisorientierte* Simulation verlangen; sei dazu $A = (S, N, \varphi)$ ein ZA, der eine Sprache $L \subseteq T^*$ für ein $T \subset S$ erkennt. Das heißt, eine gewisse ausgezeichnete Zelle nimmt unter Anwendung von A genau dann in endlicher Zeit einen ausgezeichneten (akzeptierenden) Zustand ein, wenn A auf einer Konfiguration gestartet wird, die einem Wort aus L entspricht.

Definition 1.10 (ergebnisorientierte Simulation)
Sei $A = (S_A, N_A, \varphi_A)$ *ein ZA, der die Sprache* L_A *erkennt. Der ZA* $B = (S_B, N_B, \varphi_B)$ *simuliert* A *ergebnisorientiert, wenn es einen Alphabethomomorphismus* $h : S_A \to S_B$ *gibt (den man zu einem Homomorphismus* $S_A^* \to S_B^*$ *fortsetzen kann), so dass* B *die Sprache* L_B *erkennt und gilt:*

$$h^{-1}(L_B) = \bigcup_{w \in L_B} \{\, h(w) \,\} = L_A.$$

Es ist unentscheidbar, ob ZA sich ergebnisorientiert simulieren, denn ein entsprechendes Verfahren müsste die Äquivalenz beliebiger Turingmaschinen erkennen. Wir gehen daher von einem strengeren Begriff aus, der *schrittweisen* Simulation, wie sie zum Beispiel Delorme definiert [19].

Definition 1.11 (schrittweise Simulation)
Seien $A = (S, N, \varphi)$ *und* $B = (T, M, \psi)$ *zwei ZA. Wir sagen, dass der ZA* B *den ZA* A *schrittweise simuliert, wenn es eine Abbildung* $h : T \to S$ *gibt,*

so dass für alle Konfigurationen c *über* T *gilt:*

$$\Phi(h(c)) = h(\Psi(c)). \tag{1.13}$$

Dabei stehen Φ *und* Ψ *wieder für die globalen Überführungsfunktionen zu* φ *und* ψ.

Wir sprechen von *reversibler Simulation*, wenn der simulierende ZA reversibel ist.

Lemma 1.13
Sei A *ein ZA wie in Definition 1.11. Wenn man* T *und* h *(ebenfalls wie in der Definition) nicht so wählen kann, dass* A *auf Konfigurationen über* $h(T)$ *surjektiv ist, kann* A *nicht schrittweise reversibel simuliert werden.*

Beweis: Ist A auf Konfigurationen über $h(T)$ nicht surjektiv, so gibt es eine Konfiguration $d \in (h(T))^{\mathbb{Z}}$, die unter der globalen Überführungsfunktion Φ von A kein Urbild hat. Andererseits gibt es mindestens eine Konfiguration $c \in S^{\mathbb{Z}}$ mit $h(c) = d$. Nehmen wir an, $B = (T, M, \psi)$ wäre ein RZA, der A schrittweise simuliert. Da die globale Überführungsfunktion Ψ von B bijektiv ist, existiert $\Psi^{-1}(c)$.

Aus $\Psi(\Psi^{-1}(c)) = c$ folgt aber $h(\Psi(\Psi^{-1}(c))) = d$; andererseits ist mit Gleichung 1.13 $h(\Psi(\Psi^{-1}(c))) = \Phi(h(\Psi^{-1}(c)))$, also $\Phi(h(\Psi^{-1}(c))) = d$, im Widerspruch zu der Annahme, d habe kein Urbild unter Φ. □

Der Simulationsbegriff aus Definition 1.11 ist demnach für unsere Zwecke zu streng. Man kann die Definition zum Beispiel dadurch erweitern, dass man für h nicht nur Alphabethomomorphismen zulässt. Falls man keine Einschränkungen an h macht, erhält man ebenfalls keinen sinnvollen Simulationsbegriff, weil man dann die Simulation vollständig in die Funktion h verlagern kann, wie Hertling gezeigt hat [38].

Er definiert die *Einbettung* von $A = (S, N, \varphi)$ in $B = (T, M, \psi)$ als ein Paar von Funktionen $\mu : S^{\mathbb{Z}} \to T^{\mathbb{Z}}$ und $\nu : T^{\mathbb{Z}} \to S^{\mathbb{Z}}$ so dass für alle $t \in \mathbb{N}$ gilt:

$$\Phi^t = \nu \circ \Psi^t \circ \mu,$$

wobei Φ^t (Ψ^t) für die t-fach iterierte globale Überführungsfunktion von A (B) steht. Da die Gleichung auch für $t = 0$ gelten soll, muss μ injektiv sein. Hertling lässt zu, dass A und B ZA unterschiedlicher Dimension sind; wir geben hier seine Ergebnisse nur für den eindimensionalen Fall an.

Lemma 1.14 (Hertling)
Falls keine weiteren Einschränkungen an μ und ν vorliegen, ist jeder ZA in den RZA $(\{0,1\},2,\sigma)$ (also in die Verschiebung) einbettbar.

Der Beweis nutzt aus, dass die eigentliche Simulation vollständig von den Funktionen ν und μ übernommen werden kann. Eine relativ schwache Einschränkung an μ reicht aus, um dies zu verhindern: Man muss nur fordern, dass μ mit der Verschiebung kommutiere. Da ZA selbst dadurch charakterisiert sind, dass sie mit der Verschiebung kommutieren, ist diese Forderung naheliegend. Hertling hat eine wesentlich verstärkte Version von Lemma 1.13 bewiesen:

Lemma 1.15 (Hertling)
Falls μ mit der Verschiebung kommutieren muss, ist kein irreversibler eindimensionaler ZA in einen reversiblen eindimensionalen ZA einbettbar.

Eine strenge Definition führt folglich nicht zu einem brauchbaren Simulationsbegriff. Eine weitere Abschwächung der Forderung an μ erscheint ebenfalls nicht sinnvoll; man kann aber andere Elemente der Simulationsdefinition verändern. Beispielsweise kann man beliebige d-dimensionale ZA mit $d+1$-dimensionalen RZA ohne Zeitverlust simulieren. Falls man die zusätzliche Dimension vermeiden will, kann man Zeitverlust in Kauf nehmen.

1.4.3 Zusätzliche Dimensionen

Toffoli hat gezeigt [80], dass man jeden d-dimensionalen ZA mit einem $d+1$-dimensionalen RZA ohne Zeitverlust simulieren kann.

Sei dazu A ein d-dimensionaler ZA über dem Alphabet S. Eine globale Konfiguration für A ist ein Element von $S^{\mathbb{Z}^d}$. Die Idee von Toffoli besteht

darin, die aktuelle Konfiguration von A als eine Hyperebene in $S^{\mathbb{Z}^{d+1}}$ einzubetten und sämtliche Vorgängerkonfigurationen in parallelen Hyperebenen zu speichern.

Mit dieser Methode wurde zum ersten Mal bewiesen, dass RZA zu universeller Simulation von allgemeinen ZA fähig sind; daraus folgt insbesondere die Berechnungsvollständigkeit reversibler zweidimensionaler ZA, weil bekannt ist, dass eindimensionale ZA universelle Turingmaschinen simulieren können. Praktisch bedeutet die zusätzliche Dimension so viel zusätzlichen Aufwand, dass sie nur aus prinzipiellen Gründen interessant ist.

1.4.4 ZA zweiter Ordnung

Eine weitere Idee zur reversiblen Simulation stammt von Toffoli und Margolus [82]; wir stellen sie kurz vor und begründen, warum sie für unsere Zwecke nicht nützlich ist. Sei $A = (S, 3, \varphi)$ ein irreversibler ZA (die Beschränkung auf Nachbarschaftsgröße drei ist nicht wesentlich und dient nur der leichteren Darstellung). Wir wählen eine Menge T mit $T \cong S^2$ und simulieren $\varphi : S^3 \to S$ mittels einer Funktion $\psi : T^3 \to T$. Dabei interpretieren wir $(s_1, s_2) \in T$ dahingehend, dass s_2 der aktuelle Zustand ist und s_1 der Vorgängerzustand dieser Zelle.

Wir definieren ψ durch

$$\psi((x_1, x_2), (y_1, y_2), (z_1, z_2)) \to (y_2, \varphi(x_2, y_2, z_2) - y_1). \tag{1.14}$$

Die Inverse ist dann durch

$$\psi^{-1}((x_1, x_2), (y_1, y_2), (z_1, z_2)) \to (\varphi(x_1, y_1, z_1) - y_1, y_1) \tag{1.15}$$

gegeben. Die Subtraktion erfolgt modulo $|S|$. Man sieht hier schon, dass ψ^{-1} nur unter speziellen Voraussetzungen die Inverse von ψ sein kann, weil die rechte Seite von Gleichung 1.15 von x_2, y_2 und z_2 unabhängig und folglich ψ^{-1} nicht reversibel ist. In der Tat funktioniert die Invertierung mit ψ^{-1} nur unter der Bedingung, dass x_2, y_2 und z_2 Folgezustände von x_1, y_1 und z_1 sind.

Zum Beispiel sei $\varphi : \{0,1\}^3 \to \{0,1\}$ durch $\varphi(x,y,z) = 0$ definiert. Dann ist

$$\psi((x_1,x_2),(y_1,y_2),(z_1,z_2)) = (y_2, 0 - y_1)$$

und

$$\psi^{-1}((x_1,x_2),(y_1,y_2),(z_1,z_2)) = (0 - y_1, y_1),$$

also

$$\psi^{-1}(\psi((x_1,x_2),(y_1,y_2),(z_1,z_2))) = (0 - y_2, y_2).$$

Wäre ψ^{-1} wirklich die Inverse von ψ, so müsste $\psi^{-1}(\psi(x,y,z))) = (x,y,z)$ erfüllt sein. Das gilt aber nur für $y_1 = 0 - y_2$. Es handelt sich bei ψ nicht um die Überführungsfunktion eines RZA, sondern um eine Funktion, die auf einer bestimmten Teilmenge ihrer Eingaben reversibel ist. Für die Verwendung in einem Quantenzellularautomaten reicht diese Eigenschaft nicht aus; wir brauchen Überführungsfunktionen, die auf allen Eingaben reversibel sind.

1.4.5 Universelle RZA

Turingmaschinen können ZA auf endlichen Konfigurationen mit Zeitverlust simulieren, indem sie die Rechnung sequentialisieren und die neuen Zustände für alle aktiven Zellen nacheinander berechnen. Da es universelle reversible Turingmaschinen gibt – Morita et al. haben zum Beispiel eine mit nur einem Band und zwei Symbolen gefunden [62] – können auch reversible Turingmaschinen Zellularautomaten simulieren.

Andererseits können ZA Turingmaschinen simulieren. Wenn man also einen reversiblen ZA findet, der eine universelle Turingmaschine simuliert, dann kann dieser RZA auch beliebige andere ZA simulieren.

Morita und Harao [60] haben einen berechnungsuniversellen reversiblen ZA angegeben, der die oben erwähnte reversible universelle Turingmaschine simuliert. Morita hat dieses Ergebnis noch verbessert, indem er einen reversiblen *Einweg-ZA* (einen ZA mit Nachbarschaftsgröße zwei) angegeben

hat [61], der die gleiche Turingmaschine simuliert. Die universelle reversible Turingmaschine von Morita benötigt allerdings quadratische Zeit, um irreversible Turingmaschinen zu simulieren. Dubacq hat einen reversiblen ZA angegeben, der beliebige Turingmaschinen ohne Zeitverlust simuliert [23].

Alle drei zitierten Simulationen verwenden partitionierte ZA. Wir skizzieren die Konstruktion von Dubacq. Die Idee besteht wie üblich darin, einen Zustand des ZA als Position des Schreib-Lese-Kopfes der Turingmaschine zu interpretieren. Der ZA führt die internen Zustandsübergänge, Schreibvorgänge und Kopfbewegungen der Turingmaschine gemäß ihrer Überführungsfunktion aus und sorgt außerdem dafür, dass alte Zustände mit Hilfe eines zusätzlichen Bandes kopiert und in dem zu Beginn stillen Bereich der Konfiguration abgelegt werden, um sicherzustellen, dass die Rechnung reversibel ist.

Sei $T = (F, Q, \tau)$ eine Turingmaschine mit dem Bandalphabet F, der internen Zustandsmenge Q und der Übergangsfunktion $\tau : F \times Q \to F \times Q \times \{l, r\}$. Dabei stehen l und r für die Bewegung des Schreib-Lese-Kopfes. Außerdem gebe es einen Ruhezustand $0 \in F$.

Für die Simulation von T mit einem RZA verwendet Dubacq einen partitionierten ZA mit Nachbarschaftsgröße vier. Er erweitert die Zustandsmenge T um einen neuen stillen Zustand $\perp$; sei $\Sigma = T \cup \{\perp\}$.

Die Nachbarschaft einer Zelle besteht aus der Zelle selbst, ihren direkten linken und rechten Nachbarn und dem übernächsten rechten Nachbarn. Die Zustandsmenge hat die Form

$$F \times \Sigma \times \Sigma \times (F \times \Sigma \times \{l, r\}).$$

Eine Eingabe $(a, b, c, (d, e, \delta))$ für die lokale Überführungsfunktion bedeutet: Die aktuelle Zelle enthält den Schreib-Lese-Kopf im Zustand a, in der linken Nachbarzelle steht das Bandsymbol b, in der rechten Nachbarzelle steht das Bandsymbol c und von rechts wird die Kopie eines Zustandes (d, e, δ) aus internem Zustand d, Bandsymbol e und $\delta \in \{l, r\}$ durchgereicht.

Die meisten solcher Eingaben sind unzulässig, weil sie im Laufe der Simulation einer Turingmaschine nicht auftreten können. Bei partitionierten ZA reicht es aus, die Überführungsfunktion auf den zulässigen Eingaben zu

definieren, weil sich eine Funktion, die dort bijektiv ist, immer so fortsetzen lässt, dass sie auf allen Eingaben bijektiv ist [60, 23].

Sei C die Beschreibung eines Startzustandes der Turingmaschine; C weist jeder Zelle j auf dem Band ein Bandsymbol $C(j)$ so zu, dass alle bis auf endlich viele Zellen im Zustand 0 sind. Die Zelle 1 enthält den Schreib–Lese–Kopf im internen Zustand q_0. Daraus gewinnt man die Anfangskonfiguration des ZA, indem man Zelle 1 den Zustand $(C(1), q_0, \bot, (0, \bot, l))$ zuweist und allen anderen Zellen i den Zustand $(C(i), \bot, \bot, (0, \bot, l))$. Eine Anwendung der globalen Überführungsfunktion des ZA entspricht genau einem Rechenschritt der Turingmaschine. In zulässigen Konfigurationen hat immer genau eine Zelle den Schreib-Lese-Kopf; folglich wird auch immer nur in genau einer Zelle die Funktion τ angewandt, so dass nur an einer Stelle die Notwendigkeit entsteht, den vorherigen Zustand zu kopieren.

Die Simulation nach Dubacq braucht mit fortschreitender Rechnung immer mehr Platz, weil mehr und mehr Zellen mit historischer Information belegt werden. Für reversible Turingmaschinen mit drei Bändern gibt es ein Uncomputing (Ent-Rechnen) genanntes Verfahren von Bennett [6], das den zusätzlich benötigten Platz einschränkt. Will man damit eine irreversible 1-Band-Turingmaschine simulieren, die Platz P und Zeit T benötigt, so kommt man für die Simulation mit Zeit $O(T^{1+\varepsilon})$ und Platz $O(P \log T)$ aus. Man könnte also auch bei ZA den zusätzlich benötigten Platz verringern, indem man Turingmaschinen simuliert, die nach dem Verfahren von Bennett arbeiten.

Dank den Ergebnissen von Morita, Harao und Dubacq weiß man, dass es berechnungsuniverselle RZA gibt. Die Rechnung erfolgt allerdings sequentialisiert, mittels Simulation einer Turingmaschine; damit gibt man einen entscheidenden Vorteil von ZA, nämlich die Parallelität, auf. Darüber hinaus ist für die Komplexität von ZA nicht nur wichtig, wie viele Zellen im Laufe der Berechnung belegt werden, sondern auch, wie groß das Zustandsalphabet ist. Dieses ist in den hier genannten Verfahren verhältnismäßig groß, was aber zum Teil am Einsatz partitionierter ZA liegt.

1.4.6 Linearzeit-Simulation auf endlichen Konfigurationen

Man muss nicht wirklich Turingmaschinen simulieren, die ihrerseits ZA simulieren, um ZA mit RZA zu simulieren. Der folgende Ansatz von Morita erlaubt die Simulation eines irreversiblen ZA mit $|S|$ Zuständen auf endlichen Konfigurationen mittels eines reversiblen partitionierten ZA mit $O(|S|^5)$ Zuständen in einer Zeit, die linear in der Länge des Bereiches aktiver Zellen ist [59]. Wie die Ansätze im vorherigen Abschnitt arbeitet auch dieser sequentiell.

Sei $A = (S, 3, \varphi)$ der zu simulierende ZA. Wir nehmen ohne Einschränkung an, S enthalte einen stillen Zustand $\perp$, so dass gilt:

$$\forall s \in S \setminus \{\perp\}, u, t \in S : \varphi(u, s, t) \neq \perp$$

Die Simulation funktioniert nur bezüglich Anfangskonfigurationen, deren nicht-stiller Teil zusammenhängend ist.

Außerdem führen wir die Zustandsmengen $\tilde{S} = \{\tilde{s} : s \in S\}$ und $\tilde{S}_* = \{\tilde{s}_* : s \in S\}$ ein. Der simulierende ZA B ist partitioniert mit Nachbarschaftsgröße drei und der Zustandsmenge $L \times M \times R$:

$$\begin{aligned} L &= S \cup S^2 \cup \{\tilde{\perp}, *\} \\ M &= S \\ R &= S^2 \cup \tilde{S} \cup \tilde{S}_* \cup \{\perp, *\}. \end{aligned}$$

Sei nun $c \in S_F^{\mathbb{Z}}$ eine endliche Anfangskonfiguration über S. Wir bilden daraus eine Anfangskonfiguration für B, indem wir für die i-te Zelle den Zustand $(\perp, c_i, \perp)$ festlegen. Die erste stille Zelle rechts vom aktiven Bereich versetzen wir in den Zustand $(*, \perp, \perp)$, um die Simulation beginnen zu lassen.

Nehmen wir an, die am weitesten rechts stehende aktive Zelle sei im Zustand $(\perp, s, \perp)$, Wenn sie das Signal $*$ bekommt, gibt sie ihren Zustand s nach links weiter und den Zustand $(s, \perp)$ nach rechts. Ihre linke Nachbarzelle erhält den Zustand s von rechts und schickt ihren eigenen Zustand t nach links weiter und (t, s) nach rechts zurück. Eine Zelle, die von links (s, t) und von rechts (t, u) erhält, kann die simulierte Überführungsfunktion

ausführen und wechselt in den Zustand $((s, t), \varphi(s, t, u), \tilde{u})$; das bedeutet, sie schickt (s, t) nach links zurück und $\tilde{u}$ als historische Information nach rechts.

In dieser Art setzt sich die Ausführung von φ von rechts nach links fort, während historische Information nach rechts weitergegeben wird, um die Reversibilität sicherzustellen. Wenn die am weitesten links stehende aktive Zelle φ ausgeführt hat, schickt sie ein Signal nach rechts; sobald dieses am rechten Rand des aktiven Bereiches angekommen ist, kann die nächste Iteration von φ berechnet werden.

Nach dem gleichen Prinzip arbeitet der universelle RZA von Durand-Lose, der beliebige andere RZA simuliert [25].

1.4.7 Simulation auf unendlichen Konfigurationen

Die reversiblen Simulationen, die wir bis jetzt vorgestellt haben, waren immer sequentialisiert und auf endliche Konfigurationen eingeschränkt; diese Einschränkung folgt daraus, dass alte Zustände von Zellen nie gelöscht, sondern nur in andere, zu Beginn inaktive, Zellen verschoben werden. Damit dies möglich ist, muss es hinreichend viele inaktive Zellen geben, die die ganze Information aufnehmen können. Bei einer Simulation auf unendlichen Konfigurationen, die ja überhaupt keine inaktiven Zellen haben müssen, ist scheinbar kein Platz für diese historische Information.

Wir haben aber abzählbar unendlich viele Zellen zur Verfügung und können den Platz einfach und reversibel schaffen, wenn wir einen asynchronen Simulationsbegriff zu Grunde legen. Das ist die Idee an dem Ansatz von Durand-Lose [27]. Um einen ZA mit Alphabet S zu simulieren, benötigt er einen reversiblen PZA mit $100|S|^3(|S|^3+1)^2$ Zuständen. Die benötigte Zeit ist nicht so einfach anzugeben, weil es sich hier um einen asynchronen Simulationsbegriff handelt (aber es ist wirklich nur die *Simulation*, die asynchron ist, nicht der simulierende ZA). Wir beschreiben das Verfahren informell und verweisen für die konkrete Überführungsfunktion auf den Aufsatz von Durand-Lose [27].

Sei $c \in S^{\mathbb{Z}}$ die Konfiguration, auf der der zu simulierende ZA $A = (S, N, \varphi)$ gestartet werden soll. Ohne Einschränkung sei $N = 3$. Wir über-

führen c in eine Konfiguration d des simulierenden ZA $B = (T, 3, \psi)$, indem wir in der i-ten Zelle von d drei Kopien von c_i ablegen. Außerdem wird die Zelle mit dem Index 0 in d markiert; dies ist die Zelle, die den ersten simulierten Zustandsübergang ausführt. Es ist nicht wichtig, dass genau die Zelle 0 markiert wird, aber es ist wichtig, dass nur eine Zelle markiert wird.

Zu jedem Zeitpunkt gibt es einen mittleren Bereich, der die aktiven Zellen enthält. Die äußeren Zellen sind inaktiv und geben nur die bei der Rechnung im aktiven Bereich anfallenden historischen Informationen nach außen weiter. Ein Signal überstreicht den aktiven Bereich in Pendelbewegungen und führt die simulierte Überführungsfunktion aus. Jedes Mal, wenn es einen Rand erreicht, wächst der aktive Bereich um eine Zelle.

In der Mitte des aktiven Bereiches ist die Rechnung am weitesten fortgeschritten, an den Rändern hat sie gerade erst begonnen. Hat die Anfangskonfiguration unendlichen Träger, so dauert es unendlich lang, bis alle Zellen mindestens einen Schritt des simulierten ZA vollzogen haben.

1.5 Mit Reversibilität verwandte Eigenschaften

1.5.1 Einleitung

Wir untersuchen, wie Surjektivität und Injektivität mit zwei Eigenschaften zusammenhängen, die den Informationserhalt in einem ZA quantifizieren. Zuerst untersuchen wir Entropieerhalt bezüglich zweier verschiedener Begriffe von Entropie; danach führen wir den Begriff der Informationsvollständigkeit nach Nishio ein und beweisen, dass jeder surjektive ZA informationsvollständig ist.

1.5.2 Entropieerhalt

Es liegt nahe zu vermuten, dass reversible ZA die geeignet definierte) Entropie ihrer Eingabe erhalten. Betrachten wir dazu folgende zwei Definitionen von Entropie.

Definition 1.12 (Mengenentropie [74])
Die Mengenentropie von $L \subseteq S^*$ *ist für alle* $n \in \mathbb{N}$, $n > 0$ *durch*

$$s(L, n) = \frac{1}{n} \log_2 |L \cap S^n| \tag{1.16}$$

definiert.

Die Mengenentropie einer Sprache misst, wieviel Information über ein Wort $w \in L$ der Länge n in einem beliebigen Buchstaben von w enthalten ist. Dabei wird nur die Anzahl von Wörtern der Länge n in L in Betracht gezogen.

Ein etwas anderes Maß ist die *räumliche Maßentropie*; sie erlaubt es, auch die relativen Häufigkeiten (Wahrscheinlichkeiten) von Wörtern zu berücksichtigen.

Definition 1.13 (Räumliche Maßentropie [74])
Zur der Sprache $L \subseteq S^*$ *sei* p_L *eine Wahrscheinlichkeitsverteilung, die jedem Wort aus* L *eine Wahrscheinlichkeit zuordnet. Dann ist die räumliche Maßentropie von* L*:*

$$s_m(L, n) = -\frac{1}{n} \sum_{w \in L \cap S^n} p_L(w) \log_2 p_L(w). \tag{1.17}$$

Die räumliche Maßentropie ist eng mit der Shannon-Entropie

$$H(L) = -\sum_{w \in L} p_L(w) \log_2(p_L(w)) \tag{1.18}$$

verwandt.

Zu einer Konfiguration $c \in S^{\mathbb{Z}}$ sei $L(c)$ definiert als die Menge aller endlichen Wörter w über S, für die ein $i \in \mathbb{Z}$ existiert, so dass c_{i+k} für $1 \leq k \leq |w|$ das k-te Symbol von w ist. Eine Konfiguration c ist durch $L(c)$ bis auf Verschiebung eindeutig bestimmt [16].

Surjektive ZA sind gerade diejenigen, für deren globale Überführungsfunktion Φ gilt: $L(\Phi^t(S^{\mathbb{Z}})) = S^*$ für alle $t \in \mathbb{N}$. Insbesondere gilt daher für alle $t_1 \neq t_2$ und alle $n \in \mathbb{N}$

$$s(\Phi^{t_1}(S^{\mathbb{Z}}), n) = s(\Phi^{t_2}(S^{\mathbb{Z}}), n);$$

$L(\Phi^t(S^{\mathbb{Z}}))$ ist immer gleich S^* und somit ändert sich auch an der Entropie nichts. Um zu zeigen, dass eine entsprechende Aussage auch für s_m gilt, erinnern wir an Lemma 1.3, das besagt, dass unter einem surjektiven ZA jedes endliche nichtleere Wort genau $|S|^{N-1}$ Urbilder besitzt.

Wenn man die Wahrscheinlichkeiten p_L aus Definition 1.13 über die relativen Häufigkeiten definiert:

$$p_L(w) = |S^{|w|+N-1} \cap L|^{-1} \cdot |\{v \in S^{|w|+N-1} \cap L : \varphi(v) = w\}|,$$

so folgt

$$s_m(\Phi^{t_1}(S^{\mathbb{Z}}), n) = s_m(\Phi^{t_2}(S^{\mathbb{Z}}), n).$$

Wenn wir allerdings unter Entropieerhalt verstehen wollen, dass für beliebige Teilmengen $C \subseteq S^{\mathbb{Z}}$ gelte $s(L(\Phi(C)), n) = s(L(C), n)$, so erhalten surjektive ZA die Entropie nicht.

Sei zum Beispiel $A_{xor} = (\{0,1\}, 3, \varphi)$ mit $\varphi(x,y,z) = x+z \bmod y$ ähnlich dem aus früheren Beispielen bekannten ZA. Wir wählen für C die Menge der Konfigurationen, deren Zellen abwechselnd mit 0 und 1 belegt sind; es gilt demnach $|C| = |L(C) \cap S^n| = 2$ für alle $n > 0$. $A(C)$ aber enthält nur ein Element, nämlich die Konfiguration, in der alle Zellen im Zustand 1 sind. Daher ist $|A(C)| = |L(A(C)) \cap S^n| = 1$. Folglich kann A die Mengenentropie nicht erhalten, denn es ist $s(L(C), n) = n^{-1}$, aber $s(L(A(C)), n) = 0$ für alle n. A ist damit ein surjektiver ZA, der die Mengenentropie nicht erhält; die räumliche Maßentropie kann A damit erst recht nicht erhalten.

Unter dieser Bedingung erhalten selbst injektive ZA nicht die Entropie. Sei zum Beispiel c die periodische Konfiguration $\ldots 012012012 \ldots$ und $\varphi(012) = 1$, $\varphi(120 = 1)$, $\varphi(201) = 0$. Es gibt mehrere RZA, deren lokale Überführungsfunktion diese Eigenschaften hat; ein Beispiel ist derjenige mit der Wolfram-Kodierung $00011122200021112200011122 2$. Dann wird c von φ auf die Konfiguration $\ldots 011011011 \ldots$ abgebildet; demnach kommen in c drei verschiedene Wörter der Länge eins vor und in $\varphi(c)$ nur zwei. Daher kann dieser RZA die Mengentropie und folglich auch die räumliche Maßentropie nicht erhalten.

1.5.3 Informationserhalt

Ein RZA ist deswegen invertierbar, weil es möglich ist, aus der aktuellen Konfiguration eindeutig auf die Vorgängerkonfiguration zu schließen. Was aber, wenn wir uns nur für die Zustände einzelner ausgewählter Zellen in der Vorgängerkonfiguration interessieren?

Mit anderen Worten, wieviel Information über den Zustand von Zelle i zum Zeitpunkt t ist zum Zeitpunkt $t+k$ noch vorhanden? Dieser Frage ist H. Nishio nachgegangen [67, 68].

Nishio betrachtet ZA, bei denen die Zustandsmenge die Struktur eines endlichen Körpers besitzt. Er formuliert seine Aussagen nur für den Fall $|N| = 3$; dies ist keine Einschränkung der Allgemeinheit. Die lokale Überführungsfunktion schreibt er als Polynom in drei Variablen über S. Man erhält also den Folgezustand der Zelle i, indem man in das Überführungspolynom P die alten Zustände der Zellen $i-1$, i und $i+1$ einsetzt.

Nehmen wir nun an, wir kennten die Zustände aller Zellen bis auf den der Zelle i. Diesen unbekannten Zustand repräsentieren wir mit einem neuen Symbol X. Nun erweitern wir die Definition von P so, dass als Eingabe auch X erlaubt ist. Der neue Zustand einer Zelle kann dann auch wieder ein Polynom in X sein. Nishio bezeichnet diese Klasse von ZA als $ZA[X]$, weil ihr Überführungspolynom über $S[X]$ statt über S definiert ist.

Sei $c : \mathbb{Z} \to S[X]$ eine globale Konfiguration. Dann steht $P(c)$ für die Menge aller Polynome, die als Zustände von Zellen in c vorkommen. Wir übernehmen die folgenden Begriffe aus [68]:

Definition 1.14 (Informations-vollständige Konfiguration)
Eine Teilmenge $G \subseteq S[X]$ *heißt* informations-vollständig, *falls* X *im Abschluss von* G *unter Addition, Subtraktion und Multiplikation enthalten ist. Eine Konfiguration* c *heißt informations-vollständig, wenn* $P(c)$ *informations-vollständig ist.*

Definition 1.15 (t-Vollständigkeit)
A *aus* $ZA[X]$ *heißt* t-vollständig, *falls für alle Konfigurationen* c, *die genau ein* X *enthalten gilt, dass* $A^t(c)$ *informations–vollständig ist. Ist* A t-*vollständig für alle* $t \geq 0$, *so heißt* A ∞-*vollständig.*

Lemma 1.16 (Nishio [68])
Alle RZA sind ∞-vollständig, aber nicht alle ∞-vollständigen ZA sind reversibel.

Ein nicht reversibler ∞-vollständiger ZA ist zum Beispiel $\varphi(x, y, z) = x$ xor z über dem Alphabet $\{0, 1\}$. Dieser ist surjektiv, also reversibel auf endlichen Konfigurationen.

Lemma 1.17
Jeder ∞-vollständige ZA ist surjektiv.

Beweis: Ist $A = (S, N, \varphi)$ nicht ∞-vollständig, so gibt es ein endliches t sowie eine unendliche Konfiguration $\ldots wXw' \ldots$, so dass $A^t(\ldots wXw' \ldots)$ nicht vollständig ist; nach Satz 3.7 in Nishios Aufsatz [68] folgt, dass es $a \neq b \in S$ gibt, so dass $A^t(\ldots waw' \ldots) = A^t(\ldots wbw' \ldots)$. Nun hängt aber der Zustand der i-ten Zelle zum Zeitpunkt t nur von einer endlichen Zahl weiterer Zellen ab, also gibt es endliche Konfigurationen $\ldots 000v a v' 000 \ldots$ und $\ldots 000v b v' 000$ (wobei wir ohne Einschränkung einen stillen Zustand 0 verwenden), die unter A^t das gleiche Bild haben. Folglich ist A nicht surjektiv. □

Man könnte vermuten, dass auch die Umkehrung von Lemma 1.17 gilt, dass also die ∞–vollständigen ZA mit den surjektiven zusammenfallen. Diese Frage können wir nicht abschließend beantworten. Ein Beweisansatz wäre:

Sei $A = (S, N, \varphi)$ ein nicht surjektiver ZA. Es gibt endliche Konfigurationen $c_w = \ldots 000w000 \ldots$ und $c_v = \ldots 000v000 \ldots$ über S, so dass $A(c_w) = A(c_v)$. Ohne Beschränkung der Allgemeinheit sei $|w| = |v|$. Wir bilden einen abgeleiteten ZA $A' = (S^{|w|}, N, \varphi')$, die Fortsetzung von A auf Blöcken der Länge $|w|$, indem wir φ' gemäß Gleichung 1.1 definieren. A' ist wie A nicht surjektiv und außerdem nicht ∞-vollständig.

Um zu folgern, dass dann auch A nicht ∞-vollständig ist, muss man zeigen, ∞-Vollständigkeit unter der Blockzusammenfassung, mit der wir A' aus A erhalten haben, invariant ist, was nicht offensichtlich ist.

1.6 Zusammenfassung

Reversible Zellularautomaten sind selten. Solange Nachbarschaft und Alphabet überschaubar klein bleiben, sind RZA überdies meistens trivial. Ausgehend von einer empirischen Untersuchung der RZA mit relativ kleinem Alphabet und kleiner Nachbarschaft haben wir die strukturellen Folgen der Reversibilität für ZA herausgearbeitet und die Ergebnisse mit Hilfe des Darstellungssatzes von Kari präzisiert.

Verschiedene Verfahren erlauben es, gezielt reversible ZA zu erzeugen. Dies ist vor allem für die Simulation von Bedeutung; in der Tat sind RZA nicht grundsätzlich ein uninteressantes Berechnungsmodell (was man anhand ihrer Seltenheit befürchten könnte), sondern zu universeller Rechnung und daher auch zu nichttrivialem Verhalten in der Lage.

Eine Simulation beliebiger ZA mit RZA ist nur dann möglich, wenn der Simulationsbegriff hinreichend weit gefasst ist. Man kann nicht mit je einem globalen Schritt des RZA einen des irreversiblen ZA simulieren. Die bekannten Simulationsverfahren arbeiten sequentiell und benötigen $O(n)$ Schritte des RZA, um einen Schritt des irreversiblen ZA auf einer Konfiguration mit n aktiven Zellen zu simulieren. Daneben haben wir noch ein Verfahren vorgestellt, das zwar ebenfalls lineare Zeit benötigt, aber nicht völlig sequentiell ist und außerdem eine Simulation auch auf unendlichen Konfigurationen zulässt.

KAPITEL 2

Stochastische Zellularautomaten

2.1 Einleitung

Stochastische Zellularautomaten zeichnen sich dadurch aus, dass ihre lokale Überführungsfunktion nicht deterministisch sein muss; sie weist verschiedenen Ergebnissen Wahrscheinlichkeiten zu. Insofern besteht ein gewisser Zusammenhang mit Quantenzellularautomaten, deren lokale Überführungsfunktion den verschiedenen Ergebnissen Amplituden zuweist, aus denen man die Wahrscheinlichkeit erhält, bei einer Messung den einen oder anderen Zustand zu beobachten.

Wie unterschiedlich andererseits Quantenzellularautomaten und stochastische ZA sind, offenbart sich schon daran, dass alle surjektiven stochastischen ZA sich deterministisch verhalten. Dennoch beschäftigen wir uns mit dieser Klasse von ZA, denn einige der Schwierigkeiten, die zum Beispiel bei der Beschreibung und dem Vergleich von Folgekonfigurationen auftreten, sind durchaus vergleichbar mit denen, die uns bei Quantenzellularautomaten begegnen werden.

Stochastische ZA werden gewöhnlich mit Hilfe von Markov-Ketten analysiert. Diese Methode ist erfolgreich, wird aber für Konfigurationen mit vielen aktiven Zellen sehr kompliziert. Wir entwickeln eine Definition von stochastischen ZA, die sich an denen für Quantenzellularautomaten orientiert, die wir in Kapitel 4 kennenlernen werden und diskutieren die Schwie-

rigkeiten, die beim Versuch einer lokalen Beschreibung globaler Konfigurationen auftreten.

Eine Frage, die sich im Zusammenhang mit stochastischen ZA (und mit Quantenzellularautomaten) aufdrängt ist die nach der Wahl der Übergangswahrscheinlichkeiten (beziehungsweise -amplituden). Konkret müssen wir wissen, welche Auswirkungen kleine Änderungen an den Wahrscheinlichkeiten auf das Verhalten eines ZA haben können. Für diese Frage gibt es eine Vielzahl von Gründen. Zum Beispiel werden stochastische ZA typischerweise für Simulationen eingesetzt; die Wahrscheinlichkeiten dienen dazu, Eigenschaften der Umgebung wiederzugeben, die entweder wirklich zufällig sind oder sich unserer Kontrolle entziehen (und damit für die Zwecke der Simulation zufällig erscheinen). Da diese Wahrscheinlichkeiten üblicherweise durch Raten und Probieren gefunden werden, ist es wichtig zu wissen, wie sehr ein Fehler die Ergebnisse entwertet. Um ein weiteres Beispiel zu nennen, gibt es offenbar Wahrscheinlichkeiten, deren Verwendung zumindest fragwürdig ist: Wir können nicht erwarten, nicht-berechenbare Wahrscheinlichkeitsfunktionen einsetzen zu können. Inwiefern ist es sinnvoll, solche Wahrscheinlichkeiten zu approximieren?

Um diese Fragen zu beantworten brauchen wir eine Methode, globale Konfigurationen zu vergleichen. Wir entwickeln eine Metrik, die unseren Zwecken angemessen ist und setzen sie ein, um die Unterschiede abzuschätzen, die sich bei Anwendung eng verwandter stochastischer ZA auf die gleiche Eingabekonfiguration mit der Zeit entwickeln.

2.2 Definitionen

2.2.1 Grundlagen aus der Wahrscheinlichkeitstheorie

Zunächst benötigen wir einige Begriffe aus der Wahrscheinlichkeitstheorie.

Definition 2.1

1. *Ein* Zufallsexperiment *ist eine Handlung, die eines von mehreren Ergebnissen haben kann, zum Beispiel das Werfen eines Würfels.*

2. *Ein* Merkmalsraum *ist die Menge aller möglichen Ergebnisse bei ein-*

maliger Durchführung eines Zufallsexperiments. Im Folgenden bezeichnet Ω einen Merkmalsraum.

3. *Ein* Ereignis *ist eine Teilmenge des Merkmalsraums. Die einelementigen Teilmengen von Ω heißen auch* Elementarereignisse.

4. *Eine* Zufallsvariable *ist eine reellwertige Funktion X auf dem Merkmalsraum.*

Wir wollen Ereignissen Wahrscheinlichkeiten zuordnen. Dies geschieht mittels *Wahrscheinlichkeitsverteilungen*.

Definition 2.2 (Wahrscheinlichkeitsfunktion)
Eine Funktion $f : \Omega \to \mathbb{R}^+$ aus einem abzählbaren Merkmalsraum in die nichtnegativen reellen Zahlen heißt Wahrscheinlichkeitsfunktion, *falls gilt:*

$$\sum_{\omega \in \Omega} f(\omega) = 1.$$

Daraus folgt insbesondere $0 \leq f(\omega) \leq 1 \ \forall \omega \in \Omega$.

Im Folgenden betrachten wir ausschließlich abzählbare Merkmalsräume.

Definition 2.3 (Wahrscheinlichkeit eines Ereignisses)
Ist f eine Wahrscheinlichkeitsfunktion auf dem diskreten Merkmalsraum Ω und $A \subseteq \Omega$ ein Ereignis, so bezeichnet

$$P_f(A) = \sum_{\omega \in A} f(\omega)$$

die Wahrscheinlichkeit *des Ereignisses A.*
Die Funktion P_f heißt die Wahrscheinlichkeitsverteilung *auf Ω.*

Wir schreiben P statt P_f, wenn die Wahrscheinlichkeitsfunktion aus dem Zusammenhang klar ist. Wir verwenden auch $\Pr[A]$, um die Wahrscheinlichkeit des Ereignisses A zu bezeichnen.

Zufallsvariablen bieten eine elegante Darstellung komplexer Ereignisse. Sei zum Beispiel $X : \Omega \to \mathbb{R}$ eine Zufallsvariable und $x \in \mathbb{R}$. Dann schreiben wir $\Pr[X \leq x]$ für $\Pr[\{\omega \in \Omega : X(\omega) \leq x\}]$.

Definition 2.4 (Stochastische Unabhängigkeit)
Auf dem Raum Ω *sei die Wahrscheinlichkeitsverteilung* P *definiert. Zwei Ereignisse* $A, B \subseteq \Omega$ *heißen* stochastisch unabhängig, *wenn* $P(A \cap B) = P(A) \cdot P(B)$ *gilt.*

2.2.2 Eine Definition für stochastische ZA

Sei wie bei deterministischen ZA S ein endliches Zustandsalphabet und N eine Nachbarschaftsgröße. Wir beschränken uns wieder auf eindimensionale ZA.

Für die stochastischen Zustände und Konfigurationen verwenden wir gewichtete Summen der Form $p_1x_1+p_2x_2+\ldots+p_kx_k$, wobei die x_i Elemente eines diskreten Merkmalsraums X sind und alle p_i in dem reellen Intervall $[0,1]$ liegen. Außerdem fordern wir $\sum_{i=1}^{k} p_i = 1$. Solche Summen nennen wir *stochastische Summen* und fassen die p_i als Wahrscheinlichkeiten auf.

Sei $P : \mathcal{P}(\{x_1, \ldots, x_k\}) \to [0,1]$ mit $P(\{x_i\}) = p_i$ und $P(Y) = \sum_{y \in Y} P(\{y\})$ für $Y \subseteq X$ eine Wahrscheinlichkeitsverteilung. Dabei steht $\mathcal{P}$ für die Potenzmenge. Ist Z eine Zufallsvariable, so ist die Wahrscheinlichkeit, dass $Z = x_i$ gilt, gerade $\Pr[Z = x_i] = P(\{x_i\}) = p_i$.

Definition 2.5 (Stochastischer Zustand)
Sei S *die endliche Zustandsmenge eines ZA. Ein* stochastischer Zustand *über* S *ist eine stochastische Summe* $q = \sum_{s \in S} q_s s$. Q *steht für die Menge der stochastischen Zustände.*

Deterministische Zustände sind Spezialfälle von stochastischen Zuständen q, für die nur genau ein q_s von Null verschieden ist.

Definition 2.6 (Stochastische lokale Konfiguration)
Eine stochastische lokale Konfiguration ist eine stochastische Summe $\tilde{q} = \sum_{w \in S^N} q_w w$. $\tilde{Q}$ *steht für die Menge der stochastischen lokalen Konfigurationen.*

Stochastische globale Konfigurationen als stochastische Summen über $S^{\mathbb{Z}}$ zu definieren ist problematisch, denn $S^{\mathbb{Z}}$ ist überabzählbar. Wir beschränken uns daher zunächst auf stochastische Summen über den endlichen Konfigurationen $S_F^{\mathbb{Z}}$, in denen außerdem nur endlich viele von Null

verschiedene p_i vorkommen dürfen. In Abschnitt 2.2.4 geben wir eine mögliche Erweiterung der Definition auf unendliche Konfigurationen an.

Definition 2.7 (Stochastische globale Konfiguration)
Eine stochastische globale Konfiguration ist eine stochastische Summe $\widehat{q} = \sum_{c \in S_F^{\mathbb{Z}}} q_c c$ *mit* $q_c = 0$ *für alle bis auf endlich viele* c. $\widehat{Q}$ *steht für die Menge der stochastischen globalen Konfigurationen.*

Ist $F : \mathbb{Z} \to Q$ eine Funktion, die jeder Zelle unabhängig von allen anderen Zellen einen stochastischen Zustand zuweist, so dass alle bis auf endlich viele Zellen in einem stillen Zustand sind, so induziert F eine stochastische globale Konfiguration $\widehat{q}$ mittels

$$\begin{aligned} \widehat{q} &= \sum_c q_c c \text{ für} \\ q_c &= \prod_{i \in \mathbb{Z}} \Pr[F(i) = c_i]. \end{aligned} \tag{2.1}$$

Das Produkt existiert, wenn F endlichen Träger hat (das heißt, wenn F allen bis auf endlich vielen Zellen einen stillen Zustand zuweist), oder allgemeiner, wenn $F(i)$ für alle bis auf endlich viele i ein deterministischer Zustand ist.

Nach diesen Vorarbeiten können wir stochastische lokale Überführungsfunktionen definieren.

Definition 2.8 (Stochastische lokale Überführungsfunktion)
Eine stochastische lokale Überführungsfunktion ist eine Abbildung $\varphi : S^N \to Q$ *mit* $N \in \mathbb{N}$.

Ähnlich wie bei deterministischen ZA induziert φ eine globale Überführungsfunktion Φ. Beginnen wir dazu mit einer deterministischen globalen Konfiguration c.

$$\Phi(c)_i = \varphi(c_{i-(N-1)/2}, c_{i-(N-1)/2+1}, \ldots, c_{i+(N-1)/2}), \tag{2.2}$$

wobei N ohne Einschränkung als ungerade angenommen wird. Wir können Φ mittels

$$\Phi(\widehat{q}) = \sum_c q_c \Phi(c) \tag{2.3}$$

zu einer Funktion auf $\widehat{Q}$ fortsetzen.

Lemma 2.1 (Wohlgeformtheit von Φ)
Ist Φ gemäß Gleichungen 2.2 und 2.3 aus einer stochastischen lokalen Überführungsfunktion hervorgegangen, so ist $\Phi(\widehat{q}) \in \widehat{Q}$ für alle $\widehat{q} \in \widehat{Q}$.

Beweis: Sei $\widehat{q}$ eine deterministische globale Konfiguration. Wir wenden φ gemäß Gleichung 2.2 an und erhalten für jede Zelle einen stochastischen Zustand. Dabei sind alle Zellen voneinander stochastisch unabhängig; wir können daher Gleichung 2.1 verwenden und erhalten eine stochastische globale Konfiguration. Die Erweiterung auf ganz $\widehat{Q}$ erfolgt linear und ergibt

$$\varphi\left(\sum_{i=1}^{k} p_i c_i\right) = \sum_{i=1}^{k} p_i \varphi(c_i),$$

was ein Element von $\widehat{Q}$ ist, wenn $\sum_{i=1}^{k} p_i = 1$ gilt. □

Wiederum dank Gleichung 2.1 induziert Φ eine Funktion $\widehat{Q} \to \widehat{Q}$. Wir bezeichnen die induzierte Funktion ebenfalls mit Φ.

Ein stochastischer ZA (SZA) ist bis auf die Überführungsfunktion genau wie ein deterministischer ZA definiert.

Definition 2.9 (Stochastischer ZA)
Ein SZA ist ein 3-Tupel (S, N, φ) aus einem endlichen Zustandsalphabet S, einer Nachbarschaftsgröße $N \in \mathbb{N}$ und einer stochastischen lokalen Überführungsfunktion φ.

Unsere Definition ermöglicht es, SZA als stochastische Summen von ZA zu schreiben.

Lemma 2.2
Sei φ die lokale Überführungsfunktion eines SZA mit der Nachbarschaftsgröße N. Dann gibt es $p_1, \ldots, p_k \in [0, 1]$ mit $\sum_{i=1}^{k} p_i = 1$ und deterministische lokale Überführungsfunktionen $\psi_1, \ldots, \psi_k$ so dass für alle $w \in S^N$ gilt: $\varphi(w) = \sum_{s \in S} q_s s$ mit $q_s = \sum_{i:\psi_i(w)=s} p_i$.

Beweis: Wir wählen eine Reihenfolge der $w \in S^N$ und bezeichnen das n-te Wort dieser Reihenfolge mit w_n. Es gilt $\varphi(w_n) = \sum_{s \in S} q_{n,s} s$ mit

$\sum_{s\in S} q_{n,s} = 1$. Nun wählen wir ein m zwischen 1 und $|S|^{|N|}$ sowie ein $t \in S$ so, dass $q_{m,t} = \min_{n,s} q_{n,s}$. Wir setzen $p_1 = q_{m,t}$ und $\psi_1(w_m) = t$; für die Werte von ψ_1 auf Eingaben $w'_m \neq w_m$ wählen wir beliebige t' mit $q_{m',t'} > 0$.

Nun ersetzen wir die $q_{n,s}$ durch $q'_{n,s}$:

$$q'_{n,s} := \begin{cases} q_{n,s} & \psi(w_n) \neq s \\ q_{n,s} - p_1 & \psi(w_n) = s \end{cases}$$

für alle n, s. Das gleiche wiederholen wir für p_2 und ψ_2, p_3 und ψ_3, und so weiter, bis alle p_i und ψ_i gefunden sind.

Das Verfahren terminiert, wenn alle $q_{n,s}$ Null sind. Bevor dies eintritt, gilt in jeder Iteration $\sum_{s\in S} q_{n,s} > 0$ für alle n, denn in jeder Iteration gilt

$$\sum_{s\in S} q_{n,s} = \sum_{s\in S} q_{m,s} \tag{2.4}$$

für alle $1 \leq n, m \leq |S|^{|N|}$. Dies zeigen wir durch Induktion über die Anzahl Iterationen. Zu Beginn sind alle $\sum_{s\in S} q_{n,s}$ gleich eins. In der $i$ten Iteration subtrahieren wir p_i von allen $q_{n,s}$ mit $\psi_i(w_n) = s$; es wird also jede der Summen $\sum_{s\in S} q_{n,s}$ gerade um p_i reduziert. Daraus folgt, dass nach jedem Iterationsschritt Gleichung 2.4 erfüllt ist.

Schließlich gilt nach Beendigung des Verfahrens $\sum_{i=1}^{k} p_i = 1$, denn zu Beginn ist $\sum_{s\in S} q_{n,s} = 1$ für alle n, und wir erreichen Null, indem wir alle p_i von dieser Summe abziehen. □

Wir schreiben gelegentlich SZA in der Form $\sum_{i=1}^{k} p_i\psi_i$. Dabei ist es nicht erforderlich, dass alle ψ_i deterministisch sind. Selbst wenn alle ψ_i deterministisch sind, ist die Summendarstellung nicht eindeutig.

Wir nennen einen Zustand, eine lokale oder globale Konfiguration oder einen ZA *deterministisch*, wenn in der Darstellung als stochastische Summe nur ein von Null verschiedener Summand vorkommt.

2.2.3 Alternative Definitionen

Es gibt Alternativen zu unserer Definition von SZA. Zum Beispiel könnte man lokale Überführungsfunktionen der Form $\psi : \tilde{Q} \to Q$ zulassen, sie

also auf stochastischen anstelle von deterministischen lokalen Konfigurationen definieren. Allerdings ermöglicht dies lokale Überführungsfunktionen, die nicht durch eine endliche Tabelle darstellbar sind und damit wäre eine der definierenden Eigenschaften von ZA verletzt. Darüber hinaus können Zustände infolge der Aktion des ZA voneinander stochastisch abhängig werden und es wäre dann sehr schwierig, stochastische lokale Konfigurationen zu extrahieren. Schließlich ist es nicht intuitiv, dass eine Zelle Zugriff auf die Wahrscheinlichkeitsfunktionen ihrer Nachbarn hat; plausiblerweise kann eine Zelle nur auf die Ergebnisse entsprechender Zufallsexperimente reagieren.

Eine weitere denkbare Definition der lokalen Überführungsfunktion wäre als Wahrscheinlichkeitsfunktion $\xi : (S^N \to S) \to [0,1]$; das heißt, ξ gibt die Wahrscheinlichkeit an, mit der eine bestimmte Überführungsfunktion ausgewählt wird. Zwei Varianten sind denkbar: Entweder die Überführungsfunktion wird einheitlich für alle Zellen bestimmt, oder jede Zelle entscheidet selbst, welche Überführungsfunktion sie anwendet. Letzteres führt zu einem Modell, das nach Lemma 2.2 äquivalent zu Definition 2.9 ist. Ersteres dagegen verletzt die Gleichheit aller Zellen, denn es muss eine ausgezeichnete Zelle geben, die das Zufallsexperiment zu ξ durchführt und das Ergebnis allen anderen mitteilt.

Merkle hat SZA ausgehend von globalen stochastischen Überführungsfunktionen definiert [53, 54]. Unser Modell ist äquivalent zu dem zweiten dort vorgestellten.

2.2.4 SZA auf unendlichen Konfigurationen

Wir haben uns bis jetzt auf endliche Konfigurationen beschränkt; unsere Definition von globaler Konfiguration machte dies unumgänglich. Betrachten wir nämlich den SZA $A = (\{a, b, 0\}, 1, \varphi)$ mit $\varphi(a) = \varphi(b) = 1/2a + 1/2b$ und $\varphi(0) = 0$. Wenden wir A auf eine beliebige deterministische Konfiguration mit unendlichem Träger an, so befindet sich danach jede Zelle in dem gleichen stochastischen Zustand, nämlich $1/2a + 1/2b$. Wollte man Wahrscheinlichkeiten für globale Konfigurationen ausrechnen, so käme man für deterministische Konfigurationen nicht auf wohldefinierte

Zahlen. Dennoch ist das Ergebnis der Anwendung von A nicht undefiniert; es ist nur unser Begriff von globaler Konfiguration, der an dieser Stelle nicht ausreicht. Wir geben eine Erweiterung an, die die Behandlung von SZA auf beliebigen Konfigurationen erlaubt.

Das Problem, das hier auftritt, existiert für deterministische ZA nicht. Dort ist durch Angabe des Zustandes jeder einzelnen Zelle eine globale Konfiguration eindeutig festgelegt. Im stochastischen Modell dagegen können Zellen (zum Beispiel durch die Aktion eines SZA) voneinander stochastisch abhängig werden. Betrachten wir zum Beispiel den SZA $B = (\{a, b, c, 0\}, 3, \psi)$ mit

$$\begin{aligned} \psi(XaY) &= 1/2b + 1/2c & \psi(bXY) &= b \\ \psi(XYc) &= c & \psi(XcY) &= 0 \\ \psi(XbY) &= 0 & \psi(XYZ) &= Y, \end{aligned}$$

wobei X, Y und Z Platzhalter für Elemente des Zustandsalphabetes sind. Diese verkürzte Schreibweise ist so zu lesen, dass man, um die Ausgabe von ψ auf einer gegebenen Eingabe zu ermitteln, die Regeln von links nach rechts und von oben nach unten durchgeht und die erste anwendet, die passt. Aus einer globalen Konfiguration der Form

$$\ldots 0\,0\,0\,a\,0\,0\,0 \ldots$$

wird bei einmaliger Anwendung von B

$$\ldots 0\,0\,0\,(1/2b + 1/2c)\,0\,0\,0 \ldots .$$

Im nächsten Schritt entsteht eine Konfiguration, in der b oder c einzeln jeweils mit Wahrscheinlichkeit $1/2$ vorkommen, aber nicht beide zusammen:

$$1/2(\ldots 0\,0\,c\,0\,0\,0\,0 \ldots) + 1/2(\ldots 0\,0\,0\,0\,b\,0\,0 \ldots). \tag{2.5}$$

In diesem Fall wäre es nicht nötig gewesen, Wahrscheinlichkeiten für globale Konfigurationen auszumultiplizieren; die Gleichung

$$\ldots 0\,0\,(1/2(c\,0\,0) + 1/2(0\,0\,b))\,0\,0 \ldots \tag{2.6}$$

beschreibt die gleiche globale Konfiguration wie Gleichung 2.5. Im Allgemeinen erlauben stochastische Konfigurationen keine so bequeme Darstellung; wir werden aber mit Definition 2.11 eine Möglichkeit angeben, lokale und globale Konfigurationen zueinander in Beziehung zu setzen.

In dem Beispiel mit dem SZA A können wir zwar keine Wahrscheinlichkeitsverteilung über globale Konfigurationen angeben, wohl aber eine für jede endliche Menge von Zellen. Wir verallgemeinern daher die Schreibweise aus Gleichung 2.6 und bauen unsere Definition auf der Beschreibung endlicher Intervalle von Zellen auf.

Definition 2.10
Ein endliches stochastisches Wort der Länge k, $k \in \mathbb{N}$, *ist eine stochastische Summe* $\overline{q} = \sum_{w \in S^k} q_w w$. $\overline{Q}_k$ *steht für die Menge der endlichen stochastischen Wörter der Länge* k. *Wir setzen*

$$\overline{Q} = \bigcup_{k \in \mathbb{N}} \overline{Q}_k. \tag{2.7}$$

Eine globale stochastische Konfiguration weist jeder endlichen zusammenhängenden Menge von Zellen ein endliches stochastisches Wort zu. Es kann aber nicht jede solche Zuordnung eine globale Konfiguration sein; nehmen wir zum Beispiel an, die einzelne Zelle i bekäme das endliche Wort $p \cdot a + (1-p) \cdot b$ zugewiesen, die Zellen $i-1, i, i+1$ als Menge jedoch das endliche Wort $q \cdot aaa + (1-q) \cdot bab$. Bezüglich des letzteren Wortes wäre Zelle i immer im Zustand a, was nicht zu der ersteren Zuweisung passt. Passend wäre es, wenn für die endlichen Wörter $\overline{q}_i = \sum_{s \in S} p_s s$ und $\overline{q}_{i-1,i,i+1} = \sum_{w \in S^3} r_w w$ gälte:

$$p_s = \sum_{t,t' \in S} r_{tst'}.$$

Hieraus formulieren wir eine *Konsistenzbedingung*.

Sei I_k die Menge aller Intervalle der Länge k, also aller zusammenhängender Mengen von k Zellen und $I = \cup_{k \in \mathbb{N}} I_k$.

Definition 2.11
Eine stochastische globale k*-Konfiguration ist eine Funktion* $\mathcal{F}_k : I_k \to \overline{Q}_k$. *Eine stochastische globale Konfiguration ist eine Familie* $\mathcal{F}_{k \in \mathbb{N}}$ *von globalen*

stochastischen k*-Konfigurationen, die der folgenden Konsistenzbedingung genügt: Aus* $J \subseteq J'$ *(ohne Einschränkung* $J = \{1, \ldots, n\}$, $J' = \{k, \ldots, l\}$ *mit* $1 \leq k \leq l \leq n$*) mit* $\mathcal{F}_{|J|}(J) = \sum_{w \in S^n} p_w w$ *und* $\mathcal{F}_{|J'|}(J') = \sum_{v \in S^{l-k+1}} q_v v$ *folgt*

$$q_v = \sum_{x \in S^{k-1}, y \in S^{n-l}} p_{xvy} \tag{2.8}$$

für alle $v \in S^{l-k+1}$.

Lemma 2.3
Zu jeder stochastischen globalen Konfiguration gemäß Definition 2.7 gibt es eine stochastische globale Konfiguration gemäß Definition 2.11.

Beweis: Sei $\widehat{q} = \sum_{i=1}^{k} q_i c_i \in \widehat{Q}$. Wir zeigen, wie man daraus zu beliebigen endlichen Intervallen $J_k \in I_k$ die Funktion $\mathcal{F}_k$ erhält. Ist nämlich $J_k = \{j, \ldots, j+k-1\}$ ein solches Intervall, so bezeichne $C(J_k)$ die Menge aller endlichen deterministischen Konfigurationen, die auf den Indizes j bis $j+k-1$ mit J_k übereinstimmen. Dann können wir $\mathcal{F}_k(I_k) = \sum_{c_i \in C(J_k)} q_i$ setzen. Gleichung 2.8 ist bei dieser Festlegung erfüllt. □

Der einzige Unterschied zwischen den Definitionen 2.7 und 2.11 besteht darin, dass letztere auch unendliche Konfigurationen erfasst. Eine vergleichbare Idee haben Maes und Shlosman verwendet [48]. Unsere Definition von SZA können wir ohne Änderung übernehmen.

Lemma 2.4
SZA bilden stochastische globale Konfigurationen auf ebensolche ab.

Beweis: Sei $\mathcal{F}$ eine globale stochastische Konfiguration nach Definition 2.11 und $A = (S, N, \varphi)$ ein SZA. Es ist zu zeigen, dass $A(\mathcal{F})$ eine globale stochastische Konfiguration ist.

Dazu geben wir für jedes Intervall $J_k = \{l, \ldots, l+k-1\}$ in $A(\mathcal{F})$ ein endliches stochastische Wort an. Diese hängt von dem endlichen stochastischen Wort des Intervalls $J_{k+N-1} = \{l-(N-1)/2, \ldots, l+k-1+(N-1)/2\}$ (ohne Einschränkung sei N ungerade) unter $\mathcal{F}$ ab. Aus

$$\mathcal{F}(J_{k+N-1}) = \sum_{w \in S^{k+N-1}} p_w w$$

bilden wir

$$A(\mathcal{F})(J_k) = \sum_{w \in S^{k+N-1}} p_w \varphi(w).$$

Es ist noch zu zeigen, dass dann Gleichung 2.8 erfüllt ist.

Ohne Beschränkung der Allgemeinheit sei $J_{k+N-1} = \{1, \ldots, k+N-1\}$, also für N ungerade $J_k = \{(N-1)/2+1, \ldots, k+(N-1)/2\}$. Wir schreiben $A(\mathcal{F})(J_k)$ als Summe $\sum_{v \in S^k} s_v v$ mit $s_v = \sum_{w \in S^{k+N-1}} p_w \Pr[\varphi(w) = v]$.

Nehmen wir an, $A(\mathcal{F})$ verletze Gleichung 2.8. Dann gibt es ein Intervall $J_l \subseteq J_k$, $J_k = \{(N-1)/2+1+n, \ldots, k+(N-1)/2-m\}$ mit $n, m \in \mathbb{N}$, so dass

$$A(\mathcal{F})(J_k) = \sum_{v \in S^{k-n-m}} q_v v,$$

aber

$$\exists v : q_v \neq \sum_{x \in S^n, y \in S^m} s_{xvy}.$$

Es gilt

$$A(\mathcal{F}(J_l) = \sum_{w \in S^{l+N-1}} r_w \varphi(w)$$

für

$$\mathcal{F}(J_{l+N-1}) = \sum_{w \in S^{l+N-1}} r_w w.$$

Daher können wir für alle $v \in S^l$ q_v auch mittels der r_w ausdrücken:

$$q_v = \sum_{w \in S^{l+N-1}} r_w \Pr[\varphi(w) = v].$$

Weil $\mathcal{F}$ die Gleichung 2.8 erfüllt, ist

$$r_w = \sum_{x \in S^n, y \in S^m} p_{xwy},$$

also

$$\begin{aligned} q_v &= \sum_{w \in S^{l+N-1}} \sum_{x \in S^n, y \in S^m} p_{xwy} \Pr[\varphi(w) = v] \\ &= \sum_{w \in S^{k+N-1}} p_w \sum_{a \in S^n, b \in S^m} \Pr[\varphi(w) = avb] \\ &= \sum_{x \in S^n, y \in S^m} s_{xvy}, \end{aligned}$$

wobei die erste Gleichung wegen der Lokalität von φ gilt und die zweite Zeile wegen $l+n+m = k$ folgt. □

Damit ist gezeigt, dass Definition 2.11 eine brauchbare Erweiterung von Definition 2.7 auf den unendlichen Fall ist. In Abschnitt 4.4 werden wir ähnliche Ideen verwenden, um Quantenzellularautomaten auf unendlichen Konfigurationen zu definieren.

2.3 Markov-Ketten

Markov-Ketten sind das am meisten benutzte Werkzeug in der Analyse von stochastischen ZA. Wir geben hier nur eine knappe Einführung, die sich an der Darstellung von Motwani und Raghavan [63] orientiert.

Definition 2.12 (Markov-Kette)
Eine Markov-Kette besteht aus einer endlichen oder abzählbaren Menge Z *von* Zuständen *und einer Matrix* P *mit* Übergangswahrscheinlichkeiten. *Dabei steht der Eintrag* $P[i,j]$ *für die Wahrscheinlichkeit, mit der die Markov-Kette vom Zustand* s_i *in den Zustand* s_j *übergeht.*

Um SZA mit Markov-Ketten zu beschreiben, identifiziert man Z mit $S_F^{\mathbb{Z}}$ und setzt für $\Phi(c_i) = \sum_{l=1}^{k} p_l c_l$ in der Matrix P den Eintrag $P[i,j]$ auf p_j. Für unendliche Konfigurationen ist dieses Vorgehen so nicht möglich; man kann allerdings wie Maes und Shlosman [48] lokale Übergangsmatrizen auf beliebig großen endlichen Teilkonfigurationen angeben.

Auf endlichen Konfigurationen erhält man ganz ähnlich wie in unseren Definitionen die stochastischen Zustände als Wahrscheinlichkeitsverteilungen über Z und die Überführungsfunktion als eine Selbstabbildung dieser

Wahrscheinlichkeitsverteilungen (für überabzählbare Z sollte man besser von Wahrscheinlichkeitsmaßen sprechen).

Sei π^0 eine Wahrscheinlichkeitsverteilung über Z, die wir als Anfangsverteilung betrachten. Nach einem Schritt der Markov-Kette erhalten wir die Verteilung $\pi^1 = \pi^0 P$, induktiv nach n Schritten: $\pi^n = \pi^0 P^n$. Nun gibt es Markov-Ketten, die ihre Anfangsverteilung vergessen: für $n \to \infty$ konvergiert π^n schwach gegen eine Verteilung, die unabhängig von π^0 ist. Solche Markov-Ketten bezeichnet man als *ergodisch* (siehe auch de Jong und Maes [17]).

Viele Arbeiten über SZA interessieren sich für diese Grenzwerte, die auch *stationäre Verteilungen* heißen; zum Beispiel gibt es Kriterien dafür, wann die stationäre Verteilung ein *Gibbs-Maß* ist (auch bekannt als *Markov Random Field*). Solche Arbeiten sind zum Beispiel Marroquín und Ramírez [50] und Lebowitz et al. [45]. Viele, wenn auch nicht alle, SZA sind ergodisch.

Wegen der Motivation über Quantenzellularautomaten sind wir eher an Reversibilität interessiert. Diese steht zur Ergodizität im Widerspruch, denn wenn ein SZA von beliebigen Anfangsverteilungen aus gegen eine stationäre Verteilung konvergiert, kann er nicht reversibel sein. Dabei verstehen wir Reversibilität in dem Sinn, dass aus der Verteilung π^{t+1} eindeutig auf die Verteilung π^t geschlossen werden kann. Es gibt im Zusammenhang mit Markov-Ketten auch den Begriff der reversiblen Markov-Kette, der aber mit unserer Definition von Reversibilität von ZA nicht viel zu tun hat.

Als Beschreibungsformalismen sind Markov-Ketten und unsere Definition äquivalent, solange man nur endliche Konfigurationen betrachtet. Allerdings wird es für Konfigurationen mit vielen aktiven Zellen sehr aufwändig, die Übergangswahrscheinlichkeiten anzugeben. Die Darstellung mittels SZA ist dann kompakter.

2.4 Surjektivität und Reversibilität bei SZA

Wir geben zwei Definitionen von Surjektivität für SZA und zeigen, dass die stärkere nur von deterministischen ZA erfüllt werden kann. Daraus folgt insbesondere, dass Reversibilität für SZA kein interessanter Begriff ist.

Es ist nicht sinnvoll, surjektive SZA als Epimorphismen von $\widehat{Q}$ zu definieren, denn $\widehat{Q}$ ist nur über endlichen Konfigurationen definiert. Auf diese eingeschränkt sind aber selbst die surjektiven deterministischen ZA nicht surjektiv (Beispiel: A_{xor}, siehe Kapitel 2). Wir definieren daher Surjektivität als die Fähigkeit, jedes endliche stochastische Wort zu erzeugen; dies ist analog zu der Fähigkeit surjektiver deterministischer ZA, jedes endliche Wort über S zu erzeugen, welche nach einem Satz von Hedlund gleichbedeutend mit Surjektivität auf $S^{\mathbb{Z}}$ ist.

Definition 2.13 (Surjektivität von SZA)
Ein SZA $A = (S, N, \varphi)$ ist surjektiv, wenn für jedes endliche stochastische Wort $\overline{q}$ der Länge k über S ein endliches stochastisches Wort $\overline{p}$ der Länge $k + N - 1$ über S existiert, so dass $\varphi(\overline{p}) = \overline{q}$.

Lemma 2.5
Jeder surjektive SZA ist äquivalent zu einem deterministischen ZA.

Beweis: Sei $A = (S, N, \varphi)$ ein surjektiver SZA und $\overline{q} = w \in S^k$. Dann gibt es laut Definition ein $\overline{p} = \sum_{v \in S^{k+N-1}} p_v v$ mit

$$w = \varphi(\overline{p}) = \sum_{v \in S^{k+N-1}} p_v \varphi(v),$$

also gilt für alle $v \in S^{k+N-1}$ mit $p_v > 0$, dass $\varphi(v) = w$ ist. Daran sieht man schon, dass φ auf den Teilwörtern der Länge N von v deterministisch ist. Außerdem muss jedes endliche deterministische Wort w ein deterministisches Urbild $\varphi^{-1}(w)$ besitzen.

Nehmen wir nun an, φ wäre nicht auf ganz S^N deterministisch. Dann gibt es ein $u \in S^N$ mit $\varphi(u) = pu' + (1-p)u''$. Folglich haben Wörter, in denen u als Teilwort vorkommt, nie ein deterministisches Bild; anders ausgedrückt kommt u nie im Urbild einer deterministischen endlichen Konfiguration vor, aber alle deterministischen endlichen Konfigurationen haben ein deterministisches Urbild.

Wir erhalten eine deterministische lokale Überführungsfunktion ψ, indem wir für $x \in S$ vereinbaren, dass $\psi(\varphi^{-1}(c)) = x$ sein soll. Wenn φ surjektiv ist, muss ψ auf deterministischen Konfigurationen ebenfalls surjektiv sein, egal, wie wir ψ auf den übrigen Eingaben (wie zum Beispiel

u) definieren. Dann könnten wir ψ aber unbalanciert wählen und würden Lemma 1.3 widersprechen. □

Eine abgeschwächte Definition ist möglich, wenn wir nur verlangen, dass jedes endliche Wort mit einer von Null verschiedenen Wahrscheinlichkeit generierbar sein soll.

Definition 2.14 (Quasi-Surjektivität)
Ein SZA $A = (S, N, \varphi)$ *heißt* quasi-surjektiv, *wenn für jedes endliche stochastische Wort* $\overline{p}$ *gilt:*

$$\sum_{w \in S^{k+N-1}} \Pr[\varphi(w) = \overline{p}] = 1. \tag{2.9}$$

Für diese Eigenschaft kann man ein hinreichendes Kriterium angeben:

Lemma 2.6
Ein SZA ist quasi-surjektiv, wenn er eine Darstellung als Summe surjektiver deterministischer ZA besitzt.

Beweis: Sei $A = \sum_{i=1}^{l} p_i \varphi_i$ mit φ_i surjektiv für alle i. Dann ist

$$\sum_{w \in S^{k+N-1}} \Pr[\varphi_i(w) = v] = 1$$

für alle $1 \leq i \leq l$ und alle $v \in S^k$. Daraus folgt:

$$\begin{aligned}
\sum_{w \in S^{k+N-1}} \Pr[\varphi(w) = v] &= \sum_{w \in S^{k+N-1}} \sum_{i=1}^{l} p_i \Pr[\varphi(w) = v] \\
&= \sum_{i=1}^{l} p_i \sum_{w \in S^{k+N-1}} \Pr[\varphi_i(w) = v] \\
&= \sum_{i=1}^{l} p_i = 1.
\end{aligned}$$

Damit ist die Behauptung für den Fall $\overline{p} = v \in S^k$ bewiesen. Sei nun

$\overline{p} = \sum_{v \in S^k} p_v v$ und $\sum_v p_v = 1$. Dann ist

$$\begin{aligned}
\sum_{w \in S^{k+N-1}} Pr[\varphi(w) = \overline{p}] &= \sum_{w \in S^{k+N-1}} \sum_{i=1}^{l} p_i Pr[\varphi_i(w) = \overline{p}] \\
&= \sum_{w \in S^{k+N-1}} \sum_{i=1}^{l} p_i \sum_{v \in S^k} p_v Pr[\varphi_i(w) = v] \\
&= \sum_{v \in S^k} p_v \sum_{w \in S^{k+N-1}} \sum_{i=1}^{l} p_i Pr[\varphi_i(w) = v] \\
&= \sum_{v \in S^k} p_v = 1.
\end{aligned}$$

□

Aus Lemma 2.6 folgt insbesondere, dass jeder surjektive deterministische ZA quasi-surjektiv ist. Wenn man in Gleichung 2.9 das $= 1$ durch > 0 ersetzt, reicht es aus, dass einer der Summanden surjektiv ist.

Quasi-Surjektivität gestattet keine sinnvolle Definition von Reversibilität: Wenn nur bekannt ist, dass die Gesamtwahrscheinlichkeit, summiert über möglichen Eingaben, ein gewisses endliches Wort zu erzeugen, gleich Eins ist, folgt daraus nicht die Existenz eines Urbildes. Definiert man aber $\varphi^{-1}(v)$ für $v \in S^k$ in der Art

$$\sum_{w \in S^{k+N-1}} Pr[\varphi(w) = v]w,$$

so ist $\varphi^{-1}(\varphi(w)) = w$ nur dann, wenn φ deterministisch ist. Reversibilität in dem Sinn, der für Quantenzellularautomaten von Bedeutung wäre, ist erst möglich, wenn wir statt Übergangswahrscheinlichkeiten komplexe Amplituden verwenden können.

2.5 Eine Metrik für SZA

2.5.1 Einleitung

Topologische Methoden erfreuen sich bei der Untersuchung deterministischer ZA großer Beliebtheit. Auf SZA sind sie allerdings noch nicht über-

tragen worden, obwohl es auch hier Anwendungen gäbe. Zum Beispiel beschäftigen wir uns im folgenden Abschnitt mit der Ähnlichkeit von stochastischen ZA stochastischen globalen Konfigurationen.

Dabei definieren wir die Ähnlichkeit globaler Konfigurationen über ein Abstandsmaß, welches wir von einer Metrik beziehen. Diese müssen wir allerdings erst noch entwickeln.

Statt dieser Metrik könnten wir auch den Abstandsbegriff aus dem Markov-Ketten-Ansatz übernehmen; dieser vergleicht allerdings nur Wahrscheinlichkeitsverteilungen miteinander und berücksichtigt nicht die verschieden großen Unterschiede zwischen den zugrundeliegenden deterministischen Konfigurationen.

2.5.2 Metriken auf deterministischen Konfigurationen

Topologien und Metriken statten Mengen mit einer Struktur aus, in der Begriffe wie „Abstand“ oder „Konvergenz“ eine Bedeutung haben. Wir verwenden die Definitionen aus dem Buch von Jänich [41].

Definition 2.15 (topologischer Raum)
Ein topologischer Raum *ist ein Paar* $(X, \mathcal{O})$ *aus einer Menge* X *und einer Menge* $\mathcal{O}$ *von Teilmengen (genannt* offene Mengen*) von* X*, so dass gilt:*

1. *Beliebige Vereinigungen von offenen Mengen sind offen.*
2. *Der Durchschnitt von endlich vielen offenen Mengen ist offen.*
3. *Die leere Menge und* X *sind offen.*

Man bezeichnet $\mathcal{O}$ auch als die *Topologie*. des Raumes X. Eine Menge heißt *abgeschlossen*, wenn ihr Komplement offen ist.

Definition 2.16 (metrischer Raum)
Ein metrischer Raum *ist ein Paar* (X, d) *aus einer Menge* X *und einer Funktion* $d : X \times X \to \mathbb{R}$ *(der* Metrik*), für die gilt:*

1. *(Positivität) Für alle* $x, y \in X$ *ist* $d(x, y) \geq 0$ *und* $d(x, y) = 0$ *genau dann, wenn* $x = y$.

2. *(Symmetrie) Für alle* $x, y \in X$ *ist* $d(x, y) = d(y, x)$.

3. *(Dreiecksungleichung) Für alle* $x, y, z \in X$ *gilt* $d(x, z) \leq d(x, y) + d(y, z)$.

Jeder metrische Raum besitzt eine Topologie.

Definition 2.17 (Topologie eines metrischen Raumes)
Ist (X, d) *ein metrischer Raum, so heiße eine Teilmenge* $V \subseteq X$ *offen, wenn es zu jedem* $x \in V$ *ein* $\varepsilon > 0$ *gibt, so dass die* ε*-Umgebung* $U_\varepsilon(x) = \{y \in X : d(x, y) \leq \varepsilon\}$ *von* x *ganz in* X *liegt. Die Menge aller offenen Teilmengen von* X *heißt die Topologie von* (X, d).

Ein metrischer Raum ist *kompakt*, wenn jede Folge eine konvergente Teilfolge hat. Er heißt *vollständig*, wenn jede Cauchy-Folge konvergiert und *total unzusammenhängend*, wenn die einzigen zusammenhängenden Teilmengen die einelementigen sind.

Für deterministische Konfigurationen von ZA ist die sogenannte Cantor-Metrik die populärste. Seien dazu $c, d \in S^{\mathbb{Z}}$. Dann ist ihr Abstand in der Cantor-Metrik

$$d_C(c, d) = 2^{-i}, \tag{2.10}$$

wobei i die betragskleinste ganze Zahl ist, für die $c_i \neq d_i$ gilt. Der Abstand d_C ist demnach um so größer, je näher am Nullpunkt sich c und d unterscheiden.

Der metrische Raum $(S^{\mathbb{Z}}, d_C)$ ist kompakt, vollständig und total unzusammenhängend [11]. Die deterministischen ZA entsprechen in diesem Raum genau der Klasse der stetigen und mit der Verschiebung kommutierenden Selbstabbildungen [37].

Es gibt einige Alternativen zur Cantor-Metrik: Cattaneo et al. haben den Hamming-Abstand untersucht [12], Choffrut und Pighizzini Editierdistanz [14] und Formenti bedingte Kolmogorov-Komplexität [30].

2.5.3 Anforderungen an eine Metrik auf $\widehat{Q}$

Wir beschränken uns auf die abzählbare Menge $S_F^{\mathbb{Z}}$. Wir wählen eine Aufzählung der Konfigurationen in $S_F^{\mathbb{Z}}$ und bezeichnen die i-te Konfiguration

mit c_i, solange keine Gefahr besteht, dies mit der i-ten Zelle der Konfiguration c zu verwechseln.

Seien $\widehat{q} = \sum_{i=1}^{k} q_i c_i$ und $\widehat{p} = \sum_{i=1}^{k} q_i c_i$ Elemente von $\widehat{Q}$. Was wäre ein sinnvolles Maß für ihren Abstand?

Wir könnten $\widehat{Q}$ als einen unendlichdimensionalen Vektorraum auffassen; die i-te Komponente des Vektors zu $\widehat{q}$ wäre q_i. Dann könnten wir uns jeder Metrik auf diesem Vektorraum als einer Metrik auf $\widehat{Q}$ bedienen. Zum Beispiel induziert

$$d_1(\widehat{q}, \widehat{p}) = \sum_{i=1}^{k} |q_i - p_i|$$

auf dem Teilraum $S_F^{\mathbb{Z}}$ die triviale Topologie. Das gleiche Problem tritt mit allen Metriken auf, die nur auf einem Vergleich der q_i und p_i fußen.

Ignorieren wir also die q_i und p_i und konzentrieren uns auf die beteiligten deterministischen Konfigurationen. Seien dazu $C_q = \{c_i : q_i > 0\}$,$C_p = \{c_i : p_i > 0\} \setminus C_q$ und

$$f(\widehat{q}, \widehat{p}) = \begin{cases} 0 & C_p = \emptyset \\ \min_{c \in C_q, c' \in C_p} d_C(c, c') & \text{sonst} \end{cases}$$

und

$$d_2(\widehat{q}, \widehat{p}) = \min(f(\widehat{q}, \widehat{p}), f(\widehat{p}, \widehat{q}),$$

so ist d_2 keine Metrik, denn $d_2(0.1c_1 + 0.9c_2, 0.9c_1 + 0.1c_2) = 0$. Dieses Problem haben alle Metriken, die ähnlich wie d_2 nur die deterministischen Konfigurationen berücksichtigen.

Was wir suchen ist eine Metrik d auf stochastischen Konfigurationen, die sowohl von den Gewichten in den stochastischen Summen als auch von den Abständen zwischen den deterministischen Konfigurationen abhängt. Formal nehmen wir $c_1, c_2, c_3 \in S_F^{\mathbb{Z}}$ und $0 < q, p < 1$ und fordern

$$\begin{aligned} &d_C(c_1, c_2) < d_C(c_1, c_3) \\ &\qquad \Rightarrow d(c_1, qc_1 + (1-q)c_2) < d(c_1, qc_1 + (1-q)c_3) \end{aligned} \tag{2.11}$$

sowie

$$\begin{aligned} &q > p \\ &\quad \Rightarrow d(c_1, qc_1 + (1-q)c_2) < d(c_1, pc_1 + (1-p)c_2) \end{aligned} \tag{2.12}$$

Schließlich wäre es wünschenswert, wenn d auf deterministischen Konfigurationen mit d_C zusammenfiele.

2.5.4 Eine Metrik

Seien $\widehat{q}$ und $\widehat{p}$ wie oben definiert. Wir betrachten Abstandsmaße der Form

$$d_f(\widehat{q}, \widehat{p}) = \sum_{i=1}^{k} \sum_{j=1}^{k} f(\widehat{q}, \widehat{p}, i, j) d_C(c_i, c_j),$$

also gewichtete Summen über die Cantor-Distanzen deterministischer Konfigurationen. Wir brauchen eine Funktion f. Hängt f nur von i und j ab, so ist d_f im Allgemeinen keine Metrik: Entweder wir erhalten eine Pseudometrik oder eine, für die $d_f(\widehat{q}, \widehat{q})$ für einige $\widehat{q}$ gilt.

Unser Ziel ist es zu messen, wie unterschiedlich zwei stochastische Konfigurationen sind. Normalerweise betrachtet man Dinge als unterschiedlich, wenn sie leicht zu unterscheiden sind. Diese Idee liegt der folgenden Metrik zugrunde. Ausgehend von einem Spiel ersetzen wir nach und nach die Entscheidungen der Spieler durch Zufallsexperimente. Zum Schluss ist nicht mehr viel von dem Spiel übrig, aber wir haben eine Metrik.

An dem Spiel sind zwei Spieler beteiligt: Z (der Zweifler) und B (der Beweiser). Z kennt nur $\widehat{q}$, während B sowohl $\widehat{q}$ als auch $\widehat{p}$ kennt. B will Z davon überzeugen, dass $\widehat{q}$ und $\widehat{p}$ gleich sind.

Als erstes wählt Z eine Konfiguration c_i mit $q_i > 0$. Er teilt B seine Wahl mit. B wählt eine Konfiguration c_j mit $p_j > 0$ und obwohl er Z nicht sagt, was er gewählt hat, ist er an seine Entscheidung gebunden. Dann nennt Z einen Index $k \in \mathbb{Z}$ und fordert damit B auf, $c_i(k)$ mit $c_j(k)$ zu vergleichen. Sind sie unterschiedlich, so hat Z gewonnen. Die Metrik basiert auf der Gewinnwahrscheinlichkeit von Z – je einfacher das Spiel für Z ist, als desto unterschiedlicher sollen $\widehat{q}$ und $\widehat{p}$ gelten.

Um diese Wahrscheinlichkeit abzuschätzen, müssen wir spezifizieren, wie die Spieler ihre Wahlen treffen. Offenbar sollen hier die q_i und p_i eine Rolle spielen. Z soll zufällig wählen; es ist naheliegend zu fordern, er solle c_i mit der Wahrscheinlichkeit q_i wählen.

Erlauben wir B freie Auswahl bei seiner Antwort, so gibt es unterschiedliche Konfigurationen, bei denen Z trotzdem nicht gewinnen kann, so dass wir höchstens eine Pseudometrik bekommen könnten. Ein Beispiel ist $\widehat{q} = 0.1c_1 + 0.9c_2$ und $\widehat{p} = 0.9c_1 + 0.1c_2$. Wir müssen B zur Fairness zwingen; wählt Z c_2, so muss es eine von Null verschiedene Wahrscheinlichkeit geben, dass B mit c_1 antwortet.

Wir bezeichnen mit $Pr(i, j)$ die Wahrscheinlichkeit, dass Z c_i und dann B c_j wählt. Wir werden fordern, dass für alle $1 \leq j \leq k$ gelte:

$$\sum_{i=1}^{k} Pr(i, j) = p_j.$$

Solange diese Bedingung erfüllt ist, kann B Pr wählen, wie er will. Naheliegenderweise wird er versuchen, damit die Gewinnchancen von Z zu minimieren.

Nun fehlt noch die Wahl des Indexes k. Auch sie sollte zufällig sein, denn würde Z immer den gleichen Index wählen, so könnte B seine Strategie darauf hin optimieren. Die Wahrscheinlichkeitsfunktion, die Z hier verwendet, bestimmt den Abstandsbegriff auf deterministischen Konfigurationen, der unserer Metrik am Ende zugrunde liegen wird. Wählt Z jede Stelle mit gleicher Wahrscheinlichkeit (da unsere Konfigurationen endlich sind, können wir davon ausgehen, dass entsprechende Schranken Z bekannt sind), wird unsere Metrik auf der Hamming-Distanz aufbauen. Wir wollen die Cantor-Metrik verwenden und lassen daher Z den Index k so wählen, dass die Wahrscheinlichkeit, ein k zu wählen, an dem sich c und c' unterscheiden, proportional zu $d_C(c, c')$ ist.

Insgesamt erhalten für wir die Gewinnwahrscheinlichkeit von Z

$$\sum_{1 \leq i,j \leq k} Pr(i, j) x d_C(c_i, c_j)$$

mit einer Konstanten $x \in \mathbb{R}$.

Als Nächstes geben wir eine genauere Beschreibung von $\Pr(i,j)$, zeigen, dass es immer zulässige und optimale Funktionen $\Pr$ gibt und dass man so wirklich eine Metrik erhält.

$\Pr(i,j)$ lässt sich als Matrix schreiben und dies werden wir von nun an tun. Das Spiel brauchen wir nicht mehr: Alle Wahlmöglichkeiten der Spieler sind durch Zufallsexperimente ersetzt, so dass von dem Spiel nichts übrig ist. Außerdem lassen wir die Konstante $\varkappa$ weg und schreiben unsere Metrik einfach als gewichtete Summe von Cantor-Distanzen, denn $\varkappa$ war nur als Normalisationsfaktor für die probabilistische Interpretation von Bedeutung.

Definition 2.18 (Paarung)
Eine reelle $k \times k$*-Matrix* $\Xi_{q,p}$ *heißt* Paarung *von* $\widehat{q}$ *und* $\widehat{p}$*, wenn gilt:*

$$\forall 1 \leq i,j \leq k : 0 \leq \Xi_{q,p}[i,j] \leq \min\{q_i, p_j\} \tag{2.13}$$

$$\forall 1 \leq i \leq k : \sum_{j=1}^{k} \Xi_{q,p}[i,j] = q_i \tag{2.14}$$

$$\forall 1 \leq j \leq k : \sum_{i=1}^{k} \Xi_{q,p}[i,j] = p_j. \tag{2.15}$$

Ist $\Xi_{q,p}$ eine Paarung, so heißt $W(\Xi_{q,p}) = \sum_{i,j} \Xi_{q,p}[i,j] d_C(c_i, c_j)$ das *Gewicht* von $\Xi_{q,p}$. Wir nennen eine Paarung $\Xi_{q,p}$ *optimal*, wenn für jede andere Paarung $\Xi'_{q,p}$ gilt: $W(\Xi_{q,p}) \leq W(\Xi'_{q,p})$.

Definition 2.19 (Die Metrik)
Mit $\widehat{q}, \widehat{p} \in \widehat{Q}$ *wie oben definieren wir*

$$d(\widehat{q}, \widehat{p}) = \inf_{\Xi_{q,p}} W(\Xi_{q,p}). \tag{2.16}$$

Lemma 2.7 (Existenz der optimalen Paarung)
Das Infimum in Gleichung 2.16 ist ein Minimum; es gibt immer mindestens eine optimale Paarung.

Beweis: Die Gleichungen 2.14 und 2.15 legen ein System von $2k$ linearen Gleichungen für die k^2 Matrixelemente fest. Dies ist ein unterbestimmtes

System und besitzt daher einen Lösungsraum (im Fall $k = 1$ ist es überbestimmt, aber in diesem Fall ist $\Xi[1,1] = 1$ ohnehin die einzige Lösung). Von den Elementen dieses Lösungsraumes interessieren uns nur diejenigen, die Gleichung 2.13 erfüllen. Ist also L der Lösungsraum, so schneiden wir ihn mit dem Produkt der Intervalle $[0, \min\{q_0, p_0\}] \times [0, \min\{q_0, p_1\}] \times \ldots \times [0, \min\{q_k, p_k\}]$ und erhalten einen kompakten Teilraum $\mathcal{L}$ von $\mathbb{R}^{k^2}$. $\mathcal{L}$ ist nicht leer: er enthält zumindest das Element Ξ mit $\Xi[i,j] = q_i p_j$. Dieses ist als obere Schranke für die Metrik nützlich, wenn auch $f(\widehat{q}, \widehat{p}) = \sum_{i,j} q_i p_j d_C(c_i, c_j)$ selbst keine Metrik ist, da $f(\widehat{q}, \widehat{q})$ nicht immer Null ist.

Als stetige Funktion auf einem kompakten Raum nimmt W auf $\mathcal{L}$ ein Maximum und ein Minimum an [73]. □

Für den Beweis, dass d eine Metrik ist, verwenden wir folgende Eigenschaft optimaler Paarungen.

Lemma 2.8
Für alle $\widehat{q}, \widehat{p} \in \widehat{Q}$ *existiert eine optimale Paarung* $\Xi_{q,p}$ *mit* $\Xi_{q,p}[i,i] = \min\{q_i, p_i\}$ *für alle* $1 \leq i \leq k$.

Beweis: Sei Ξ eine optimale Paarung mit $\Xi[i,i] < \min\{q_i, p_i\}$ für einige i. Wir gewinnen aus Ξ eine Paarung Ξ', deren Gewicht nicht größer als das von Ξ ist und für die gilt: $Xi'[i,i] = \min\{q_i, p_i\}$.

Wir beginnen mit $\Xi' = \Xi$. Dann setzen wir $\Xi'[i,i] = \min\{q_i, p_i\}$. Ohne Beschränkung der Allgemeinheit sei $q_i \leq p_i$. Nun sind die i-ten Zeilen- und Spaltensummen für Ξ' zu groß; wir müssen einige der $\Xi'[i,j]$ und $\Xi'[j,i]$ reduzieren. Einträge in Zeile i müssen um insgesamt $q_i - \Xi[i,i]$ kleiner werden; Einträge in Spalte i um insgesamt $p_i - \Xi[i,i] - p_i + q_i = q_i - \Xi[i,i]$. Insbesondere bedeutet dies, dass alle Einträge der i-ten Zeile bis auf $\Xi'[i,i]$ auf Null gesetzt werden müssen.

Setzen wir also $\Xi'[i,j] = 0$ für $j \neq i$. Da die j-te Spaltensumme unverändert bleiben muss, müssen wir nun insgesamt $\Xi[i,j]$ zu den übrigen Einträgen der j-ten Spalte addieren. Addieren wir aber etwas zu $\Xi[k,j]$, so wächst die k-te Zeilensumme und wir müssen wieder andere Einträge reduzieren. Dafür können wir aber die in der i-ten Spalte verwenden, denn die müssen ohnehin schrumpfen.

Wir suchen also für alle $\Xi[i,j] > 0$ mit $i \neq j$ Indizes $k_1, k_2, \ldots \neq i$ und reelle Zahlen δ_{ijl} so dass $\sum_l \delta_{ijl} = \Xi[i,j]$ und für alle l gilt: $\Xi[k_l, i] \geq \delta_{ijl}$. Dann setzen wir $\Xi'[k_l, j] := \Xi[k_l, j] + \delta_{ijl}$ und $\Xi'[k_l, i] := \Xi[k_l, i] - \delta_{ijl}$. Solche Indizes und reelle Zahlen gibt es, denn $\sum_{j:j\neq i} \Xi[j,l] = q_i - \Xi[i,i] > 0$ und $\sum_{j:j\neq i} \Xi[i,j] = q_i - \Xi[i,i]$.

So erhalten wir eine Paarung Ξ' für $\widehat{q}$ und $\widehat{p}$ und es gilt $\Xi'[i,i] = \min\{q_i, p_i\}$. Es bleibt zu zeigen, dass $W(\Xi') \leq W(\Xi)$ erfüllt ist.

Wir erhalten $W(\Xi')$ aus $W(\Xi)$ folgendermaßen. Für jeder $j \neq i$,

1. subtrahiere $\Xi[i,i] d_C(c_i, c_j) = \sum_l d_{ijl} d_C(c_i, c_j)$
2. addiere $\sum_l \delta_{ijl} d_C(c_{kl}, c_j)$ und
3. subtrahiere $\sum_l \delta_{ijl} d_C(c_{kl}, c_i)$.

Insgesamt:

$$W(\Xi') = W(\Xi) + \sum_j \sum_l (\delta_{ijl} d_C(c_{kl}, c_j) - (d_C(c_i, c_j) + d_C(c_{kl}, c_j))).$$

Da d_C eine Metrik ist, ist $d_C(c_{kl}, c_j) \leq d_C(c_i, c_j) + d_C(c_{kl}, c_i)$, folglich ist $W(\Xi') \leq W(\Xi)$. □

Lemma 2.9
Die Funktion d aus Gleichung 2.16 ist eine Metrik.

Beweis: Für $\widehat{q} = \widehat{p}$ ist die $k \times k$-Matrix Ξ mit

$$\Xi[i,j] = \begin{cases} \min q_i, p_j & i = j \\ 0 & \text{sonst} \end{cases}$$

eine Paarung mit dem Gewicht Null.

Sei $d(\widehat{q}, \widehat{p}) = 0$ Dann gibt es eine Paarung mit Gewicht Null; die Matrix kann also außerhalb der Diagonale keine von Null verschiedenen Einträge haben. Demnach ist $\widehat{q} = \widehat{p}$.

Sei Ξ eine optimale Paarung für $\widehat{q}$ und $\widehat{p}$. Dann ist die Transponierte Ξ^T eine optimale Paarung für $\widehat{p}$ und $\widehat{p}$. Das Gewicht ist das gleiche wie für Ξ, denn für alle i, j ist $d_C(c_i, c_j) = d_C(c_j, c_i)$.

Für die Dreiecksungleichung seien $\widehat{q}, \widehat{p}, \widehat{r} \in \widehat{Q}$ so gewählt, dass $d(\widehat{q}, \widehat{p}) + d(\widehat{p}, \widehat{r}) < d(\widehat{q}, \widehat{r})$ ist. Dann gibt es optimale Paarungen $\Xi_{q,p}, \Xi_{p,r}$ und $\Xi_{q,r}$ mit

$$\begin{aligned} & W(\Xi_{q,p}) + W(\Xi_{p,r}) < W(\Xi_{q,r}) \\ \Leftrightarrow \quad & \sum_{i \neq j} \Xi_{q,p}[i,j] d_C(c_i, c_j) + \sum_{i \neq j} \Xi_{p,r}[i,j] d_C(c_i, c_j) < \sum_{i \neq j} \Xi_{q,r}[i,j] d_C(c_i, c_j) \\ \Leftrightarrow \quad & \sum_{i \neq j} d_C(c_i, c_j) \left(\Xi_{q,p}[i,j] + \Xi_{p,r}[i,j]\right) < \sum_{i \neq j} \Xi_{q,r}[i,j] d_C(c_i, d_j). \end{aligned}$$

Nach Gleichungen 2.14 und 2.15 gilt

$$\begin{aligned} \sum_{j=1}^{k} \Xi_{q,p}[i,j] + \Xi_{p,r}[i,j] = & \quad q_i + p_i \\ \sum_{i=1}^{k} \Xi_{q,p}[i,j] + \Xi_{p,r}[i,j] = & \quad p_j + r_j \end{aligned}$$

und daraus könnte man eine Paarung mit geringerem Gewicht als $\Xi_{q,r}$ gewinnen. Sei dazu M eine reelle $k \times k$-Matrix mit $M[i,j] = \Xi_{q,p}[i,j] + \Xi_{p,r}[i,j]$. Wir machen aus M eine Paarung für $\widehat{q}$ und $\widehat{r}$, deren Gewicht höchstens $W(M)$ ist.

Wegen Lemma 2.8 können wir annehmen, dass $M[i,i] = \min\{q_i, p_i\} + \min\{p_i, r_i\}$ für alle $1 \leq i \leq k$ gilt. Um eine Paarung zu erhalten, müssen wir die i-ten Zeilen- und Spaltensumme jeweils um p_i reduzieren. Am einfachsten (und gewichtsneutral) geht dies, indem man p_i von $M[i,i]$ abzieht; dies geht allerdings nur für $q_i + r_i \geq p_i$, da eine Paarung keine negativen Einträge haben darf.

Sei j ein problematischer Index, das heißt, $q_j + r_j < p_j$. Ohne Beschränkung der Allgemeinheit sei $q_j < r_j$. Wir müssen insgesamt p_j von Einträgen in der j-ten Zeile beziehungsweise Spalte abziehen. Da $M[j,j] = q_j + r_j$ und weil die j-te Zeilensumme gerade $q_j + p_j$ ist, müssen wir noch $p_j - q_j - r_j$ von der j-ten Zeile abziehen, wenn wir $M[j,j]$ zu Null reduzieren. Eine ähnliche Überlegung zeigt, dass wir von der j-ten Spalte ebenfalls $p_j - q_j - r_j$ abzuziehen haben.

Wir können die Technik aus dem Beweis von Lemma 2.8 verwenden und so die j-te Zeilen- und Spaltensumme um genau den richtigen Betrag

reduzieren, ohne andere Zeilen- oder Spaltensummen zu verändern und ohne das Gewicht zu erhöhen.

Unsere Behandlung von Index j kann andere Diagonalelemente verändern, wird sie aber nur vergrößern, so dass es nur wahrscheinlicher wird, dass man p_i ohne Schwierigkeiten abziehen kann. Sind wir mit allen problematischen j fertig, subtrahieren wir je p_i von allen übrigen Diagonaleinträgen $M[i,i]$ und erhalten eine Paarung, deren Gewicht nicht größer als das von M ist.

Damit ist gezeigt, dass aus der Verletzung der Dreiecksungleichung folgt, dass $\Xi_{q,r}$ nicht optimal gewesen sein kann, im Widerspruch zur Annahme. □

2.5.5 Eigenschaften dieser Metrik

Der Raum $(\widehat{Q}, d)$ kann nicht vollständig sein, denn schon $(S_F^{\mathbb{Z}}, d_C)$ ist nicht vollständig.

Wie sieht es mit den Forderungen aus? Wir zeigen eine allgemeinere Eigenschaft von d, aus der die Gleichungen 2.11 und 2.12 als Spezialfälle folgen.

Lemma 2.10 (Konvexität von d)
Sei $\widehat{q} = q_1\widehat{p} + q_2\widehat{r}$ *mit* $\widehat{p}, \widehat{r} \in \widehat{Q}$. *Dann ist* $d(\widehat{q}, \widehat{p}) \leq q_2 d(\widehat{r}, \widehat{p})$.

Beweis: Seien $\widehat{p} = \sum_{i=1}^{k} p_i c_i$ und $\widehat{r} = \sum_{i=1}^{k} r_i c_i$. Wir beginnen mit dem Fall, dass $\widehat{p}$ und $\widehat{r}$ zueinander orthogonal sind, das heißt, $p_i > 0 \Rightarrow r_i = 0$ und umgekehrt für alle i. Dann gibt es eine optimale Paarung Ξ mit

$$\Xi[i,i] = \min\{q_1 p_i + q_2 r_i, p_i\} = \begin{cases} 0 & p_i = 0 \\ q_1 p_i & p_i \neq 0 \end{cases}.$$

Wir nummerieren die c_i so, dass $p_i > 0$ für alle $1 \leq i \leq l$ gilt und $r_i > 0$ für alle $l < i \leq k$. Dann besteht Ξ aus folgenden Teilen:

1. In der oberen linken Ecke ist eine $l \times l$-Diagonalmatrix deren i-tes Diagonalelement $q_1 p_i$ ist.

2. Die rechte Seite ist eine $k-l \times k$-Nullmatrix.

3. In der unteren linken Ecke ist eine $k-l \times k-l$-Matrix, deren j-te Zeilensumme $q_2 r_j$ ist und deren j-te Spaltensumme $(1-q_1)p_j = q_2 p_j$. Teilt man diese Matrix durch q_2, so erhält man eine optimale Paarung für $\widehat{q}$ und $\widehat{r}$ – wäre sie nicht optimal, so könnte Ξ auch nicht optimal sein.

Das Gewicht der Diagonalmatrix ist Null, und das der Matrix in der linken unteren Ecke ist $q_2 d(\widehat{r}, \widehat{p})$. Im orthogonalen Fall gilt das Lemma also sogar mit einem Gleichheits- anstelle des Ungleichheitszeichens.

Seien nun $\widehat{p}$ und $\widehat{r}$ nicht orthogonal. Bei geeigneter Nummerierung der c_i gibt es dann eine Paarung der Form $q_1\Xi_1 + q_2\Xi_2$, wobei Ξ_1 eine Paarung für $\widehat{p}$ mit sich selber ist und Ξ_2 eine für $\widehat{p}$ und $\widehat{r}$. Das Gewicht dieser Paarung ist $q_2 d(\widehat{p}, \widehat{r})$, aber diese Paarung muss nicht optimal sein. □

Lemma 2.11
Die Metrik d *erfüllt die in den Gleichungen 2.11 und 2.12 formulierten Forderungen.*

Beweis: Aus Lemma 2.10 folgt für den Spezialfall, dass eine der beiden Konfigurationen deterministisch ist,

$$d(c, \widehat{q}) = \sum_{i=1}^{k} p_i d_C(c, c_i).$$

Insbesondere gilt für deterministische Konfigurationen c_1, c_2 :

$$d(c_1, qc_1 + (1-q)c_2) = (1-q)d(c_1, c_2).$$

Wir haben

$$d(c_1, qc_1 + (1-q)c_2) = (1-q)d(c_1, c_2) \text{ und}$$
$$d(c_1, qc_1 + (1-q)c_2) = (1-q)d(c_1, c_3)$$

und damit ist Gleichung 2.11 erfüllt. In ähnlicher Weise folgt Gleichung 2.12.
□

Man hätte die Metrik auf beliebigen Metriken auf $S^{\mathbb{Z}}$ aufbauen können. Sie lässt sich auch auf höhere Dimensionen übertragen, denn wir haben in

keinem unserer Beweise spezielle Eigenschaften der Cantor-Metrik verwendet; solange man d_C durch eine Metrik auf deterministischen Konfigurationen ersetzt, erhält man mit dem beschriebenen Verfahren immer eine Metrik.

2.5.6 Anwendung der Metrik

Wir wenden unsere Metrik an, um die Ähnlichkeit von SZA zu untersuchen. Dieses Thema hat viele Anwendungen und Fragestellungen, die wir unmöglich alle behandeln können; im Hinblick auf das folgende Kapitel über Quantenzellularautomaten konzentrieren wir uns auf die Frage, wie sich kleine Änderungen an der Überführungsfunktion auf das Verhalten von SZA auswirken.

Wir interessieren uns für den Fall, dass die implementierte Überführungsfunktion von der intendierten abweicht. Dies modellieren wir mittels einer stochastischen lokalen Überführungsfunktion der Form

$$\psi = (1 - \varepsilon)\varphi + \varepsilon\varphi',$$

wobei ε die Fehlerwahrscheinlichkeit repräsentiert. Ein Grund für solche Fehler könnten (im Rahmen einer Rechnerarchitektur, die auf ZA basiert) fehlerhaft arbeitende Zellen sein. Andererseits ist es auch denkbar, dass wir mit unserem ZA ein natürliches Phänomen modellieren, dessen stochastisches Verhalten wir in der Überführungsfunktion abzubilden versuchen. Schätzen wir hierbei die Verteilungsfunktion falsch ab, so weicht die Überführungsfunktion unseres Modells von der der Wirklichkeit ab.

Eine andere Motivation entsteht aus der Frage nach zulässigen Übergangswahrscheinlichkeiten. Bis jetzt haben wir keine Einschränkungen vorgenommen; es dürfte aber zumindest schwierig werden, SZA mit nicht berechenbaren Wahrscheinlichkeiten zu realisieren. Wir müssen unter Umständen die gewünschten Wahrscheinlichkeiten mit denen approximieren, die wir realisieren können und müssen uns fragen, wie aussagekräftig die Ergebnisse sein können, die man so erzielt.

Sei also $\psi = (1-\varepsilon)\varphi + \varepsilon\varphi'$ die Überführungsfunktion eines fehlerbehafteten oder approximativen SZA. Wir wenden sie auf eine deterministische

Konfiguration c mit endlichem Träger an. Was ist dann der Abstand zwischen $\psi(c)$ und dem eigentlich beabsichtigten $\varphi(c)$?

Im schlimmsten Fall enthält c nur lokale Konfigurationen, auf denen sich φ und φ' unterscheiden. Dann ist nach einer Anwendung des gestörten SZA jede Zelle im Zustand $(1-\varepsilon)c' + \varepsilon c''$, wobei c' der erwünschte und c'' ein falscher neuer Zustand ist. Wir haben also mit Wahrscheinlichkeit ε einen Unterschied in Zelle 0, mit Wahrscheinlichkeit $(1-\varepsilon)\varepsilon$ einen in Zelle 1 aber keinen in Zelle 0; allgemein kommt mit Wahrscheinlichkeit $(1-\varepsilon)^i\varepsilon$ ein Fehler in Zelle i und keiner in Zelle 0 bis $i-1$ vor. Die gleichen Wahrscheinlichkeiten gelten für die Zellen $-i$; demnach ist die Wahrscheinlichkeit dafür, dass Zelle i oder $-i$ im falschen Zustand ist, während alle Zellen j mit $-i < j < i$ im richtigen Zustand sind

$$(1-\varepsilon)^{2i-1}\varepsilon(2-\varepsilon). \tag{2.17}$$

Gleichung 2.17 beschreibt die Gesamtwahrscheinlichkeit aller deterministischen Konfigurationen, die von $\psi(c)$ den Abstand 2^{-i} haben, für den Fall $i > 0$. Für $i = 0$ ist die gesuchte Wahrscheinlichkeit gleich ε.

Wegen der Konvexität von d ist dann

$$d(\varphi(c), \psi(c)) = \varepsilon + \sum_{i=1}^{T} (1-\varepsilon)^{2i-1}\varepsilon(2-\varepsilon) \cdot 2^{-i} \tag{2.18}$$

falls $T - (N-1)/2$ die Länge des Bereiches nicht-stiller Zellen von c ist. Wegen $(1-\varepsilon)^2/2 < 1$ erhalten wir den Grenzwert für $T \to \infty$ über die Formel der geometrischen Reihe:

$$\begin{aligned}
&\varepsilon + \sum_{i=1}^{\infty} (1-\varepsilon)^{2i-1}\varepsilon(2-\varepsilon) \cdot 2^{-i} \\
&= \varepsilon + \frac{\varepsilon(2-\varepsilon)}{1-\varepsilon} \sum_{i=1}^{\infty} \left(\frac{(1-\varepsilon)^2}{2}\right)^i \\
&= \varepsilon + \frac{\varepsilon(2-\varepsilon)}{1-\varepsilon} \left(\frac{1}{1-\frac{(1-\varepsilon)^2}{2}} - 1\right) \\
&= \varepsilon \frac{3-\varepsilon}{1+2\varepsilon-\varepsilon^2} \\
&< 3\varepsilon.
\end{aligned}$$

Die Abschätzung für $c \in \widehat{Q}$ ist ähnlich: Sei $c = \sum_{i=1}^{k} q_i c_i$. Dann ist $\psi(c) = \sum_{i=1}^{k} q_i \psi(c_i)$. Mit der Konvexität von d folgt

$$\begin{aligned} d(\varphi(c), \psi(c)) &\leq \sum_{i=1}^{k} q_i d(\varphi(c_i), \psi(c_i)) \\ &< \sum_{i=1}^{k} q_i 3\varepsilon = 3\varepsilon. \end{aligned}$$

Die Abweichung im ersten Schritt ist also durchaus klein. Wie sieht es in den folgenden Schritten aus? Betrachten wir wieder für jede Zelle i die Wahrscheinlichkeit, dass sich $\psi^2(c)_i$ und $\varphi^2(c)_i$ unterscheiden. Hier sind zwei Fälle möglich. Im ersten Fall ist bei der ersten Anwendung von ψ ist in der Nachbarschaft von Zelle i kein Fehler aufgetreten und bei der zweiten Anwendung geschieht ein Fehler; die Wahrscheinlichkeit hierfür ist $(1-\varepsilon)^N \varepsilon$.

Der zweite Fall tritt ein, wenn bei der ersten Anwendung von ψ in der Umgebung von i mindestens ein Fehler gemacht wurde, der dazu führt, dass der neue Zustand von Zelle i ebenfalls fehlerhaft ist. Unter der vereinfachenden Annahme, dass bei Anwendung von φ auf eine fehlerhafte lokale Konfiguration nie zufällig der richtige Wert herauskommt, erhalten wir die Wahrscheinlichkeit für den zweiten Fall als $1 - (1-\varepsilon)^N$.

Diese vereinfachende Annahme führt dazu, dass die Wahrscheinlichkeit für einen Unterschied in Zelle 0 ziemlich groß eingeschätzt wird. Daraus erhält man für deterministische globale Konfigurationen c

$$\begin{aligned} d(\varphi(c), \psi(c)) &\geq (1-\varepsilon)^N \varepsilon + 1 - (1-\varepsilon)^N \\ &= 1 - (1-\varepsilon)^{N+1}, \end{aligned} \tag{2.19}$$

das heißt, im Vergleich zur ersten Iteration wäre der Abstand erheblich gewachsen; im Verlauf der weiteren Rechnung würde diese untere Schranke dann gegen 1 konvergieren, weil der Exponent in der zweiten Zeile immer größer würde.

Die Annahme, dass fehlerhafte lokale Konfigurationen nie zufällig zu dem korrekten Ergebnis führen, ist aber nicht nur vereinfachend, sondern sogar unerfüllbar. Nehmen wir daher an, bei Anwendung von φ auf eine

fehlerhafte lokale Konfiguration erhalte man mit Wahrscheinlichkeit p den Wert, den man auch auf der fehlerfreien lokalen Konfiguration bekäme. Damit wird aus Gleichung 2.19

$$\begin{aligned} d(\varphi(c), \psi(c)) &\geq (1-\varepsilon)^N \varepsilon + (1-p)(1-(1-\varepsilon)^N) \\ &= 1 - p - (1-\varepsilon)^N (1 - p - \varepsilon). \end{aligned} \tag{2.20}$$

Man sieht hier, dass es für die Entwicklung der Abweichung entscheidend ist, wie groß diese Wahrscheinlichkeit p ist. Das ist plausibel, denn je stärker φ (oder vielmehr, der Unterschied zwischen φ und ψ) von den Eingaben abhängt, desto stärker sollten sich Fehler auswirken; umgekehrt sollte die Ausgabe eher gegen den richtigen Wert gehen, wenn φ gegenüber Abweichungen in der Eingabe tolerant ist. Eine ähnliche Eigenschaft ist in der statistischen Mechanik aus dem Dobrushin-Shlosman–Kriterium bekannt (siehe zum Beispiel Maes und Shlosman [48]); dieses besagt gerade, dass Markov-Ketten um so schneller ergodisch konvergieren, je schwächer die Überführungsfunktion von den Zuständen abhängt.

Allgemein müssen wir aus diesen Ergebnissen schließen, dass kleine Abweichungen von der lokalen Überführungsfunktion große Auswirkungen haben können. Daher ist es zum Beispiel bei Simulationen wohl keine gute Idee, die Wahrscheinlichkeiten zu raten. Andererseits ist dies in der Praxis häufig erfolgreich. Vielleicht sind die Systeme, die erfolgreich modelliert werden, hinreichend robust. Schließlich scheinen viele SZA ergodisch zu sein, was eine gewisse Robustheit impliziert. Unsere Ergebnisse zeigen jedoch, dass es Situationen gibt, wo es wichtig ist, die richtigen Wahrscheinlichkeiten zu verwenden.

2.6 Zusammenfassung

Wir verfügen nun über eine Definition von stochastischen Zellularautomaten, die auch auf unendliche Konfigurationen übertragbar ist. Als Schwierigkeit bei der Beschreibung von Folgekonfigurationen stellt sich die Entwicklung stochastischer Abhängigkeiten heraus. Im Kapitel über Quantenzellularautomaten werden wir eine ähnlich motivierte Definition entwickeln.

Dort ist die Entwicklung von Verschränkung ein Hindernis bei der globalen Beschreibung (allerdings sollte man Verschränkung und stochastische Abhängigkeit gut voneinander trennen; es handelt sich um verschiedene Eigenschaften).

Es ist für stochastische (und für Quanten-) Rechner wichtig zu wissen, ob man die Auswirkungen von Fehlern prinzipiell begrenzen kann. Bernstein und Vazirani haben 1993 gezeigt [7], dass für Quantenturingmaschinen eine ε-nahe Simulation möglich ist. Um eine vergleichbare Frage für SZA beantworten zu können, muss man globale stochastische Konfigurationen miteinander vergleichen können. Hierfür haben wir erstmals ein Verfahren angegeben und seinen Einsatz demonstriert.

Bei der ε-nahen Simulation von Turingmaschinen ist das Ziel Spracherkennung; bei unserem Modell von SZA liegt der Schwerpunkt anders, weil wir die erzeugten Konfigurationen insgesamt vergleichen. Insbesondere wachsen Abweichungen bei SZA deswegen schneller als bei Turingmaschinen, weil letztere in jedem Berechnungsschritt nur ein Zufallsexperiment durchführen, während SZA maximal so viele durchführen, wie sie aktive Zellen haben. Würden wir mit einem SZA eine Turingmaschine simulieren, wären die Abschätzungen wesentlich günstiger.

KAPITEL 3

Grundlagen zum Quantenrechnen

3.1 Einleitung

Quanteneffekte sind mit klassischen Rechnern außerordentlich schwierig zu modellieren. Dies hat R. Feynman dazu inspiriert, ein Rechnermodell vorzuschlagen, das diese Effekte ausnutzt. Dieses Modell erregt seit einigen Jahren zunehmendes Interesse, vor allem seit der Entwicklung eines polynomialen Faktorisierungsalgorithmus durch Shor [77] und eines Suchverfahrens, das beweisbar schneller ist als jedes äquivalente klassische Verfahren, durch Grover [34].

Für eine umfassende Einführung in die Theorie des Quantenrechnens reicht der Platz hier nicht aus. Daher beschränken wir uns auf eine rein mathematische Behandlung der im nachfolgenden Kapitel benötigten Konzepte und verweisen für alles Weitere auf die Bücher von Gruska [35] oder von Nielsen und Chuang [66] sowie auf das Skript von Preskill [70]; die folgenden Abschnitte sind an alle drei Quellen angelehnt.

Wir beginnen mit der Darstellung von Information in Quantenrechnern. Daran anschließend befassen wir uns damit, wie man mit dieser Information rechnet, wie man also einen Quantenzustand manipuliert. Nach Beendigung der Rechnung müssen wir das Ergebnis ablesen, es folgt daher ein Abschnitt über Messungen.

Für diesen ersten Teil nehmen wir an, wir hätten es mit einem abge-

schlossenen Quantensystem zu tun. Es folgt eine Erweiterung auf offene Systeme; wir führen Dichtematrizen ein, um Zustände zu repräsentieren und Superoperatoren, um mit ihnen zu rechnen. Wir behandeln die operatoralgebraische Sichtweise ausführlicher als in der Literatur zum Quantenrechnen üblich, weil sie uns bei der Definition von Quantenzellularautomaten nützlich sein wird.

Schließlich behandeln wir kurz Verschränkung und Maße für die Ähnlichkeit von Quantenzuständen.

3.2 Information speichern: Quantenbits

Klassische Rechner repräsentieren Information in Form von Bits. Die definierende Eigenschaft eines Bits ist, dass es sich in genau einem von zwei möglichen Zuständen befinden kann, die man üblicherweise mit `0` und `1` bezeichnet.

Quantenrechner sind anders. Sie repräsentieren Information in Form von Quantenbits, kurz qubits. Diese haben zwar ebenfalls nur zwei Basiszustände, $|0\rangle$ und $|1\rangle$, können aber statt in einem von beiden auch in einer *Überlagerung* vorliegen. Eine solche Überlagerung hat die Gestalt

$$\alpha|0\rangle + \beta|1\rangle$$

für komplexe Zahlen α, β, deren Betrag zwischen Null und Eins liegt. Außerdem muss $|\alpha|^2+|\beta|^2 = 1$ sein. Wir können daher ein qubit als einen zweidimensionalen normierten komplexen Vektor (α, β) schreiben. Die Komponenten dieses Vektors heißen *Amplituden*.

Es ist möglich, die Amplituden eines oder mehrerer qubits zu manipulieren und die qubits interagieren zu lassen. Es ist aber nicht möglich, zu einem beliebigen qubit den exakten Quantenzustand, also die Werte von α und β, zu ermitteln. Wird das qubit *gemessen*, so nimmt es einen seiner beiden Basiszustände an, und zwar $|0\rangle$ mit der Wahrscheinlichkeit $|\alpha|^2$ und $|1\rangle$ mit der Wahrscheinlichkeit $|\beta|^2$.

Einige Begriffe sind bis jetzt vage geblieben: Wie interagieren qubits, wie manipuliert man sie, und was genau ist eine Messung? Wir wollen dies

in den folgenden Abschnitten präzisieren, benötigen jedoch zuerst etwas Mathematik.

Wie wir oben schon gesehen haben, sind qubits Elemente eines komplexen Vektorraumes. Diesen statten wir mit einem Skalarprodukt aus. Dabei schreiben wir Vektoren immer in der Dirac-Notation: $|\varphi\rangle$ steht für einen Spalten- $\langle\varphi|$ für einen Zeilenvektor.

Definition 3.1 (Skalarprodukt)
Ein Skalarprodukt auf einem komplexen Vektorraum V ist eine Funktion $\langle\cdot|\cdot\rangle : V \times V \to \mathbb{C}$, für die gilt:

1. *Sie ist positiv: $\langle\varphi|\varphi\rangle > 0$ für alle vom Nullvektor verschiedenen $|\varphi\rangle$.*

2. *Sie ist im zweiten Argument linear:*

$$\langle\varphi|\left(a|\psi_1\rangle + b|\psi_2\rangle\right)\rangle = a\langle\varphi|\psi_1\rangle + b\langle\varphi|\psi_2\rangle.$$

3. *Sie ist schiefsymmetrisch: $\langle\varphi|\psi\rangle = \langle\psi|\overline{\varphi}\rangle$ wobei $\overline{x}$ für das konjugiert Komplexe von $x \in \mathbb{C}$ steht.*

Jedes Skalarprodukt induziert mittels $\|\varphi\| = \sqrt{\langle\varphi|\varphi\rangle}$ eine Norm, aus der wir mit $d(|\varphi\rangle, |\psi\rangle) = \||\varphi\rangle - |\psi\rangle\|$ eine Metrik für V erhalten. V heißt bezüglich dieser Metrik *vollständig*, falls in (V, d) jede Cauchyfolge konvergiert. Ein komplexer Vektorraum mit einem Skalarprodukt, der in diesem Sinne vollständig ist, ist ein *Hilbertraum*.

Der für unsere Zwecke wichtigste Hilbertraum ist durch die ℓ_2-Norm gegeben.

Definition 3.2
Für abzählbare Mengen Q bezeichnet $\ell_2(Q)$ den Raum der komplexwertigen Funktionen auf Q, die durch die ℓ_2-Norm begrenzt sind:

$$\ell_2(Q) = \left\{ f \in \mathbb{C}^Q : \sqrt{\sum_{q \in Q} \overline{f(q)} f(q)} < \infty \right\}. \tag{3.1}$$

Mit dem Skalarprodukt

$$\langle f_1|f_2\rangle = \sum_{q\in Q} \overline{f_1(q)} f_2(q) \tag{3.2}$$

ist $\ell_2(Q)$ ein Hilbertraum.

Im Allgemeinen wollen wir nicht nur ein qubit betrachten, sondern mehrere. Zu jedem von ihnen gehört ein zweidimensionaler Hilbertraum; betrachten wir mehrere zugleich, so beschreiben wir ihren gemeinsamen Zustand durch einen Vektor aus dem *Tensorprodukt* der einzelnen Hilberträume.

Definition 3.3 (Tensorprodukt)
Es seien V und W komplexe Vektorräume, V von der Dimension n und W von der Dimension m. Ein Tensorprodukt ist eine Verknüpfung $\otimes : V\times W \to V\otimes W$, wobei $V\otimes W$ ein nm-dimensionaler komplexer Vektorraum ist, der von den $v\otimes w$ für $v\in V, w\in W$ erzeugt wird. Die Verknüpfung muss folgende Eigenschaften haben:

1. *Für alle $z\in\mathbb{C}, v\in V, w\in W$:*

$$z\,(v\otimes w) = (zv)\otimes w = v\otimes(zw) \tag{3.3}$$

2. *Für alle $v_1, v_2\in V, w\in W$:*

$$(v_1+v_2)\otimes w = v_1\otimes w + v_2\otimes w \tag{3.4}$$

3. *Für alle $v\in V, w_1, w_2\in W$:*

$$v\otimes(w_1+w_2) = v\otimes w_1 + v\otimes w_2 \tag{3.5}$$

Wir beschreiben also zwei qubits durch einen vierdimensionalen Vektor, allgemein n qubits durch einen 2^n-dimensionalen Vektor.

Seien A und B zwei qubits mit den Zuständen $|\varphi_A\rangle = \alpha_1|0\rangle_A + \alpha_2|1\rangle_A$ und $|\varphi_B\rangle = \beta_1|0\rangle_B + \beta_2|1\rangle_B$. Ihr Tensorprodukt $A\otimes B$ ist dann im Zustand

$$\begin{aligned}
& |\varphi_A\rangle\otimes|\varphi_B\rangle \\
= \;& (\alpha_1|0\rangle_A + \alpha_2|1\rangle_A)\otimes(\beta_1|0\rangle_B + \beta_2|1\rangle_B \\
= \;& \alpha_1\beta_1(|0\rangle_A\otimes|0\rangle_B) + \alpha_1\beta_2(|0\rangle_A\otimes|1\rangle_B) \\
& +\alpha_2\beta_1(|1\rangle_A\otimes|0\rangle_B) + \alpha_2\beta_2(|1\rangle_A\otimes|1\rangle_B) \\
= \;& \alpha_1\beta_1|00\rangle + \alpha_1\beta_2|01\rangle + \alpha_2\beta_1|10\rangle + \alpha_2\beta_2|11\rangle,
\end{aligned}$$

wobei wir in der letzten Zeile die tensorierten Einzelvektoren zu Vektoren der Länge zwei zusammengefasst haben. Der Zustandsvektor im Gesamtsystem ist $(\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2)$. Die Möglichkeit zum Ausmultiplizieren existiert dank der Linearität von Quantensystemen.

3.3 Quantenzustände manipulieren

Um zu rechnen, muss es möglich sein, den Zustand eines Quantensystems zu verändern. Das Verhalten eines physikalischen Systems (definiert als die Änderung seines Zustandes mit der Zeit) ist vollständig durch den Hamiltonoperator H festgelegt. Der Vektor, der den Systemzustand beschreibt, verändert sich gemäß der Schrödinger-Gleichung

$$\frac{d}{dt}|\varphi(t)\rangle = -iH|\varphi(t)\rangle. \tag{3.6}$$

Für Hamiltonoperatoren H, die nicht von der Zeit abhängen, erhält man aus Gleichung 3.6:

$$|\varphi(t)\rangle = e^{-itH}|\varphi(0)\rangle. \tag{3.7}$$

Es hat sich in der Literatur zum Quantenrechnen eingebürgert, Rechnungen durch Angabe von e^{-itH} zu spezifizieren. Nicht jeder Operator lässt sich in dieser Form schreiben, wenn H ein Hamilton-Operator sein soll, denn nicht jeder Operator lässt sich als Hamilton-Operator auffassen.

Sei A ein Operator auf einem Vektorraum V. Dann bezeichnet $A^\dagger$ die *Adjungierte* von A, also den eindeutig bestimmten Operator, für den gilt:

$$\langle v|Aw\rangle = \langle A^\dagger v|w\rangle \tag{3.8}$$

für alle $v, w \in V$. Für Matrizen A erhält man $A^\dagger$, indem man A transponiert und jeden Eintrag durch sein komplex Konjugiertes ersetzt. Dann steht $\langle v|A$ beziehungsweise $A|w\rangle$ für ein Vektor-Matrix beziehungsweise Matrix-Vektor-Produkt.

Ein Operator A heißt *selbstadjungiert* oder *hermitesch*, wenn $A = A^\dagger$ ist. Die Hamilton-Operatoren von Quantensystemen sind immer selbstadjungiert. Daraus folgt, dass der Operator $U = e^{-itH}$ aus Gleichung 3.7 unitär sein muss; das heißt, es muss gelten $UU^\dagger = I$, wobei I für die Identität steht.

Solange wir Quantenzustände als endlichdimensionale Vektoren in Hilberträumen schreiben, handelt es sich bei diesen Operatoren immer um Matrizen.

Die Forderung nach Unitarität impliziert insbesondere die Forderung nach Reversibilität, denn jede unitäre Matrix ist invertierbar, folglich ist jeder mit unitären Matrizen beschreibbare Prozess zumindest theoretisch reversibel.

Anschaulich bedeutet die Unitarität einer Matrix, dass sie die Norm von und die Winkel zwischen Vektoren erhält. Daher müssen die Zeilen- und Spaltenvektoren einer solchen Matrix normiert und paarweise orthogonal sein.

Beispiele für eine unitäre Matrizen sind die Hadamard-Transformation:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.9}$$

und die Drehung um ω:

$$U_\omega = \begin{pmatrix} e^{i\omega} & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.10}$$

Um vorzuführen, wie zwei qubits miteinander interagieren, geben wir noch die unitäre Matrix für eine Operation an, die als `CNOT` (für *controlled not*) bekannt ist:

$$U_{\text{cnot}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.11}$$

Wenden wir U_{cnot} auf einen Quantenzustand $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, dargestellt durch den Vektor $(\alpha_{00}\alpha_{01}\alpha_{10}\alpha_{11})$, an, so erhalten wir

$$U_{\text{cnot}} \cdot (\alpha_{00}\alpha_{01}\alpha_{10}\alpha_{11})^T = (\alpha_{00}\alpha_{01}\alpha_{10}\alpha_{11})^T.$$

Für den Spezialfall, dass alle α_{ij} entweder 0 oder 1 sind, ergibt sich

$$\begin{aligned} U_{cnot}|00\rangle &= |00\rangle \\ U_{cnot}|01\rangle &= |01\rangle \\ U_{cnot}|10\rangle &= |11\rangle \\ U_{cnot}|11\rangle &= |10\rangle, \end{aligned}$$

das heißt, das zweite qubit wird negiert, falls das erste im Zustand $|1\rangle$ ist.

Angenommen, wir haben zwei Gruppen von qubits; jede ist durch Vektoren in einem Hilbertraum beschrieben und beide Gruppen zusammen durch Vektoren aus dem Tensorprodukt der Hilberträume. Haben wir nun Matrizen, die auf den beiden Gruppen getrennt operieren, so operiert auf dem Tensorprodukt der Hilberträume das Tensorprodukt dieser Matrizen.

Dieses ist wie folgt definiert. Zu Matrizen $A = (a_{ij})_{1\leq i,j\leq n}$ und $B = (b_{kl})_{1\leq k,l\leq m}$ ist $A \otimes B$ eine nm-dimensionale Matrix:

$$\begin{pmatrix} a_{11}\cdot B & a_{12}\cdot B & \dots & a_{1n}\cdot B \\ a_{21}\cdot B & & & \\ \vdots & & \dots & \vdots \\ a_{n1}\cdot B & a_{n2}\cdot B & \dots & a_{nn}\cdot B \end{pmatrix}. \tag{3.12}$$

Jegliche Quantenrechnungen lassen sich durch Angabe der entsprechenden unitären Matrizen spezifizieren. Man erhält ein universelles Berechnungsmodell; Quanten-Turingmaschinen haben zum Beispiel Benioff [4, 5], Deutsch [21] sowie Bernstein und Vazirani [7] untersucht.

3.4 Das Ergebnis extrahieren

Will man etwas über den Zustand eines oder mehrerer qubits erfahren, so muss man messen. Dabei erfährt man nicht die Werte der einzelnen Amplituden; vielmehr ist das Ergebnis stochastisch und darüber hinaus zerstört die Messung den Originalzustand.

Wir beginnen mit dem einfachen Fall, dem der projektiven Messung. Gemessen werden immer *Observable*. Das sind Eigenschaften wie zum Beispiel der Aufenthaltsort oder die Geschwindigkeit eines Teilchens, die prinzipiell

messbar sind. Formal entspricht einer Observablen ein selbstadjungierter Operator.

Ist A eine selbstadjungierte Matrix in einem Hilbertraum $\mathcal{H}$, so bilden die Eigenvektoren von A eine Orthonormalbasis von $\mathcal{H}$. Bezüglich dieser Orthonormalbasis hat A die Gestalt $\sum_n a_n P_n$, wobei die a_n die Eigenwerte von A sind und die P_n Projektionen auf die entsprechenden Eigenräume. Die Projektionen P_n sind vollständig in dem Sinne, dass $\sum_n P_n$ die Einheitsmatrix ist und sie sind paarweise orthogonal in dem Sinne, dass für alle n, m gilt: $P_n P_m = \delta_{n,m} P_n$, wobei $\delta_{n,m}$ für das Kronecker-Delta steht.

Das Ergebnis der Messung einer Observablen A ist ein Eigenwert von A. Dieser ist reell, denn selbstadjungierte Matrizen haben nur reelle Eigenwerte. Nachdem das Messergebnis abgelesen ist, befindet sich das System in einem Zustand aus dem Eigenraum von A zu dem gemessenen Eigenwert, genauer, in der Projektion des Ausgangszustandes in den Eigenraum. Darüber, welcher Eigenwert bei der Messung beobachtet wird, kann man nur eine stochastische Aussage treffen: Ist der Quantenzustand vor der Messung $|\varphi\rangle$, so beobachten wir den Eigenwert a_n mit der Wahrscheinlichkeit

$$||P_n|\varphi\rangle||^2 = \langle\varphi|P_n|\varphi\rangle \tag{3.13}$$

und in diesem Fall befindet sich das System nach der Messung in dem Zustand

$$\frac{P_n|\varphi\rangle}{\sqrt{\langle\varphi|P_n|\varphi\rangle}}. \tag{3.14}$$

Der Term im Nenner dient dabei der Renormalisierung. Die Messung projiziert den Zustand des Quantensystems in den Eigenraum zu dem gemessenen Eigenwert; daher ergibt jede weitere Messung mit der gleichen Observablen das gleiche Ergebnis wie die erste.

Wichtige Observable eines qubits sind die Pauli-Matrizen:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{3.15}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{3.16}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.17}$$

Die Pauli-Matrizen sind nicht nur selbstadjungiert, sondern auch unitär. Außerdem sind sie ein Beispiel für nicht-kommutierende Observable. Diese Eigenschaft ist wichtig, denn wenn zwei Observable nicht kommutieren, messen sie Eigenschaften, deren exakte Kenntnis sich gegenseitig ausschließt. Ein berühmtes Beispiel sind Geschwindigkeit und Aufenthaltsort eines Elektrons. Formal kommutieren zwei Observable genau dann, wenn sie *simultan diagonalisierbar* sind, das heißt, wenn sie bezüglich der gleichen Basis Diagonalgestalt haben.

Die Gesamtheit der Observablen eines Systems repräsentiert alles, was man durch Messung über den Systemzustand erfahren kann. Wir gehen in Abschnitt 3.6 genauer auf die Rolle von Observablen bei der Beschreibung von Zuständen ein.

3.5 Nicht-abgeschlossene Quantensysteme

3.5.1 Nicht alle Zustände sind Tensorprodukte

Bis jetzt sind wir vereinfachend davon ausgegangen, dass unser Quantensystem abgeschlossen ist: Der Zustandsvektor gibt eine vollständige Beschreibung des Systems zu einem gewissen Zeitpunkt und es findet abgesehen von eventuellen Messungen keine Interaktion mit der Außenwelt statt.

Nehmen wir nun aber an, wir hätten ein System, das aus zwei qubits besteht, von denen wir nur eines manipulieren und beobachten können. Wir kennen den Zustandsvektor des Gesamtsystems und wollen daraus ein Modell für unsere eingeschränkte Sicht entwickeln. Dieser Vektor könnte

$|\varphi\rangle = \alpha(|0\rangle_A \otimes |0\rangle_B) + \beta(|1\rangle_A \otimes |1\rangle_B)$ sein. Hier besteht eine Beziehung zwischen den Zuständen der qubits A und B; insbesondere ist es nicht möglich, $|\varphi\rangle$ als Tensorprodukt der Einzelzustände zu schreiben. Dieses Phänomen heißt *Verschränkung* und wir werden später näher darauf eingehen.

Wir messen qubit A in der Basis $\{|0\rangle_A, |1\rangle_A\}$. Mit der Wahrscheinlichkeit $|\alpha|^2$ finden wir qubit A im Zustand $|0\rangle_A$ vor; in diesem Fall befindet sich das Gesamtsystem nach der Messung im Zustand $|0\rangle_A \otimes |0\rangle_B$. Jede zukünftige Messung von qubit B wird es von nun an mit Sicherheit im Zustand $|0\rangle_B$ vorfinden.

Wir können eine Observable M_A, die nur qubit A misst, auf dem Tensorprodukt der beiden Hilberträume $\mathcal{H}_A$ und $\mathcal{H}_B$ durch $M_A \otimes I_B$ fortsetzen. Dabei steht I_B für die Identität auf $\mathcal{H}_B$. Wenden wir diese Observable auf den Zustand $|\varphi\rangle$ an, so erhalten wir

$$\begin{aligned}
&\langle\varphi|M_A \otimes I_B|\varphi\rangle \\
&= \left(\overline{\alpha}_A\langle 0| \otimes {}_B\langle 0| + \overline{\beta}_A\langle 1| \otimes {}_B\langle 1|\right)(M_A \otimes I_B)\left(\alpha|0\rangle_A \otimes |0\rangle_B + \beta|1\rangle_A \otimes |1\rangle_B\right) \\
&= |\alpha|^2{}_A\langle 0|M_A|0\rangle_A + |\beta|^2{}_A\langle 1|M_A|1\rangle_A.
\end{aligned}$$

Dieser Ausdruck läßt sich umschreiben zu

$$\mathrm{tr}(M_A\rho_A). \tag{3.18}$$

Dabei steht tr für die Spur der Matrix (die Summe der Diagonalelemente) und ρ_A für eine Matrix der Form

$$\rho_A = |\alpha|^2|0\rangle_{AA}\langle 0| + |\beta|^2|1\rangle_{AA}\langle 1|. \tag{3.19}$$

Solche Matrizen nennt man *Dichtematrizen*. In ihrer allgemeinen Gestalt

$$\rho = \sum_i p_i|\varphi_i\rangle\langle\varphi_i|. \tag{3.20}$$

kann man die Dichtematrix als eine Wahrscheinlichkeitsverteilung interpretieren, die dem Quantenzustand $|\varphi_i\rangle$ die Wahrscheinlichkeit p_i zuordnet. Daraus folgt, dass jede Dichtematrix ρ positiv sein und $\mathrm{tr}(\rho) = 1$ erfüllen muss. Tatsächlich sind diese beiden Bedingungen nicht nur notwendig, sondern auch hinreichend.

Die Zustände, die man als Vektoren eines Hilbertraumes schreiben kann, heißen *rein*. Die Dichtematrix zu einem reinen Zustand $|\varphi\rangle$ hat die Form $|\varphi\rangle\langle\varphi|$. Dichtematrizen wie in Gleichung 3.20 beschreiben im Allgemeinen *gemischte* Zustände. Es gibt verschiedene Zustände, die die gleiche Dichtematrix haben; man kann sie allerdings nicht durch projektive Messung unterscheiden.

Als Beispiel sei $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Die Dichtematrix ist

$$|\varphi\rangle\langle\varphi| = \begin{pmatrix} |\alpha|^2 & \alpha\overline{\beta} \\ \overline{\alpha}\beta & |\beta|^2 \end{pmatrix}.$$

Der Zustand $|\varphi'\rangle = -\alpha|0\rangle - \beta|1\rangle$ hat die gleiche Dichtematrix wie $|\varphi\rangle$, denn $|\varphi\rangle$ und $|\varphi'\rangle$ unterscheiden sich nur um den *globalen Phasenfaktor* -1 und die Wahrscheinlichkeiten dafür, bei einer projektiven Messung $|0\rangle$ oder $|1\rangle$ zu erhalten, sind in beiden Fällen gleich.

Dichtematrizen von Zuständen sind hermitesch; $|\varphi\rangle\langle\varphi|$ entspricht gerade dem Messoperator, der feststellt, ob sich ein System in dem reinen Zustand $|\varphi\rangle$ befindet.

Unser Beispiel mit den qubits A und B illustriert einen Spezialfall, nämlich die *reduzierte* Dichtematrix. Sie ist nützlich, um unsere eingeschränkte Sicht zu modellieren, indem wir den Beitrag von B aus der Zustandsgleichung eliminieren. Man nennt diese Elimination auch *Ausspuren* (tracing out) von B. Für Hilberträume $\mathcal{H}_A$ und $\mathcal{H}_B$ mit Orthonormalbasen $\mathcal{B}_A$ und $\mathcal{B}_B$ ist die reduzierte Dichtematrix ρ_A eines Zustandes $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ durch folgende Gleichung gegeben.

$$\rho_A = \mathrm{tr}_{\mathcal{H}_B}(\rho) = \sum_{|\varphi\rangle,|\varphi'\rangle \in \mathcal{B}_A} |\varphi\rangle \left(\sum_{|\psi\rangle \in \mathcal{B}_B} \langle \varphi, \psi|\rho|\varphi', \psi\rangle \right) \langle\varphi'| \qquad (3.21)$$

3.5.2 Nicht jede Entwicklung ist unitär

Wenn wir Zustände mit Dichtematrizen repräsentieren, brauchen wir eine passende Darstellung der Operationen, die auf diesen Zuständen möglich sind. Oben haben wir unitäre Matrizen eingeführt, die auf reinen Zuständen agieren. Im Allgemeinen sind aber Zustände nicht rein, sondern ge-

mischt, und wir brauchen eine allgemeinere Formulierung dessen, was wir als Quantenoperationen erlauben.

Wir suchen Operatoren, die Dichtematrizen auf Dichtematrizen abbilden. Falls der Operator eine unitäre Transformation U implementiert, können wir ihn für Dichtematrizen ρ als

$$\mathcal{E}(\rho) = U\rho U^\dagger$$

schreiben.

Verallgemeinern wir dies nun auf ein zweiteiliges Quantensystem, das aus einem Hauptystem und einer Umgebung besteht; ersteres befindet sich im Zustand ρ, letzteres im Zustand ρ_E. Wir gehen davon aus, dass sie zu Beginn nicht miteinander verschränkt sind, das heißt, wir können ihren gemeinsamen Zustand als Tensorprodukt $\rho \otimes \rho_E$ schreiben. Anwendung des unitären Operators U liefert den neuen Zustand

$$U(\rho \otimes \rho_E)U^\dagger.$$

Um hieraus den Zustand des Hauptsystems zu isolieren, spuren wir den der Umgebung mittels tr_E aus. Betrachten wir nur den Zusammenhang zwischen dem alten und dem neuen Zustand des Hauptsystems:

$$\mathcal{E}(\rho) = \mathrm{tr}_E \left(U(\rho \otimes \rho_E)U^\dagger \right). \tag{3.22}$$

Aus dieser Gleichung gewinnen wir eine Summendarstellung des Operators $\mathcal{E}$. Dazu sei $|e_k\rangle$ eine Basis des endlichdimensionalen Hilbertraumes der Umgebung; $|e_0\rangle\langle e_0|$ stehe für den Anfangszustand der Umgebung. Damit wird aus Gleichung 3.22:

$$\mathcal{E}(\rho) = \sum_k \langle e_k|U \left(\rho \otimes |e_0\rangle\langle e_0|\right) U^\dagger|e_k\rangle \tag{3.23}$$

$$= \sum_k E_k \rho E_k^\dagger, \tag{3.24}$$

wobei $E_k = \langle e_k|U|e_0\rangle$ ein Operator auf dem Zustandsraum des Hauptystems ist. Für eine Basis $|i\rangle, |j\rangle, \ldots$ des Hauptsystems (also des Gesamtsystems ohne die Umgebung), ist der Eintrag in der i-ten Zeile und j-ten

Spalte der Matrixdarstellung von E_k gleich $(\langle i| \otimes \langle e_k|)\, U\, (|j\rangle \otimes |e_0\rangle)$. Gleichung 3.24 beschreibt die *Operatorsummen-Darstellung* von $\mathcal{E}$. Solche Operatoren heißen auch *Superoperatoren* oder *vollständig positive Abbildungen* (completely positive maps).

Definition 3.4 (Superoperator)
Ein Superoperator $\mathcal{E}$ ist eine Abbildung von Matrizen auf Matrizen mit den Eigenschaften:

1. $0 \leq \mathrm{tr}(\mathcal{E}(\rho)) \leq 1$ *für alle* ρ,
2. *Für gemischte Zustände* $\sum_i p_i \rho_i$ *gilt*

$$\mathcal{E}\left(\sum_i p_i \rho_i\right) = \sum_i p_i \mathcal{E}(\rho_i),$$

3. $\mathcal{E}$ *ist vollständig positiv. Das heißt, für jede positiv definite Matrix* ρ *ist* $\mathcal{E}(\rho)$ *positiv definit. Ist ferner* R *ein beliebigdimensionales weiteres Quantensystem und* I_R *die Identität auf* R, *so ist* $(I \otimes \mathcal{E})(\rho)$ *für alle positiv definiten* ρ *positiv definit.*

Superoperatoren mit Spur 1 bilden Dichtematrizen auf Dichtematrizen ab. Diese Definition ist äquivalent zu unserer früheren Herleitung: Jeder Superoperator besitzt eine Summendarstellung und umgekehrt.

3.5.3 Nicht alle Messungen sind orthogonale Projektionen

Projektive Messungen sind für viele Zwecke völlig ausreichend. In diesem Abschnitt führen wir einen allgemeineren Formalismus ein, der in mancher Hinsicht eleganter und flexibler, wenn auch nicht mächtiger, ist. Es handelt sich dabei um Maße, deren Wertebereich aus positiven Operatoren besteht. Ein Operator heißt positiv, wenn seine Norm größer als Null ist. Diese Klasse von Maßen wird als POVM bezeichnet (für *Positive Operator-Valued Measure*).

Definition 3.5 (POVM)
Ein POVM besteht aus einer Menge $\{E_m\}$ *von positiven Operatoren mit der Eigenschaft* $\sum_m E_m = I$, *wobei* I *für die Einheitsmatrix steht.*

Die Operatoren agieren auf dem Hilbertraum der Quantenzustände. Der Index m kodiert das Ergebnis der Messung; die Wahrscheinlichkeit, das Ergebnis m zu beobachten, ist

$$\langle\varphi|E_m|\varphi\rangle. \tag{3.25}$$

POVMs unterscheiden sich von projektiven Messungen nur dadurch, dass die E_m nicht paarweise orthogonal sein müssen. Es ist möglich, jedes POVM durch eine projektive Messungen und unitäre Matrizen zu simulieren.

Ein Vorteil an der Superoperatorschreibweise besteht darin, dass auch Messungen Superoperatoren sind. Messungen entsprechen Superoperatoren, die nicht notwendigerweise spurerhaltend sind, also $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$ mit $\sum_k E_k^\dagger E_k \leq I$.

3.6 Operatoralgebra

In der Informatik-Literatur zum Quantenrechnen wird üblicherweise ausschließlich mit Vektoren in Hilberträumen gerechnet. Bei Quantenzellularautomaten liegt aber eine ungewöhnliche Situation vor, denn jede einzelne Zelle „sieht“ nur einen kleinen Ausschnitt der globalen Konfiguration; die bisher eingesetzten, auf Vektoren in Hilberträumen basierenden, Definitionen, geraten hier in Schwierigkeiten, wie wir noch sehen werden. Wir führen daher nun einen Beschreibungsformalismus ein, der eher aus der mathematischen Physik motiviert ist, nämlich Operatoralgebren. Die Betrachtungen über Dichteoperatoren aus Abschnitt 3.5 können wir mit Hilfe dieser Algebren vertiefen.

Sei $\mathcal{H}$ ein komplexer Hilbertraum. Die bezüglich der Operatornorm

$$||P|| = \sup_{\varphi\in\mathcal{H}:||\varphi||=1} ||P\varphi|| \tag{3.26}$$

beschränkten Operatoren auf $\mathcal{H}$ bilden eine Algebra, die wir mit $\mathcal{B}(\mathcal{H})$ bezeichnen. Sie ist unter Adjunktion abgeschlossen: mit A ist auch $A^\dagger$ ein

Element von $\mathcal{B}(\mathcal{H})$. Darüber hinaus verleiht die Norm des Hilbertraumes $\mathcal{H}$ der Algebra der beschränkten Operatoren ebenfalls eine Norm und $\mathcal{B}(\mathcal{H})$ ist bezüglich der von dieser Norm induzierten Metrik abgeschlossen. Demnach ist $\mathcal{B}(\mathcal{H})$ gemäß der folgenden Definition eine $C^\star$-Algebra.

Definition 3.6 ($C^\star$-Algebra)
Eine $C^\star$-Algebra ist ein vollständiger normierter Raum $(A, +, \|\cdot\|)$ über den komplexen Zahlen zusammen mit Operationen $\cdot : A \times A \to A$ und $\star : A \to A$, in dem für alle $a, b, c \in A$ und $\alpha, \beta \in \mathbb{C}$ gilt:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$
2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. $(\alpha a) \cdot (\beta b) = \alpha\beta(a \cdot b)$
4. $a^{\star\star} = a$, $(\alpha a)^\star = \overline{\alpha} a^\star$, $(a + b)^\star = a^\star + b^\star$, $(a \cdot b)^\star = b^\star \cdot a^\star$
5. $\|a \cdot b\| \leq \|a\|\|b\|$, $\|a^\star \cdot a\| = \|a\|^2$

Eine Einführung in die Theorie der $C^\star$-Algebren findet man in dem Buch von Bratteli und Robinson [9] oder dem Skript von de la Harpe und Jones [18]; wir geben hier nur diejenigen Ergebnisse an, die im folgenden Kapitel Verwendung finden.

Die beschränkten Observablen auf $\mathcal{H}$ sind gerade die hermiteschen Elemente von $\mathcal{B}(\mathcal{H})$; sie bilden eine Teil-$C^\star$-Algebra von $\mathcal{B}(\mathcal{H})$, die auch *Observablenalgebra* (von $\mathcal{H}$) heißt. Zum Beispiel sind die Pauli-Matrizen Elemente der Observablenalgebra des Hilbertraumes, in dem die Zustände eines qubits liegen; ebenso sind die Dichteoperatoren aus Abschnitt 3.5.1 Elemente der entsprechenden Observablenalgebren.

Für n-dimensionale Hilberträume $\mathcal{H}$ mit $n < \infty$ können wir die Elemente von $\mathcal{B}(\mathcal{H})$ immer als $n \times n$-Matrizen schreiben. Sowohl $\mathcal{B}(\mathcal{H})$ als auch die Observablenalgebra enthalten die Identität I; es handelt sich jeweils um $C^\star$-Algebren mit Identität, sogenannte *unitale* $C^\star$-Algebren.

Was ist nun der Zusammenhang zwischen Zuständen und Operatoren? Sei dazu $|\varphi\rangle$ ein Zustand, gegeben als Element des Hilbertraumes $\mathcal{H}$, und ρ

ein Operator aus $\mathcal{B}(\mathcal{H})$. Dann definiert $|\varphi\rangle$ eine Abbildung $f_\varphi : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ mit

$$f_\varphi(\rho) = \langle\varphi|\rho|\varphi\rangle. \tag{3.27}$$

Diese Abbildung ist *positiv*: Ist ρ ein positiver Operator (das heißt, gibt es $\tau \in \mathcal{B}(\mathcal{H})$ mit $\rho = \tau^\dagger\tau$), so ist $f_\varphi(\rho)$ eine nichtnegative reelle Zahl.

Es definiert folglich jeder Vektor aus $\mathcal{H}$ eine positive Abbildung von $\mathcal{B}(\mathcal{H})$ in $\mathbb{C}$. Umgekehrt ist durch jede positive Abbildung von $\mathcal{B}(\mathcal{H})$ in $\mathbb{C}$, die auf dem Einselement von $\mathcal{B}(\mathcal{H})$ den Wert 1 annimmt, eindeutig ein Zustand festgelegt. Dies motiviert die folgende Definition.

Definition 3.7
Ein Zustand einer unitalen $C^\star$-Algebra $\mathcal{A}$ ist eine positive identitätserhaltende Linearform $f : \mathcal{A} \to \mathbb{C}$.

Der *Zustandsraum* S_A von $\mathcal{A}$ ist die Menge aller Zustände von $\mathcal{A}$. S_A ist eine konvexe Teilmenge des Dualraumes von $\mathcal{A}$. Ein Zustand ist genau dann rein, wenn er sich nicht als konvexe Linearkombination von Zuständen schreiben lässt. Zum Beispiel bilden die Pauli-Matrizen eine Basis der Observablenalgebra des Hilbertraumes $\mathbb{C}^2$. Der zugehörige Zustandsraum ist isomorph zur dreidimensionalen Kugel und die reinen Zustände entsprechen den Punkten auf der Oberfläche. Diese Kugel heißt auch *Bloch–Kugel*.

Ist $\mathcal{A}$ endlich-dimensional, so ist der Dualraum von $\mathcal{A}$ isomorph zu $\mathcal{A}$. Damit können wir begründen, warum Dichteoperatoren (die ja eigentlich Elemente der Observablenalgebra sind) als Repräsentanten von Zuständen dienen. Für endlich-dimensionale $\mathcal{A}$ gibt es zu jedem Zustand $f : \mathcal{A} \to C$ ein $\rho \in \mathcal{A}$ mit

$$f(a) = \mathrm{tr}(\rho a) \tag{3.28}$$

für alle $a \in \mathcal{A}$. Dieses ρ ist gerade der Dichteoperator des Zustandes f. Wenn ρ eine Projektionsmatrix mit Rang 1 ist, ist f ein reiner Zustand.

Um die Bedeutung von Gleichung 3.27 zu illustrieren, betrachten wir folgendes Beispiel. Sei $|\varphi\rangle$ ein normierter Vektor aus $\mathcal{H}$ und ρ eine beschränkte Observable. Falls ρ Rang 1 hat, ist $\langle\varphi|\rho|\varphi\rangle$ gemäß Gleichung 3.13 gerade die

Wahrscheinlichkeit, bei einer Messung von $|\varphi\rangle$ mit der Observablen ρ als Ergebnis den einzigen von Null verschiedenen Eigenwert von ρ zu erhalten.

Ist ρ ein beliebiges Element der Observablenalgebra, so ist ρ hermitesch und besitzt demnach bezüglich einer geeignet gewählten Orthonormalbasis die Darstellung $\sum_n a_n P_n$ wie auf Seite 98. Nehmen wir ohne Einschränkung an, φ wäre in dieser geeigneten Orthonormalbasis gegeben. Dann ist

$$\begin{aligned}\langle\varphi|\rho|\varphi\rangle &= \langle\varphi|\sum_n a_n P_n|\varphi\rangle \\ &= \sum_n a_n \left(\langle\varphi|P_n|\varphi\rangle\right),\end{aligned}$$

$\langle\varphi|\rho|\varphi\rangle$ ist der Erwartungswert des Messergebnisses von φ mit der Observablen ρ. Definition 3.7 fasst Zustände als Funktionale auf, die jeder Observablen den Erwartungswert des entsprechenden Messergebnisses zuordnen.

Als nächstes beschäftigen wir uns mit linearen Abbildungen von $C^\star$-Algebren, den sogenannten $\star$-Morphismen.

Definition 3.8
Ein $\star$-Morphismus ist eine lineare Abbildung $V : \mathcal{A} \to \mathcal{B}$ von $C^\star$-Algebren, so dass für alle $a, b \in \mathcal{A}$ gilt:

$$V(ab) = V(a)V(b) \text{ und } V(a^\star) = (V(a))^\star.$$

$\star$-Morphismen erhalten die Struktur von $C^\star$-Algebren, denn $V(\mathcal{A})$ ist immer eine $C^\star$-Unteralgebra von $\mathcal{B}$. Ein $\star$-Automorphismus von $\mathcal{A}$ ist ein bijektiver $\star$-Morphismus von $\mathcal{A}$ nach $\mathcal{A}$. Die $\star$-Automorphismen von $\mathcal{A}$ bilden die Gruppe $\mathrm{Aut}(\mathcal{A})$.

Einen Spezialfall von $\star$-Automorphismen eines Hilbertraumes $\mathcal{H}$ erhält man aus den unitären Elementen von $\mathcal{B}(\mathcal{H})$. Ist nämlich $U \in \mathcal{B}(\mathcal{H})$ unitär, so definiert U mittels der Abbildungsvorschrift

$$a \mapsto U^\dagger a U$$

für $a \in \mathcal{B}(\mathcal{H})$ einen $\star$-Automorphismus von $\mathcal{B}(\mathcal{H})$. Diese $\star$-Automorphismen heißen auch *innere* Automorphismen von $\mathcal{B}(\mathcal{H})$. In endlichen $C^\star$-Algebren

lässt sich jeder $\star$-Automorphismus in bis auf Isomorphie eindeutig bestimmter Weise aus einem inneren Automorphismus und einer endlichen Menge von Permutationen zusammensetzen.

Wir kommen nun zu den Operatoralgebren tensorierter Hilberträume. Der Einfachheit halber betrachten wir endliche Produkte endlichdimensionaler Räume. Dann ist die Observablenalgebra des Tensorproduktes durch das Tensorprodukt der Observablenalgebren der Faktorräume wie folgt gegeben.

Seien $\mathcal{H}_1, \ldots, \mathcal{H}_n$ endlichdimensionale Hilberträume mit den Dimensionen $d_1, \ldots, d_n$. Zu $\mathcal{H}_i$ bezeichne $\mathcal{B}(\mathcal{H})_i$ die $C^\star$-Algebra der beschränkten Operatoren auf $\mathcal{H}_i$. Für alle i zwischen 1 und n ist $\mathcal{B}(\mathcal{H})_i$ endlichdimensional und folglich nach einem Satz aus der Theorie der $C^\star$-Algebren isomorph zu einer vollen Matrixalgebra auf dem Hilbertraum $\mathbb{C}^{d_i}$. Das Tensorprodukt der Operatoralgebren definieren wir dann mittels des Tensorproduktes dieser Matrixalgebren (welches wiederum elementweise über das Tensorprodukt der Matrizen definiert ist). Zusammenfassend erhalten wir auf dem Hilbertraum

$$\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$$

die Operatoralgebra

$$\mathcal{B}(\mathcal{H}) = \bigotimes_{i=1}^{n} \mathcal{B}(\mathcal{H})_i.$$

Das Element $\rho_1 \otimes \ldots \otimes \rho_n$ von $\mathcal{B}(\mathcal{H})$ operiert auf $\nu_1 \otimes \ldots \otimes \nu_n \in \mathcal{H}$ gemäß

$$\bigotimes_{i=1}^{n} \rho_i \left(\bigotimes_{i=1}^{n} \nu_i \right) = \bigotimes_{i=1}^{n} \rho_i (\nu_i) .$$

Da wir grundsätzlich unitale $C^\star$-Algebren betrachten, gibt es eine kanonische Einbettung der Faktoren in das Tensorprodukt der Algebren. Definieren wir $g : \mathcal{B}(\mathcal{H})_i \to \mathcal{B}(\mathcal{H})_i \otimes \mathcal{B}(\mathcal{H})_j$ durch $g(\rho_i) = \rho_i \otimes I_j$, wobei I_j für die Einheitsmatrix auf $\mathcal{H}_j$ steht, so ist $g(\mathcal{B}(\mathcal{H})_i)$ eine Teil-C^*-Algebra von $\mathcal{B}(\mathcal{H})_i \otimes \mathcal{B}(\mathcal{H})_j$.

Ist nun $f : \mathcal{H}(\mathcal{B})_i \otimes \mathcal{H}(\mathcal{B})_j \to \mathbb{C}$ ein Zustand, so erhalten wir durch

$$\begin{aligned} f_1 : \mathcal{H}(\mathcal{B})_i &\to \mathbb{C}, \\ \rho_i &\mapsto f(\rho_i \otimes I_j) \end{aligned}$$

einen Zustand von $\mathcal{H}(\mathcal{B})_i$ (und in analoger Weise einen Zustand von $\mathcal{H}(\mathcal{B})_j$). Wegen $f(\rho) = \mathrm{tr}(\tau\rho)$ für ein $\tau \in \mathcal{H}(\mathcal{B})_i \otimes \mathcal{H}(\mathcal{B})_j$ nach Gleichung 3.28 erhält man hieraus die Formel für den reduzierten Dichteoperator aus Gleichung 3.21.

Was aber, wenn wir unendlich viele endlich-dimensionale Hilberträume $\mathcal{H}_1, \mathcal{H}_2, \ldots$ tensorieren? Sei wieder zu jedem Hilbertraum $\mathcal{H}_i$ die zugehörige Operatoralgebra durch $\mathcal{B}(\mathcal{H})_i$ gegeben. Wie oben betten wir ein, und zwar

$$\begin{aligned} \mathcal{B}(\mathcal{H})_1 \text{ in } \mathcal{B}(\mathcal{H})_1 \otimes \mathcal{B}(\mathcal{H})_2, \\ \mathcal{B}(\mathcal{H})_1 \otimes \mathcal{B}(\mathcal{H})_2 \text{ in } \mathcal{B}(\mathcal{H})_1 \otimes \mathcal{B}(\mathcal{H})_2 \otimes \mathcal{B}(\mathcal{H})_3, \end{aligned}$$

allgemein

$$\bigotimes_{i=1}^{k} \mathcal{B}(\mathcal{H})_i \text{ in } \bigotimes_{i=1}^{k+1} \mathcal{B}(\mathcal{H})_i.$$

Mit $\mathcal{A}_l = \otimes_{i=1}^{l} \mathcal{B}(\mathcal{H})_l$ ist dann $\mathcal{A}_1 \subset \mathcal{A}_2 \subset \ldots$ ein sogenannter *Turm* von C*-Algebren. Sei $\mathcal{A}_\infty$ die Vereinigung aller $\mathcal{A}_l$; sie besitzt die Struktur einer prä-C*-Algebra, das heißt, sie erfüllt die Definition bis auf die Abgeschlossenheit. Ihre Vervollständigung ist eine C*-Algebra.

C*-Algebren, die in dieser Weise entstehen, heißen *beinahe endlich-dimensional* oder kurz AF-Algebren (für approximately finite dimensional). Wir bezeichnen die C*-Algebra, die wir hier erhalten haben, als die *quasilokale Algebra* . $\mathcal{A}_\infty$ wird manchmal auch *lokale Algebra* genannt.

Wir werden die quasilokale Algebra im folgenden Kapitel einsetzen, um globale Konfigurationen von Quantenzellularautomaten zu definieren.

3.7 Verschränkung

Nach der Einführung in die Grundlagen des Quantenrechnens gehen wir auf zwei speziellere Gebiete ein, die wir im folgenden Kapitel benötigen. Dies

sind Verschränkung und, im nächsten Abschnitt, Maße für die Ähnlichkeit von Quantenzuständen.

Sind A und B voneinander isolierte Quantensysteme, jedes für sich in einem reinen Zustand φ_A beziehungsweise φ_B, so beschreibt das Tensorprodukt $\varphi_A \otimes \varphi_B$ ihren gemeinsamen Zustand. Haben A und B aber erst einmal interagiert, so kann man ihren gemeinsamen Zustand oft nicht mehr als Tensorprodukt der Teilzustände schreiben.

Als Beispiel seien A und B Systeme aus jeweils einem qubit. Zu Beginn sei $\varphi_A = \alpha_0|0\rangle_A + \alpha_1|1\rangle_A$ und $\varphi_B = \beta_0|0\rangle_B + \beta_1|1\rangle_B$; das Tensorprodukt ist dann $\alpha_0\beta_0|0\rangle_A|0\rangle_B + \alpha_0\beta_1|0\rangle_A|1\rangle_B + \alpha_1\beta_0|1\rangle_A|0\rangle_B + \alpha_1\beta_1|1\rangle_A|1\rangle_B$. Wenden wir hierauf die aus Gleichung 3.11 bekannte Operation `CNOT` an, so erhalten wir

$$\alpha_0\beta_0|0\rangle_A|0\rangle_B + \alpha_0\beta_1|0\rangle_A|1\rangle_B + \alpha_1\beta_1|1\rangle_A|0\rangle_B + \alpha_1\beta_0|1\rangle_A|1\rangle_B \tag{3.29}$$

als neuen Zustand des Gesamtsystems.

Im Gegensatz zum ursprünglichen Zustand läßt sich der neue auch nach Basiswechsel nicht als Tensorprodukt schreiben. Es ist aber möglich, ihn in eine Summe von Tensorprodukten zu überführen. Die minimale Anzahl Summanden in dieser Summendarstellung ist eine Invariante des Zustandes und heißt *Schmidt-Zahl*. Zustände, die man nicht als Tensorprodukte schreiben kann, heißen *verschränkt*. Die Schmidt-Zahl dient als Maß ihrer Verschränktheit: Unverschränkte (*separable*) Zustände sind gerade solche mit Schmidt-Zahl 1 und ein Zustand gilt als um so stärker verschränkt, je höher seine Schmidt-Zahl ist.

Dies ist notwendigerweise eine vereinfachte Darstellung; Verschränkung besitzt viele Facetten, die wir hier übergehen müssen.

Seien A und B Quantensysteme der gleichen Dimension mit den Orthonormalbasen $|\varphi_i\rangle$ beziehungsweise $|\psi_j\rangle$. Dann können wir jeden Quantenzustand wie in Gleichung 3.29 ausmultipliziert schreiben:

$$|\xi\rangle = \sum_{ij} \alpha_{ij}|\varphi_i\rangle|\psi_j\rangle.$$

Wir wechseln Basen und ersetzen $|\psi_j\rangle$ durch $|\widetilde{\psi}_j\rangle = \sum_i \alpha_{ij}|\varphi_i\rangle$. Weiter nehmen wir an, die Basis von A wäre so gewählt, dass die Dichtematrix des

Zustandes von A Diagonalgestalt hat; dies ist keine Beschränkung der Allgemeinheit. Diese Dichtematrix ρ_A hat die Form $\sum_i p_i|\varphi_i\rangle\langle\varphi_i|$.

Wir erhalten ρ_A auch dadurch, dass wir den Zustand von B aus dem gemeinsamen Zustand ausspuren; daher gilt $p_i = \langle\widetilde{\psi_i}|\widetilde{\psi_i}\rangle$ für alle i. Zwecks Normalisierung setzen wir $|\psi_j\rangle' = p_j^{-1/2}|\widetilde{\psi_j}\rangle$ und erhalten

$$\sum_i \sqrt{p_i}|\varphi_i\rangle_A|\psi_i\rangle'_B$$

als Summendarstellung des Gesamtzustandes bezüglich der zu Beginn festgelegten Orthonormalbasen. Bezüglich anderer Basen erhalten wir andere Summen, aber die Anzahl von Null verschiedener Summanden bleibt gleich; sie ist die bereits erwähnte Schmidt-Zahl. Vertauschen wir die Rollen von A und B so ändern sich noch nicht einmal die p_i, also die Eigenwerte der reduzierten Dichtematrizen.

Im Beispiel erhalten wir mit $\widetilde{|0\rangle}_B = \alpha_0\beta_0|0\rangle_B + \alpha_0\beta_1|1\rangle_B$, $\widetilde{|1\rangle}_B = \alpha_1\beta_1|0\rangle_B + \alpha_1\beta_0|1\rangle_B$

$$|0\rangle_A(\alpha_0\beta_0|0\rangle_B + \alpha_0\beta_1|1\rangle_B) + |1\rangle_A(\alpha_1\beta_1|0\rangle_B + \alpha_1\beta_0|1\rangle_B),$$

also eine Schmidt-Zahl von 2 für den Zustand aus Gleichung 3.29. Dagegen läßt sich der Ausgangszustand als

$$(\alpha_0|0\rangle_A + \alpha_1|1\rangle_A) \otimes (\beta_0|0\rangle_B + \beta_1|1\rangle_B)$$

mit nur einem Summanden schreiben und hat die Schmidt-Zahl 1.

Die Schmidt-Zahl ist als Verschränkungsmaß nur auf bipartite Systeme anwendbar. Schon für Systeme aus drei qubits existieren zwei verschiedene nicht äquivalente (das heißt, nicht durch lokale Operationen ineinander überführbare) maximal verschränkte Quantenzustände [24, 87].

3.8 Abstandsmaße für Quantenzustände

Es gibt verschiedene Möglichkeiten, die Ähnlichkeit von zwei Quantenzuständen zu definieren. Wir gehen hier auf zwei gebräuchliche ein, nämlich den *Spurabstand* (trace distance) D und die *Treue* (fidelity) F [32, 66, 91].

Seien ρ und σ zwei Dichteoperatoren. Ihr Spurabstand ist

$$D(\rho, \sigma) = \frac{1}{2} \cdot \mathrm{tr}(|\rho - \sigma|), \tag{3.30}$$

wobei $|A|$ für Matrizen A durch $\sqrt{AA^\dagger}$ definiert ist.

Ist $\{E_m\}$ ein beliebiges POVM, so sind $p_m = \mathrm{tr}(\rho E_m)$ und $q_m = \mathrm{tr}(\sigma E_m)$ die Wahrscheinlichkeiten, bei einer Messung von ρ beziehungsweise σ das Ergebnis m zu erhalten; das POVM liefert eine Wahrscheinlichkeitsverteilung über die möglichen Ergebnisse. Sei p die Wahrscheinlichkeitsverteilung für ρ und q die für σ. Auf Wahrscheinlichkeitsverteilungen kann man mittels

$$D(p, q) = \frac{1}{2} \sum_m |p_m - q_m|$$

ein zum Spurabstand analoges Abstandsmaß einführen. Es gilt:

$$D(\rho, \sigma) = \max_{\{E_m\}} D(p, q).$$

Daraus folgt: Wenn zwei Dichteoperatoren kleinen Spurabstand haben, wird jede Messung zu Wahrscheinlichkeitsverteilungen führen, die auch kleinen Spurabstand haben.

Falls ρ und σ Zustände eines bipartiten Systems mit den Teilen A und B sind, wird durch Ausspuren eines der beiden Systeme der Spurabstand nicht größer:

$$D(\mathrm{tr}_B(\rho), \mathrm{tr}_B(\sigma)) \leq D(\rho, \sigma).$$

Insbesondere ist $D((\rho \otimes \tau), (\sigma \otimes \tau)) = D(\rho, \sigma)$.

D ist sowohl auf Dichteoperatoren als auch auf Wahrscheinlichkeitsverteilungen eine Metrik. Darüber hinaus ist D konvex: Für gemischte Zustände $\sum_i p_i \rho_i$ und $\sum_i q_i \tau_i$ gilt

$$D\left(\sum_i p_i \rho_i, \sum_i q_i \tau_i\right) \leq D(p_i, q_i) + \sum_i p_i D(\rho_i, \tau_i). \tag{3.31}$$

Ein anderes Abstandsmaß ist die Treue

$$F(\rho, \sigma) = \mathrm{Tr}\left(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right). \tag{3.32}$$

Zwischen D und F besteht der Zusammenhang

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}.$$

Sowohl D als auch F bleiben unter unitären Transformationen erhalten.

3.9 Zusammenfassung

Quantenrechner funktionieren in verschiedener Hinsicht anders als klassische Computer: Ihre Zustände können in Überlagerung vorliegen, Rechnung erfolgt unitär (insbesondere reversibel) und Beobachtung (Messung) hat stochastische Ergebnisse.

Neben der klassischen Schreibweise als Vektoren in Hilberträumen oder als Dichtematrizen verfügen wir mit der Observablenalgebra über ein weiteres mächtiges Instrument zur Beschreibung von Quantenzuständen.

KAPITEL 4

Quantenzellularautomaten

4.1 Einleitung

Als Quantenzellularautomaten (QZA) bezeichnet man Varianten von Zellularautomaten, die sich nicht wie klassische, sondern wie Quantensysteme verhalten. Üblicherweise fasst man die Menge der globalen Konfigurationen als einen Hilbertraum auf, in dem die deterministischen globalen Konfigurationen die kanonische Basis bilden. Die globale Überführungsfunktion des QZA übernimmt die Rolle des Entwicklungsoperators auf diesem Hilbertraum.

Neben ihrer theoretischen Bedeutung als Quanten-Äquivalent der klassischen ZA sind QZA auch von praktischem Interesse. Hier ist zum Einen die Modellierung von Quantensystemen zu nennen. QZA sind in naheliegender Weise verwandt mit Quanten-Spin-Systemen, einem der grundlegenden physikalischen Modelle [22, 49, 65]. Darüber hinaus sind QZA schon zur Simulation sogenannter Quanten-Gitter-Gase (Quantum Lattice Gases) eingesetzt worden [58, 88, 90, 89].

Zweitens gibt es Vorschläge für Architekturen möglicher Quantenrechner, die Eigenschaften von QZA wie Lokalität und Uniformität aufweisen; insbesondere haben diese Architekturen Ähnlichkeiten mit Spin-Systemen. Beispiele hierfür sind auf NMR (Nuklear-magnetischer Resonanz) basierende Architekturen [46, 47], der siliziumbasierte Quantenrechner nach Ka-

ne [42] oder Quanten-Punkt-Zellularautomaten [69, 78]. Als theoretische Modelle, die die Fähigkeiten dieser Architekturen erkennen und beschreiben lassen, bieten sich QZA an.

Schließlich deuten neuere Ergebnisse darauf hin, dass Quanten-Irrfahrten, die sich leicht mit QZA implementieren lassen, sich in interessanter Weise von ihren klassischen Gegenstücken unterscheiden [1, 2, 13, 64]. Wegen der Rolle von Irrfahrten bei der Entwicklung und Analyse klassischer Algorithmen (zum Beispiel der probabilistische k-SAT-Algorithmus von Schöning [75] oder die Monte-Carlo-Methode) eröffnet sich die Möglichkeit QZA-basierter Quantenalgorithmen.

Alle diese Anwendungen erfordern eine brauchbare Definition von Quantenzellularautomaten; es ist nicht sinnvoll, dass jedes Mal eine Definition des Rechenmodells inklusive der benötigten Werkzeuge ad hoc entwickelt wird. Eine brauchbare Definition sollte mindestens folgende Eigenschaften haben:

1. Es muss leicht entscheidbar sein, ob eine gegebene lokale Überführungsfunktion zu einem zulässigen QZA gehört.

2. Das Modell muss in der Lage sein, universelle Turingmaschinen effizient zu simulieren.

3. Es muss möglich sein, lokale Konfigurationen als Teile von globalen Konfigurationen aufzufassen und die lokale Überführungsfunktion auf ihnen zu definieren.

Diese Eigenschaften sollen sicherstellen, dass das Modell handhabbar und universell ist.

Es gibt eine Reihe von Definitionen von QZA, die wir in Abschnitt 4.2 vorstellen. Keine von ihnen erfüllt die dritte Forderung; wir entwickeln daher eine weitere. Im Unterschied zu den bisherigen Definitionen, die durchgängig den Hilbertraumformalismus verwenden, stützen wir uns dabei auf einen operatoralgebraischen Ansatz und definieren QZA als eine spezielle Teilklasse von Automorphismen unendlicher Quanten-Konfigurationen.

Dadurch erhalten wir ein Modell, das die bisher bekannten simulieren kann und dabei insofern eine echte Erweiterung darstellt, als es die Loka-

litätsforderung 3. von oben erfüllt. Darüber hinaus ist unser Modell das erste, das sich auch auf unendliche Konfigurationen übertragen lässt.

Wie in Kapitel 2 sind wir auch hier wieder an Metriken interessiert. Mit einem ähnlichen Ansatz wie für die stochastischen Konfigurationen in Abschnitt 2.5 erhalten wir auf den globalen Konfigurationen von QZA nur eine Pseudometrik. Außerdem ist jener Ansatz auch für QZA auf endliche Konfigurationen beschränkt. Die Lokalitätseigenschaft unseres Modells ermöglicht eine einfachere Abstandsfunktion, die für unsere Zwecke eine brauchbare Metrik darstellt.

Schließlich stellen wir einige Betrachtungen zum Zusammenhang zwischen lokalen und globalen Konfigurationen an; dieser ist bei QZA im Gegensatz zu klassischen ZA (und ähnlich wie bei stochastischen ZA) nicht trivial, weil die lokalen Konfigurationen die Verschränkung von Zellen nur begrenzt wiedergeben können. Wir gewinnen aus der Entwicklung dieser Verschränkung ein Komplexitätsmaß für QZA.

4.2 Definitionen

4.2.1 Einleitung

Definieren kann man QZA ähnlich wie SZA, mittels lokaler Überführungsfunktionen, deren Wertebereich im Hilbertraum $\ell_2(\mathrm{Q})$ über der Zustandsmenge Q liegt; die Zulässigkeit einer lokalen Überführungsfunktion nachzuweisen ist jedoch schwierig, denn dafür ist zu zeigen, dass die globale Überführungsfunktion unitär ist.

Dieses Problem ist auf unterschiedliche Weise gelöst worden; das erste Modell wurde von Grössing und Zeilinger [33] vorgeschlagen und von Meyer aufgegriffen [55, 56, 57]. Dürr, LêThanh und Santha haben QZA auf endlichen Konfigurationen definiert [28, 29] und Polynomialzeit-Algorithmen angegeben, die entscheiden, ob eine lokale Überführungsfunktion zulässig ist. Watrous hat seine Definition auf partitionierten ZA aufgebaut [85] und so die Zulässigkeitsprüfung vereinfacht, ohne allerdings die Beschränkung auf endliche Konfigurationen aufzugeben. Schließlich hat van Dam ein lokales Kriterium für die Zulässigkeit nicht-partitionierter QZA gefunden.

Die folgenden Abschnitte geben einen Überblick über diese Definitionsvarianten.

4.2.2 Irrfahrten von endlich vielen Teilchen

Die erste Definition von QZA, wie sie von Grössing und Zeilinger gegeben wurde [33], betrachtet Teilchen auf einem regelmäßigen Gitter. Jeder Gitterpunkt entspricht einer Zelle und besitzt zwei Basiszustände, die die An- beziehungsweise Abwesenheit eines Teilchens symbolisieren.

Sei L die Menge aller Gitterpunkte, also aller möglichen Aufenthaltsorte. Falls sich in dem Gitter nur ein Teilchen befindet, bilden die Vektoren $|x\rangle$ für $x \in L$ eine Orthonormalbasis eines Hilbertraumes; dieser Raum ist der Raum der globalen Konfigurationen. Für eine endliche Zahl k von Teilchen erhält man eine Orthonormalbasis, die zu jeder k-elementigen Teilmenge von L einen Basisvektor enthält.

Die globale Überführungsfunktion eines QZA ist auf diesem Raum durch eine unitäre Matrix repräsentiert; damit Lokalität und Homogenität erfüllt sind, muss die Matrix band-diagonal sein und mit der Verschiebung kommutieren.

Meyer hat gezeigt [55], dass man im einfachsten Fall einer Nachbarschaft der Größe drei hier nur triviale QZA erhält. Eine Erweiterung auf partitionierte ZA mit mehr als zwei Zuständen pro Zelle erlaubt auch nichttriviale QZA [56, 57, 58].

Dieses Modell erlegt sich selbst durch die Interpretation der globalen Zustände als Kodierung der Aufenthaltsorte von konstant vielen Teilchen starke Beschränkungen auf. Es ist dennoch von Bedeutung, weil es einigermaßen überschaubar ist und eine Analyse zum Beispiel mit Quanten-Markovketten zulässt; die oben bereits zitierten Arbeiten über Quanten-Irrfahrten [1, 2, 13, 64] nutzen dies aus.

4.2.3 QZA auf endlichen Konfigurationen

Neuere Definitionen von QZA beschränken sich nicht darauf, die Bewegungen einer endlichen Zahl von Teilchen auf einem Gitter zu modellieren.

Statt dessen betrachten sie jede Zelle als ein Quantensystem mit einer endlichen Menge Q von Basiszuständen und beschreiben mittels der Überführungsfunktion die Interaktion der Zellen mit ihren Nachbarn. Die folgenden Modelle unterscheiden sich vor allem in der Angabe der lokalen Überführungsfunktion und den Wohlgeformtheitsbedingungen.

Im Folgenden steht Q immer für eine endliche Menge von Zuständen und $\ell_2(Q)$ für den ℓ_2-Hilbertraum über Q. Der Quantenzustand einer Zelle ist ein Vektor der Länge 1 aus $\ell_2(Q)$; die i-te Komponente des Vektors steht für die Amplitude des i-ten Zustands von Q.

Definition 4.1 (QZA erster Art)
Ein QZA ist ein 3-Tupel (Q, N, φ). Q *ist eine endliche Menge von Zuständen,* N *die Nachbarschaftsgröße und* $\varphi : Q^N \to \ell_2(Q)$ *eine lokale Überführungsfunktion, für die gilt: für jedes* $w \in Q^N$ *existiert mindestens ein* $q \in Q$, *für das* $\langle \varphi(w)|q\rangle \neq 0$ *ist.*

Damit φ als lokale Überführungsfunktion eines QZA gelten kann, muss sie eine zulässige globale Überführungsfunktion induzieren, das heißt global Quantenzustände auf Quantenzustände abbilden. Um dies zu entscheiden, müssen wir zuerst definieren, was wir unter globalen Quantenzuständen, also globalen Quantenkonfigurationen, verstehen.

Reihen wir k gleichartige Zellen nebeneinander auf, so erhalten wir für endliche k den Zustand des Gesamtsystems als einen normierten Vektor im Tensorprodukt der einzelnen Hilberträume. Den subtileren Fall unendlicher k behandeln die herkömmlichen Definitionen nicht allgemein. Sie behelfen sich folgendermaßen:

Es bezeichne $Q^{\mathbb{Z}}$ die Menge aller klassischen globalen Konfigurationen über der Zustandsmenge Q. Wir setzen voraus, dass Q einen Zustand q_s enthält, der bezüglich des betrachteten QZA *still* ist. Wie bei klassischen ZA bedeutet dies, dass $\varphi(q_s^N) = q_s$ sein muss. Wir bezeichnen $c \in Q^{\mathbb{Z}}$ als *endlich*, wenn $c_i = q_s$ für alle bis auf endlich viele $i \in \mathbb{Z}$ gilt und schreiben $Q_E^{\mathbb{Z}}$ für die Menge der endlichen klassischen globalen Konfigurationen über Q.

Wir fassen $Q_E^{\mathbb{Z}}$ als eine Orthonormalbasis des Raumes der zulässigen globalen Quantenkonfigurationen auf; demnach sind alle globalen Quanten-

konfigurationen von der Form $\sum_{i=1}^{n} \alpha_i |c_i\rangle$ mit $n \in \mathbb{N}$, $\alpha_i \in \mathbb{C}$, $\sum_{i=1}^{n} |\alpha_i|^2 = 1$ und $c_i \in Q_E^{\mathbb{Z}}$.

Die lokale Überführungsfunktion φ induziert eine globale Funktion $\Phi : Q_E^{\mathbb{Z}} \times Q_E^{\mathbb{Z}} \to \mathbb{C}$. Diese schreiben wir als Matrix, in der der Eintrag $\Phi[i,j]$ die Amplitude angibt, mit der in einem Schritt ein Wechsel von der Konfiguration c_j in die Konfiguration c_i erfolgt. Diese Amplitude erhalten wir aus φ gemäß

$$\Phi[i,j] = \prod_{k \in \mathbb{Z}} \langle \varphi(c_i(k-r), \ldots, c_i(k+r)) | c_j(k) \rangle. \tag{4.1}$$

An dieser Stelle ist die Endlichkeit von c_i und c_j wichtig, denn sie garantiert die Existenz des Produktes. Wenden wir Φ auf die Konfiguration c_j an, so erhalten wir die Überlagerung von Konfigurationen

$$\Phi(c_j) = \sum_{n \in \mathbb{Z}} \Phi[n,j] |c_n\rangle. \tag{4.2}$$

Dank Linearität gilt für Überlagerungen

$$\Phi\left(\sum_{n \in \mathbb{Z}} \xi_n |c_n\rangle\right) = \sum_{n \in \mathbb{Z}} \xi_n |\Phi(c_n)\rangle. \tag{4.3}$$

Bis hierher stimmt die Herleitung gut mit der von stochastischen globalen Konfigurationen und Überführungsfunktionen überein. Wir können schließen, dass es ausreicht, die Anwendung der globalen Überführungsfunktion auf der kanonischen Basis des Raumes der globalen Quantenkonfigurationen, also auf den klassischen (deterministischen) globalen Konfigurationen, zu definieren.

Dürr et al. bezeichnen einen QZA als *wohlgeformt*, wenn Φ die Norm der Eingabevektoren erhält. Dies ist genau dann der Fall, wenn die Spaltenvektoren der Matrix Φ orthonormal sind. In vielen Zusammenhängen ist diese Eigenschaft schon hinreichend für die Unitarität von Φ; für QZA gilt dies nicht.

Endlichdimensionale Matrizen A sind genau dann unitär, wenn die Spalten- oder Zeilenvektoren von A orthonormal sind. Bei Φ handelt es sich jedoch um eine unendlichdimensionale Matrix. Jeder Spaltenvektor hat

endlichen Träger, was die Prüfung auf Orthonormalität erleichtert; der i-te Spaltenvektor repräsentiert das Bild der klassischen Konfiguration c_i unter Φ. Der i-te Zeilenvektor aber gibt an, welche Konfigurationen c_j sich mit einer von Null verschiedenen Amplitude zur Konfiguration c_i entwickeln (er repräsentiert also das Urbild von c_i unter Φ) und hat daher nicht unbedingt endlichen Träger. Insbesondere ist daher in diesem Fall die Orthonormalität der Spaltenvektoren nicht hinreichend für die Unitarität von Φ.

Dürr et al. haben gezeigt, dass man Wohlgeformtheit in $O(n^2)$ und Unitarität in $O(n^3)$ entscheiden kann, wobei n für die Länge der Beschreibung des ZA steht, also $|Q|^{|N|}$ entspricht [28, 29]. Eine ähnliche Definition gibt D. Meyer [57]; er erlaubt allerdings auch unendliche Konfigurationen unter der Bedingung, dass der QZA sich ausserhalb eines endlichen Bereiches deterministisch verhalten muss.

Der Nachteil an dieser Definition ist neben der Beschränkung auf endliche Konfigurationen, dass es kein lokales Kriterium für die Wohlgeformtheit gibt. Darüber hinaus gibt es unitäre QZA erster Art, deren Inverse kein QZA ist. Dies ist eine Folge davon, dass Dürr et al. ihren Unitaritätsbegriff auf endlichen Konfigurationen aufbauen. Wie bei klassischen reversiblen ZA erhält man einen anderen Unitaritätsbegriff, wenn man von unendlichen Konfigurationen ausgeht.

Der Ansatz von Watrous [85] tut dies implizit, indem er partitionierte ZA verwendet. Er kann damit Unitarität lokal entscheiden und seine QZA sind gegenüber Inversenbildung abgeschlossen. Aus technischen Gründen kann er jedoch die Anwendung von QZA auf unendliche Konfigurationen nicht behandeln.

4.2.4 Partitionierte QZA

Partitionierte QZA (PQZA) sind ähnlich wie klassische PZA definiert.

Definition 4.2 (PQZA)
Ein PQZA ist ein 3-Tupel (Q, N, φ). Q *hat die Gestalt* $(Q_1 \times Q_2 \times \ldots \times Q_N)$ *mit endlichen Teilalphabeten* Q_i. N *ist die Nachbarschaftsgröße und* $\varphi : Q \to \ell_2(Q)$ *die lokale Überführungsfunktion.*

Die lokale Überführungsfunktion schreiben wir als komplexe $|Q| \times |Q|$-Matrix und nennen φ unitär, wenn diese Matrix unitär ist. Ähnlich wie für PZA die lokale Reversibilität die globale bereits impliziert, gilt für PQZA:

Lemma 4.1 (Watrous)
φ ist genau dann die lokale Überführungsfunktion eines legalen PQZA, wenn φ unitär ist.

Damit existiert für PQZA ein lokales Zulässigkeitskriterium. Allerdings ist auch die Definition von Watrous auf endliche Konfigurationen eingeschränkt, denn wie Dürr et al. definiert er die globale Überführungsfunktionen nur auf der kanonischen Basis der endlichen globalen Quantenkonfigurationen. Daher muss er wie in Gleichung 4.1 vor jeder Anwendung der globalen Überführungsfunktion die Amplituden für globale Basiskonfigurationen ausmultiplizieren. Auf unendlichen Konfigurationen ist die Existenz des Produktes nicht garantiert.

Welche Auswirkung hat die Beschränkung auf partitionierte Zellularautomaten? Hinsichtlich der Berechnungsmächtigkeit keine – wie schon in Abschnitt 1.3.2 erwähnt, können PZA allgemeine ZA ohne Zeitverlust simulieren. Dafür wächst die Zustandszahl schlimmstenfalls von $|Q|$ auf $|Q|^N$, was die Analyse erschwert.

Weil es universelle reversible PZA gibt und diese legale PQZA sind, gibt es PQZA, die beliebige ZA simulieren können (allerdings unter Umständen mit Zeitverlust). Insbesondere können PQZA klassische Turingmaschinen simulieren; in der Tat können sie mit der gleichen Technik auch Quantenturingmaschinen simulieren.

Lemma 4.2 (Watrous [85], siehe auch [35])
Quantenturingmaschinen können QPZA mit quadratischem Zeitverlust simulieren. QPZA können Quantenturingmaschinen mit konstantem Zeitverlust simulieren.

4.2.5 QZA auf periodischen Konfigurationen

Eine allgemeinere Definition, für nichtpartitionierte QZA auf periodischen Konfigurationen, findet man in der Diplomarbeit von van Dam [83]. Wieder

hat jeder eindimensionale QZA eine endliche Zustandsmenge Q, eine Nachbarschaftsgröße N und eine lokale Überführungsfunktion $\varphi : Q^N \to \ell_2(Q)$. Daraus erhalten wir für $k \in \mathbb{N}$ eine Abbildung $\Phi_k : \ell_2(Q^k) \to \ell_2(Q^k)$ wie folgt. Sei $\mathbb{Z}_k$ der Restklassenring der ganzen Zahlen modulo k und $(\xi_n)_{1 \le n \le |Q|^k}$ eine Orthonormalbasis von $\ell_2(Q^k)$. Mit $\xi_n[i]$ bezeichnen wir für $1 \le i \le k$ die i-te Komponente des Vektors ξ_n. Auf den Basisvektoren definieren wir

$$\Phi_k|\xi_n\rangle = \bigotimes_{j \in \mathbb{Z}_k} \varphi(\xi_n[j], \ldots, \xi_n[j+N-1]) \tag{4.4}$$

und setzen Φ_k durch

$$\Phi_k \left(\sum_{n=1}^{|Q|^k} \alpha_n |\xi_n\rangle \right) = \sum_{n=1}^{|Q|^k} \alpha_n \Phi_k |\xi_n\rangle \tag{4.5}$$

auf ganz $\ell_2(Q^k)$ linear fort.

Für klassische ZA kann man ähnlich vorgehen: Ist der ZA auf periodische Konfigurationen eingeschränkt, so erhält man aus der lokalen Überführungsfunktion, angewandt auf eine mit Periode k periodische Konfiguration, eine Funktion $F_k : S^k \to S^k$. Ein ZA ist genau dann reversibel, wenn für alle k die Funktion F_k eine Bijektion ist. Eine entsprechende Aussage gilt auch hier und führt auf folgende Definition.

Definition 4.3 (QZA zweiter Art)
Ein QZA (Q, N, φ) heißt (wohlgeformter) QZA zweiter Art, *wenn für alle $k \in \mathbb{N}$ die gemäß den Gleichungen 4.4 und 4.5 induzierte Abbildung Φ_k unitär ist.*

Anders als bei Dürr et al. haben wir es hier immer mit endlichdimensionalen Operatoren zu tun und brauchen Wohlgeformtheit nicht von Unitarität zu unterscheiden.

Lemma 4.3 (van Dam [83])
Ein QZA zweiter Art ist genau dann wohlgeformt, wenn für die Funktion $\Phi_{\mathbb{Z}} : Q^{\mathbb{Z}} \to \ell_2(Q^{\mathbb{Z}})$ mit

$$\Phi_{\mathbb{Z}}(c) = \bigotimes_{i \in \mathbb{Z}} \varphi(c_{i-(N-1)/2}, \ldots, c_{i+(N-1)/2}) \tag{4.6}$$

für $c \in Q^{\mathbb{Z}}$ *(*N *ist ohne Einschränkung als ungerade angenommen) gilt: aus* $c \neq d \in Q^{\mathbb{Z}}$ *folgt*

$$\langle \Phi_{\mathbb{Z}}(c)_i | \Phi_{\mathbb{Z}}(d)_i \rangle = 0 \tag{4.7}$$

für ein $i \in \mathbb{Z}$.

Dieses Lemma ist nicht ganz korrekt. Solange $\Phi_{\mathbb{Z}}$ nur auf endliche globale Konfigurationen angewandt wird, stimmt die Argumentation von van Dam zwar; auf periodischen Konfigurationen führt sie jedoch zu einem Widerspruch.

Sei zum Beispiel A der QZA $(\{0,1\}, 1, H)$, der als lokale Überführungsfunktion die Hadamard-Transformation benutzt. A erfüllt die Wohlgeformtheitsbedingung, denn seine lokale Überführungsfunktion ist eine unitäre Selbstabbildung des Zustandsraumes einer Zelle. Wenden wir A jedoch auf eine beliebige deterministische globale Konfiguration an, so erhalten wir als Ergebnis einen Zustand, der kein Vektor in $\ell_2(Q^{\mathbb{Z}})$ sein kann, weil jede seiner Komponenten die Form $\pm \prod_{i \in \mathbb{Z}} 2^{-1/2}$ hat und daher kein wohldefiniertes Objekt ist.

Wir werden in Abschnitt 4.4 ein Modell entwickeln, das diese Schwierigkeit vermeidet und auf beliebige, auch unendliche aperiodische, Konfigurationen anwendbar ist.

Wegen Lemma 4.3 gibt es für van Dams QZA ein lokales Kriterium, das sogar entscheidbar ist, denn er hat gezeigt, dass man die Unitarität von Φ_k nur für k zwischen Eins und $2|Q|^{2(N-2)}$ zu prüfen braucht. Jeder QZA zweiter Art ist auch ein wohlgeformter QZA erster Art; die Umkehrung gilt jedoch nicht. Außerdem sind QZA zweiter Art gegenüber Inversenbildung abgeschlossen.

4.2.6 Zusammenfassung

Die bekannten Definitionen von QZA zerfallen in drei Klassen: Erstens QZA in der Tradition von Grössing und Zeilinger, die sich darauf konzentrieren, die Bewegung von endlich vielen Teilchen in einem Gitter zu simulieren, zweitens das Modell von Dürr, LêThanh und Santha, das zulässige QZA

über die Unitarität der globalen Überführungsfunktion auf endlichen Konfigurationen definiert, drittens die QZA von Watrous und van Dam, bei denen die Überführungsfunktion schon lokal unitär sein muss.

Gemeinsam ist diesen Modellen, dass die Anwendung der Überführungsfunktion nur global vollständig beschreibbar ist. Selbst wenn man nur den nächsten Zustand einer einzelnen Zelle berechnen will, muss man zuvor die aktuelle globale Konfiguration kennen, weil es innerhalb dieser Modelle keinen hinreichenden Begriff vom Zustand einer endlichen lokalen Konfiguration gibt. Die lokale Überführungsfunktion wird hier nur auf reinen Zuständen definiert, lokale Konfigurationen können sich aber, da sie Teile globaler Konfigurationen sind, in gemischten Zuständen befinden. Diese Idee werden wir weiter verfolgen; zuvor aber beschäftigen wir uns kurz mit grundlegenden Eigenschaften von QZA.

4.3 Einige Eigenschaften von QZA

Wir beschäftigen uns mit den Beziehungen zwischen Reversibilität von deterministischen ZA und der Wohlgeformtheit von QZA. Für den Vergleich schreiben wir auch für deterministische ZA die globale Überführungsfunktion als Matrix; für deterministische ZA handelt es sich hierbei um 0-1-Matrizen, bei denen in jeder Spalte genau eine Eins steht.

Da QZA erster Art auf endliche Konfigurationen beschränkt sind, könnte man vermuten, jeder dort injektive ZA wäre ein QZA; dies ist aber nicht der Fall, denn Injektivität auf endlichen Konfigurationen impliziert zwar Surjektivität auf allen, aber nicht Surjektivität auf endlichen Konfigurationen. Ein Beispiel dafür ist wieder der ZA $A_{\mathrm{xor}} = (\{0,1\}, 2, \varphi)$ mit $\varphi(x,y) = x + y \bmod 2$. Er ist auf endlichen Konfigurationen injektiv, aber nicht bijektiv, da $\ldots 00100 \ldots$ kein endliches Urbild besitzt; folglich ist er auf endlichen Konfigurationen nicht unitär.

Lemma 4.4
Ein deterministischer ZA A ist genau dann ein QZA der ersten Art, wenn A eingeschränkt auf endliche Konfigurationen bijektiv ist.

Beweis: Sei $A = (S, N, \varphi)$ bijektiv auf endlichen Konfigurationen. Dürr,

LêThanh und Santha haben zwei Kriterien für die Wohlgeformtheit von A angegeben [28]. Erstens müssen die Spaltenvektoren des Entwicklungsoperators normiert sein; dies ist für deterministische ZA immer der Fall.

Das zweite Kriterium besagt, dass die Bilder verschiedener endlicher deterministischer globaler Konfigurationen zueinander orthogonal sein müssen. Im deterministischen Fall ist dies gleichbedeutend damit, dass verschiedene endliche Konfigurationen verschiedene Bilder haben; dies folgt aus der Injektivität von A.

Es bleibt die Unitarität nachzuweisen; statt den Algorithmus von Dürr et al. einzusetzen, prüfen wir direkt die Orthonormalität der Zeilenvektoren des Entwicklungsoperators. Der i-te Zeilenvektor ist gerade das Urbild der i-ten endlichen Konfiguration unter A. Da aber A bijektiv und deterministisch ist, müssen die Zeilenvektoren normiert und paarweise verschieden sein. Da damit jeder Zeilenvektor genau eine Eins enthält, folgt die Orthonormalität. Weil sowohl die Zeilen- als auch die Spaltenvektoren orthonormal sind, ist damit die Unitarität bewiesen.

Sei umgekehrt der Entwicklungsoperator von A wohlgeformt und unitär. Dann kann man an ihm zu jeder endlichen Konfiguration genau ein Urbild ablesen, folglich ist A bijektiv. □

Lemma 4.5
Ein deterministischer ZA ist genau dann ein QZA zweiter Art, wenn er reversibel ist.

Beweis: Sei A ein RZA. Nach Lemma 1.1 ist dies äquivalent dazu, dass A auf periodischen Konfigurationen injektiv ist. Entwickeln wir also aus $A = (S, N, \varphi)$ die Operatoren $\Phi_k : S^k \to S^k$ für $k \in \mathbb{N}$ als

$$\Phi_k(s_0, \ldots, s_{k-1}) = (\varphi(s_i, s_{i+1 \bmod k}, \ldots, s_{i+N \bmod k}))_{i \in \mathbb{Z}_k} . \qquad (4.8)$$

Jedes Φ_k ist eine Bijektion: Angenommen, Φ_l wäre nicht injektiv. Dann gäbe es $w, v \in S^l$ mit $\Phi_l(w) = \Phi_l(v)$. Daraus folgt für die globale Überführungsfunktion von A : $\Phi(\ldots www \ldots) = \Phi(\ldots vvv \ldots)$, also ist A nicht injektiv. Ist Φ_l nicht surjektiv, so ist Φ_l wegen der Endlichkeit von S^l auch nicht injektiv.

Für die Darstellung von Φ_k als $|S|^k$-dimensionale quadratische Matrix P gilt:

$$P[i,j] = \begin{cases} 1 & \Phi_k(w_j) = w_i \\ 0 & \text{sonst} \end{cases} . \tag{4.9}$$

Dabei stehen w_i und w_j für das i-te beziehungsweise j-te Element einer Aufzählung der Wörter in S^k. P besitzt daher in jeder Zeile und jeder Spalte genau eine Eins und ist somit unitär.

Ist umgekehrt A ein deterministischer QZA zweiter Art, so ist P eine Permutationsmatrix und folglich A bijektiv auf periodischen und damit nach Lemma 1.1 auf allen Konfigurationen. □

Wie man sieht, handelt es sich bei QZA erster und zweiter Art um verschiedene Modelle; es gibt QZA erster Art, die nicht gleichzeitig QZA zweiter Art sind. Zwischen QZA der zweiten Art und PQZA besteht jedoch ein enger Zusammenhang:

Lemma 4.6
QZA der zweiten Art können PQZA ohne Zeitverlust simulieren.

Beweis: Die Idee kann man nahezu unverändert vom klassischen Fall übernehmen. □

Auf der Grundlage von Durand-Loses Linearzeitsimulation reversibler ZA mit reversiblen PZA [26] kann man vermuten, dass PQZA in der Lage sind, QZA der zweiten Art mit linearem Zeitverlust zu simulieren.

QZA zweiter Art stellen strengere Anforderungen an die lokale Überführungsfunktion als QZA erster Art. Letztere haben aber einige Nachteile; zulässige QZA erster Art sind viel schwieriger zu erkennen als wohlgeformte PQZA und außerdem sind sie nicht gegenüber Inversenbildung abgeschlossen. Wir konzentrieren uns daher auf QZA zweiter Art und nennen noch einige ihrer Eigenschaften.

Wir bezeichnen den QZA $T = (Q, 3, (x, y, z) \mapsto x)$ als *Verschiebung*. Es ist leicht nachzuprüfen, dass T ein wohlgeformter QZA zweiter Art ist.

Lemma 4.7
QZA zweiter Art kommutieren mit der Verschiebung.

Beweis: Sei $A = (Q, N, \varphi)$ (N ungerade) ein QZA zweiter Art. Es ist zu zeigen, dass für alle Konfigurationen $c \in Q_E^{\mathbb{Z}}$ gilt: $A(T(c)) = T(A(c))$. Sei dazu $i \in \mathbb{Z}$ der Index einer beliebigen Zelle. Es gilt $T(c)_i = c_{i-1}$ und $A(T(c))_i = \varphi(c_{i-1-(N-1)/2}, \ldots, c_{i-1+(N-1)/2} = A(c)_{i-1} = T(A(c))_i$. □

Wie deterministische RZA haben auch QZA eine Eigenschaft, die man als Balanciertheit bezeichnen kann.

Lemma 4.8
Für alle QZA (Q, N, φ) *gilt: Die Dimension des Urbildes jedes endlichen Blockes ist* $|Q|^N$.

Beweis: Sei zunächst $N = 2$, also φ eine Abbildung $Q^2 \to \ell_2(Q)$. Gemäß der Konstruktion von van Dam induziert φ mittels $|ab\rangle \mapsto |\varphi(ab)\rangle|\varphi(ba)\rangle$ einen Automorphismus von $\ell_2(Q^2)$. Da die globale Überführungsfunktion Φ unitär ist, ist auch dieser Automorphismus unitär und bildet Orthonormalbasen von $\ell_2(Q^2)$ auf Orthonormalbasen von $\ell_2(Q^2)$ ab. Folglich ist $\varphi^{-1}(xy)$ das eindeutig bestimmte $|ab\rangle$ mit $\varphi(ab) = |xy\rangle$. Wir erhalten damit

$$\varphi^{-1}(x) = \bigcup_{y \in \ell_2(Q)} \{\varphi^{-1}(xy)\}, \tag{4.10}$$

folglich ist $|\varphi^{-1}(x)| = |\ell_2(Q)| = |Q|$. Für die Verallgemeinerung auf beliebige N wählen wir die y in Gleichung 4.10 aus $\ell_2(Q^{N-1})$ und erhalten $|\varphi^{-1}(x)| = |Q|^{N-1}$. Es bleibt noch zu zeigen, dass $\varphi^{-1}(a)$ und $\varphi^{-1}(b)$ linear unabhängig sind, wenn a und b linear unabhängig sind.

$$\begin{aligned} y \perp y' &\Rightarrow x \otimes y \perp x \otimes y' \\ &\Rightarrow \varphi(xy) \perp \varphi(xy') \text{ und } \varphi^{-1}(xy) \perp \varphi^{-1}(xy'). \end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Van Dam hat für sein Modell eine ähnliche Eigenschaft nachgewiesen, die er ebenfalls als Balanciertheit bezeichnet: Er fordert $\sum_{x \in Q^N} |\langle y|\varphi(x)\rangle|^2 = |Q|^{N-1}$ für alle $y \in \ell_2(Q)$.

Schließlich erwähnen wir noch, dass QZA wie ihre klassischen Gegenstücke unter endlicher Hintereinanderausführung abgeschlossen sind. Sind

nämlich Φ und Ψ globale Überführungsfunktionen von QZA, so ist auch $\Phi \circ \Psi$ unitär und gehört damit zu einem QZA, denn die unitären Operatoren bilden eine Gruppe. Als Spezialfall erhält man daraus, dass man QZA durch Drehungen in QZA überführen kann.

Lemma 4.9
Sei φ die lokale Überführungsfunktion eines QZA mit der Zustandsmenge Q. Dann ist für beliebige unitäre Operatoren U auf dem Hilbertraum $\ell_2(Q)$ auch $U \circ \varphi$ ein QZA.

Beweis: Wir können U als lokale Überführungsfunktion eines QZA mit Nachbarschaftsgröße Eins auffassen; die Unitarität der globalen Überführungsfunktion folgt sofort, da keine Interaktion zwischen den Zellen stattfindet. Das Lemma folgt dann aus der Abgeschlossenheit unter Hintereinanderausführung. □

Dank Lemma 4.5 kann man für φ insbesondere die lokale Überführungsfunktion eines deterministischen RZA einsetzen. Nehmen wir als Beispiel $A = (Q, 2, \varphi)$ mit $\varphi(x, y) = x$ und verwenden für U die Hadamard-Transformation aus Gleichung 3.9, so gilt $(U \circ \varphi)(0, x) = 1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle$ und $(U \circ \varphi)(1, x) = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$. Interessanter wird es, wenn wir Q und N so groß wählen, dass nichttriviale RZA möglich sind (siehe auch Kapitel 1).

Bei klassischen ZA kann man mehrere Überführungsfunktionen nicht nur nacheinander, sondern auch parallel anwenden und erhält damit aus RZA weitere RZA. Das geht auch bei QZA.

Lemma 4.10
Sind $A = (Q_1, N, \varphi)$ und $B = (Q_2, N, \psi)$ QZA, so auch $A \times B = (Q_1 \times Q_2, N, \varphi \times \psi)$ mit

$$(\varphi \times \psi)((x_0, y_0), \ldots, (x_{N-1}, y_{N-1})) = (\varphi(x_0, \ldots, x_{N-1}), \psi(y_0, \ldots, y_{N-1}).$$

Beweis: Angenommen, der zu $A \times B$ gehörende globale Entwicklungsoperator $\Phi \times \Psi$ wäre nicht unitär. Dann gibt es deterministische globale Konfigurationen a, a' über Q_1 und b, b' über Q_2 so dass $(a, b) \neq (a', b')$ und $(\Phi(a), \Psi(b)) = (\Phi(a'), \Psi(b'))$. Aus $(a, b) \neq (a', b')$ folgt $a \neq a'$ oder

$b \neq b'$; nehmen wir ohne Beschränkung der Allgemeinheit ersteres an. Dann ist aber $\Phi(a) = \Phi(a')$, also ist schon Φ nicht unitär und somit A kein wohlgeformter QZA. □

Mit diesen beiden Operationen kann man zwar viele QZA aus RZA erzeugen, aber unmöglich alle oder auch nur eine dichte Teilmenge. Wäre dies möglich, so müsste jeder QZA mit $|Q|$ prim durch eine unitäre Transformation auf Q mit einem RZA verwandt sein.

4.4 QZA als $\star$-Morphismen

4.4.1 Einleitung

Die bisher vorgestellten Definitionen von QZA haben zwei Nachteile. Erstens sind sie auf endliche Konfigurationen beschränkt; das Modell von van Dam auf periodischen Konfigurationen hat eine Lücke, wie in Abschnitt 4.2.5 gezeigt wurde. Diese Beschränkung ist an sich nicht schwerwiegend, weil die meisten Anwendungen ohnehin nur endlichen Träger verlangen, aber es stört doch, dass die Definition von ZA sich nicht in ihrer vollen Allgemeinheit aus dem klassischen Bereich übertragen lassen soll.

Der zweite Nachteil ist die Notwendigkeit, nach jeder Anwendung der globalen Überführungsfunktion die Amplituden für globale Konfigurationen auszumultiplizieren. Die Anzahl Summanden, die man dabei erhält, wächst im Allgemeinen exponentiell mit der Anzahl Iterationen des Zellularautomaten. Dadurch ist eine analytische Untersuchung praktisch ausgeschlossen, wenn man sich nicht auf sehr stark vereinfachte Spezialfälle beschränken will (wie dies zum Beispiel D. Meyer tut). Dieses exponentielle Wachstum ist als Folge des Quantenparallelismus prinzipiell nicht vermeidbar. Wir stellen daher ein Modell vor, das ohne Kenntnis der globalen Amplituden auskommt.

Eigentlich sollte es für die Anwendung der Überführungsfunktion nicht notwendig sein, globale Amplituden zu ermitteln. Messen kann man in endlicher Zeit nur endlich viele Zellen, für die Wahrscheinlichkeiten der relevanten Messergebnisse sollte es daher ausreichen, den Zustand jeder endlichen

zusammenhängenden Menge von Zellen zu beschreiben.

Auch für die Anwendung der globalen Überführungsfunktion sollte ein ZA keine Kenntnis globaler Amplituden benötigen. Schließlich arbeiten ZA immer lokal – jede einzelne Zelle kennt nur die Zustände in ihrer Nachbarschaft. Auch auf diese hat sie nur eine eingeschränkte Sicht, denn Zellen außerhalb ihrer Nachbarschaft können durchaus mit der Nachbarschaft verschränkt sein. Durch Ausspuren der restlichen Konfiguration können wir einen Dichteoperator für den Zustand der Zellen in der Nachbarschaft erhalten, der genau diese eingeschränkte Sicht reflektiert.

Aus dieser Idee entwickeln wir nun eine Definition von QZA, die einen sinnvollen Begriff von lokalen Konfigurationen zulässt und es insofern leichter macht, Konfigurationen auch nach längerer Entwicklung des QZA zu beschreiben. Darüber hinaus erlaubt sie eine Erweiterung auf unendliche Konfigurationen.

4.4.2 Zustände

Betrachten wir zunächst die einzelnen Zellen getrennt. Jede hat den gleichen endlichen Vorrat Q an Basiszuständen. Ein reiner Quantenzustand einer einzelnen Zelle ist ein Vektor aus dem Hilbertraum $\ell_2(Q)$. Es bezeichne $\mathcal{H}_i$ den zu $\ell_2(Q)$ isomorphen Hilbertraum der reinen Zustände von Zelle i; außerdem sei $\mathcal{B}(\mathcal{H})_i$ die C*-Algebra der beschränkten Operatoren auf $\mathcal{H}_i$. Weil jeder der Hilberträume $\mathcal{H}_i$ isomorph zu $\ell_2(Q)$ ist, ist jede der Algebren $\mathcal{B}(\mathcal{H})_i$ isomorph zu $\mathcal{B}(\ell_2(Q))$.

Der *Zustand* von Zelle i ist dann durch ein hermitesches Element von $\mathcal{B}(\mathcal{H})_i$ gegeben.

Betrachten wir nun eine endliche Menge von N Zellen mit den Operatoralgebren $\mathcal{B}(\mathcal{H})_1, \ldots, \mathcal{B}(\mathcal{H})_N$, so ist entsprechend den Vereinbarungen aus Abschnitt 3.6 die zugehörige Operatoralgebra das Tensorprodukt $\mathcal{B}(\mathcal{H})_1 \otimes \ldots \otimes \mathcal{B}(\mathcal{H})_N$. Der Zustand einer solchen Menge von Zellen ist durch ein Element dieses Tensorproduktes der Algebren gegeben; insbesondere entspricht jede lokale Konfiguration einem Zustand von N nebeneinanderliegenden Zellen.

Mit der Festlegung

$$\mathcal{A}_0 = \mathcal{B}(\mathcal{H})_0 \tag{4.11}$$

$$\mathcal{A}_1 = \mathcal{B}(\mathcal{H})_{-1} \otimes \mathcal{B}(\mathcal{H})_0 \otimes \mathcal{B}(\mathcal{H})_1 \tag{4.12}$$

allgemein

$$\mathcal{A}_n = \bigotimes_{i=-n}^{n} \mathcal{B}(\mathcal{H})_i \tag{4.13}$$

erhalten wir einen Turm $\mathcal{A}_0 \subset \mathcal{A}_1 \subset \ldots$ von C*-Algebren. Nach Abschnitt 3.6 ist der Normabschluss des induktiven Limes dieses Turms selbst eine C*-Algebra, nämlich die quasilokale Algebra $\mathcal{A}_{ql}$. Damit wird es möglich, unendliche globale Konfigurationen als Elemente von $\mathcal{A}_{ql}$ aufzufassen, wenn wir das unendliche Tensorprodukt $\bigotimes_{i=-\infty}^{\infty} \mathcal{B}(\mathcal{H})_i$ durch $\mathcal{A}_{ql}$ definieren. Die Herleitung von $\mathcal{A}_{ql}$ aus einem induktiven Grenzwert ineinander eingebetteter endlicher Tensorprodukte rechtfertigt diese Festlegung.

Aus globalen Konfigurationen erhält man durch Ausspuren lokale Konfigurationen sowie die Zustände von einzelnen Zellen. Zusammenfassend erhalten wir:

Definition 4.4 (Zell- und Block-Zustände)
Ein Zell-Zustand *ist ein hermitesches Element der* Zell-Algebra $\mathcal{B}(\mathcal{H})$. *Ein* Block-Zustand *der Länge* N *ist ein hermitesches Element des* N*-fachen Tensorproduktes* $\mathcal{B}(\mathcal{H})^N$.

Es ist wichtig, zwischen der *Menge der Basiszustände* Q und der Menge der Zell-Zustände zu unterscheiden; letztere ist die Menge der beschränkten Observablen über dem Hilbertraum $\mathcal{H} = \ell_2(Q)$.

Wir bezeichnen $\mathcal{B}(\mathcal{H})^N$ auch als *Block-Algebra*; passender wäre *lokale Algebra*, aber dieser Begriff hat schon eine andere Bedeutung. Ein Block-Zustand übernimmt hier die Rolle einer lokalen Konfiguration, entspricht also in etwa einem Wort. Man könnte Block-Zustände auch Quanten-Wörter nennen; wir verwenden den Begriff Block-Zustand, weil wir später Block-QZA definieren werden. Durch einen Block-Zustand sind die Zustände der Teilblöcke eindeutig bestimmt; dafür verwenden wir reduzierte Dichteoperatoren.

Nach diesen Überlegungen liegt es nahe, globale Quanten-Konfigurationen als Elemente von $\mathcal{A}_{ql}$ aufzufassen. Dies werden wir auch tun; praktisch ist diese Definition aber etwas unanschaulich, weshalb wir folgende äquivalente Formulierung verwenden, die an Definition 2.11 erinnert.

Definition 4.5 (Globale Quanten-Konfiguration)
Eine globale Quanten-Konfiguration ist eine Funktion $\widehat{q}$, *die jedem endlichen Intervall aus* $\mathbb{Z}$ *einen Quanten-Blockzustand dergestalt zuordnet, dass die folgende Konsistenzbedingung erfüllt ist:*

Sei I_k *ein Intervall der Länge* k *und* I_l *ein Teilintervall von* I_k *mit der Länge* l. *Dann ist* $\widehat{q}(I_k) \in \mathcal{B}(\mathcal{H})^k$ *und* $\widehat{q}(I_l) \in \mathcal{B}(\mathcal{H})^l$ *und der reduzierte Dichteoperator* $\mathrm{tr}_{I_k \setminus I_l} \widehat{q}(I_k)$ *von* I_l *als Teilsystem von* I_k *ist gleich* $\widehat{q}(I_l)$.

Wegen des Zusammenhangs zwischen Zuständen von Teilsystemen und reduzierten Dichteoperatoren repräsentiert jedes $\widehat{q}$ eine Cauchy-Folge in der lokalen Algebra $\mathcal{A}_l$ und als solche ein Element von $\mathcal{A}_{ql}$. Umgekehrt existiert zu jedem Element von $\mathcal{A}_{ql}$ eine Cauchyfolge in $\mathcal{A}_l$, die dieses Element als Grenzwert hat und aus ihr gewinnen wir konsistente Zustände der endlichen Blöcke.

Ist $\widehat{q}$ eine globale Quanten-Konfiguration, so bezeichnen wir mit $\widehat{q}[i]$ den Dichteoperator, der den Zustand von Zelle i in $\widehat{q}$ repräsentiert. Entsprechend verwenden wir $\widehat{q}[i \ldots j]$ für den Zustands des Intervalls von Zelle i bis Zelle j $(i < j)$.

Im Folgenden bezeichnet $\mathcal{C}(\mathcal{H})$ die Menge der globalen Quanten-Konfigurationen, in denen $\mathcal{H}$ der Hilbertraum der Zell-Zustände ist. Wir schreiben $\mathcal{C}$, wenn $\mathcal{H}$ aus dem Zusammenhang eindeutig hervorgeht.

4.4.3 Einige $\star$-Automorphismen

Wir untersuchen $\star$-Automorphismen in ihrem Verhalten auf tensorierten Algebren und geben einige Beispiele an, aus denen wir im folgenden Abschnitt Überführungsfunktionen von QZA zusammensetzen werden.

Ein Beispiel eines Automorphismus der quasilokalen Algebra ist die *Verschiebung*, die jeder Zelle den Zustand ihrer linken Nachbarzelle zuordnet. Offenbar ist die Verschiebung ein Automorphismus von $\mathcal{C}$, denn die Ver-

schiebung der Indizes ändert nichts an der Gültigkeit der Konsistenzbedingung.

Wir verwenden daneben auch *partielle Verschiebungen*; wir definieren sie analog zu der Definition in Abschnitt 1.3.2 wie folgt.

Sei dazu der Hilbertraum $\mathcal{H}$ der Basiszustände jeder einzelnen Zelle isomorph zu einem Tensorprodukt $\mathcal{I} \otimes \mathcal{J}$ von Hilberträumen. Dann ist für jede Zelle $\mathcal{B}(\mathcal{H})$ isomorph zu $\mathcal{B}(\mathcal{I}) \otimes \mathcal{B}(\mathcal{J})$. Wir schreiben $\mathrm{tr}_{\mathcal{J}}\widehat{q}(i)$ für den Anteil des Zustands der i-ten Zelle, den wir erhalten, wenn wir den $\mathcal{J}$-Anteil ausspuren.

Definition 4.6 (Partielle Quantenverschiebung)
Eine partielle Quantenverschiebung ist eine Selbstabbildung σ von $\mathcal{C}(\mathcal{I} \otimes \mathcal{J})$, so dass für alle $\widehat{q}$ und alle $i \in \mathbb{Z}$, $k \in \mathbb{N}$ gilt: Ist $\widehat{q}(i, \ldots, i+k)$ der Zustand des Intervalles von Zelle i bis Zelle $i+k$, so ist

$$\mathrm{tr}_{\mathcal{J}}\sigma(\widehat{q})(i, \ldots, i+k) = \mathrm{tr}_{\mathcal{J}}\widehat{q}(i-1, \ldots, i+k-1) \text{ und}$$
$$\mathrm{tr}_{\mathcal{I}}\sigma(\widehat{q})(i, \ldots, k) = \mathrm{tr}_{\mathcal{I}}\widehat{q}(i, \ldots, k).$$

Lemma 4.11
Partielle Quantenverschiebungen sind Automorphismen von $\mathcal{C}$.

Beweis: Sei σ eine partielle Quantenverschiebung. Laut Definition ist σ eine Selbstabbildung von $\mathcal{C}$. Wir konstruieren eine Inverse σ^{-1}, indem wir für globale Quanten-Zustände $\widehat{q}$, und Intervalle $(i, \ldots, i+k)$ festlegen:

$$\mathrm{tr}_{\mathcal{J}}\sigma(\widehat{q})(i, \ldots, i+k) = \mathrm{tr}_{\mathcal{J}}\widehat{q}(i+1, \ldots, i+k+1) \text{ und}$$
$$\mathrm{tr}_{\mathcal{I}}\sigma(\widehat{q})(i, \ldots, k) = \mathrm{tr}_{\mathcal{I}}\widehat{q}(i, \ldots, k).$$

□

Weiter können wir *Blocktransformationen* definieren, die auf disjunkten Teilmengen der Zellen eines QZA operieren. Vereinfachend schreiben wir $\mathcal{A}^N$ für das Tensorprodukt von N zu $\mathcal{A}$ isomorphen C*-Algebren.

Definition 4.7 (Quanten-Blocktransformation)
Eine Quanten-Blocktransformation ist ein 4-Tupel $(N, i, \mathcal{A}, \varphi)$ aus Blockgröße $N \in \mathbb{N}$, Ursprung $i \in \mathbb{Z}$, einer endlichdimensionalen C-Algebra $\mathcal{A}$ und einem $\star$-Automorphismus φ von $\mathcal{A}^N$.*

Sei $\mathcal{B}(\mathcal{H})_i$ die $C^\star$-Algebra der beschränkten Operatoren auf dem Hilbertraum der Zelle i. Jede dieser Algebren ist isomorph zu $\mathcal{B}(\ell_2(Q))$. Wir teilen die Zellen so in Blöcke der Länge N ein, dass der Anfang eines Blockes auf die Zelle i fällt. Dann wenden wir auf jeden Block φ an. Wir schreiben $\Phi(\widehat{q})$ für das Ergebnis der Anwendung von φ auf $\widehat{q} \in \mathcal{C}$, wenn die übrigen Parameter der Blocktransformation aus dem Zusammenhang klar sind.

Lemma 4.12
Quanten-Blocktransformationen definieren Automorphismen von $\mathcal{C}$.

Beweis: Sei $(N, i, \mathcal{B}(\mathcal{H}), \varphi)$ eine Quanten-Blocktransformation. Sie ist offenbar reversibel, da φ nach Voraussetzung ein $\star$-Automorphismus von $\mathcal{B}(H)^N$ ist. Es ist also nur zu zeigen, dass Quanten-Blocktransformationen Selbstabbildungen von $\mathcal{C}$ sind. Sei dazu $\widehat{q} \in \mathcal{C}$ und $I = (j, \ldots, j+k-1)$ ein Intervall in $\mathbb{Z}$. Um $\Phi(\widehat{q})(I)$ zu ermitteln, unterscheiden wir zwei Fälle. Entweder es gilt $j \cong i \bmod N$ und $k \cong 0 \bmod N$; dann fallen die Intervallgrenzen mit Blockgrenzen zusammen. In diesem Fall ist $(\Phi(\widehat{q}))(I) = \varphi^{k/N}(\widehat{q}(I))$, wobei $\varphi^{k/N}$ für das k/N-fache Tensorprodukt von φ mit sich selbst steht. Der kompliziertere Fall liegt vor, wenn die Intervallgrenzen nicht mit Blockgrenzen zusammenfallen. Dann gibt es ein Intervall $I' = (l, \ldots, l+m-1)$ mit $j \leq l$ und $m \geq k$, so dass die Grenzen von I' mit Blockgrenzen zusammenfallen. Wir bilden wie eben $(\Phi(\widehat{q}))(I')$ und erhalten daraus $(\Phi(\widehat{q}))(I)$ durch partielle Spurbildung.

Nun ist zu zeigen, dass für beliebige Teilintervalle J von I gilt:

$$\mathrm{tr}_{I \setminus J}(\Phi(\widehat{q}))(I) = (\Phi(\widehat{q}))(J).$$

Weil partielle Spurbildung assoziativ ist, reicht es aus, den Fall zu betrachten, dass die Intervallgrenzen von I und J mit Blockgrenzen zusammenfallen. Die Behauptung folgt daraus, dass dann die Zellen in J und die in $I \setminus J$ bei Anwendung von Φ nicht interagieren. □

Lemma 4.13
Seien $(N, i, \mathcal{B}(\mathcal{H}), \varphi)$ und $(N, j, \mathcal{B}(\mathcal{H}), \psi)$ zwei Quanten-Blocktransformationen. Dann ist ihre Hintereinanderausführung ein Automorphismus von $\mathcal{C}(\mathcal{H})$.

Beweis: Eine Blocktransformation B mit Ursprung i ist äquivalent zu einer Verschiebung um $i-j$ gefolgt von der Blocktransformation B mit Ursprung j, gefolgt von einer Verschiebung um $j-i$.

Sind also $B_1 = (N, i, \mathcal{B}(\mathcal{H}), \varphi)$ und $B_2 = (N, j, \mathcal{B}(\mathcal{H}), \psi)$ zwei Blocktransformationen, so ist ihre Hintereinanderausführung $B_2 \circ B_1$ äquivalent zu $T_{i-j} \circ B_2' \circ T_{j-i} \circ B_1$, wobei B_2' für die Blocktransformation $(N, i, \mathcal{B}(\mathcal{H}), \psi)$ steht und T_{i-j} für eine Verschiebung um $i-j$. Der Wechsel des Ursprungs ist demnach unerheblich dafür, ob es sich bei der Hintereinanderausführung von Blocktransformationen um einen Automorphismus handelt.

Wir haben hier ohne Einschränkung vorausgesetzt, dass B_1 und B_2 die gleiche Blockgröße verwenden. Dies ist möglich, da wir leicht aus einer Blocktransformation mit Blockgröße N eine äquivalente mit Blockgröße kN erhalten, indem wir die Überführungsfunktion φ k-fach mit sich selbst tensorieren. Folglich können wir, wenn B_1 und B_2 verschiedene Blockgrößen N und M haben sollten, sie durch äquivalente Blocktransformationen mit der Blockgröße $kgV(N, M)$ ersetzen. □

Quanten-Blocktransformationen sind ein Beispiel für lokale Operationen, die Selbstabbildungen von $\mathcal{C}$ induzieren. Lokal wirken die Blocktransformationen als Superoperatoren auf den – möglicherweise gemischten – Zuständen der Blöcke. Die bisher vorgestellten Definitionen von QZA basierten als Abbildungen von Vektoren eines Hilbertraumes grundsätzlich auf reinen Zuständen. Das folgende Beispiel soll den Zusammenhang zwischen beiden Ansätzen verdeutlichen.

Der Übersichtlichkeit halber verwenden wir nur vier Zellen, die wir uns zyklisch verbunden denken; das heißt, die vierte Zelle ist Nachbar der ersten und umgekehrt. Es bezeichne $\mathcal{H}_i$ den endlichen Hilbertraum der Zustände von Zelle i. Im Hilbertraumformalismus ist ein Zustand der Zellen eins bis vier ein Element von $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3 \otimes \mathcal{H}_4$.

Wir verwenden die Blocktransformationen φ_{12}, φ_{34}, ψ_{23} und ψ_{14}, die jeweils als innere Automorphismen von $\mathcal{B}(\mathcal{H})_i \otimes \mathcal{B}(\mathcal{H})_j$ durch unitäre Matrizen dargestellt sind; für diese Matrizen schreiben wir ebenfalls φ_{12} und so weiter.

Der Vektor $|v_1\rangle \otimes |v_2\rangle \otimes |v_3\rangle \otimes |v_4\rangle$ repräsentiere den Anfangszustand. Wir

gehen davon aus, dass der Anfangszustand als Tensorprodukt darstellbar ist; ist er dies nicht, berechnen wir die Schmidt-Darstellung und rechnen linear auf den Summanden. Wir wenden nun die unitäre Matrix φ_{12} auf $|\nu_1\rangle \otimes |\nu_2\rangle$ und die unitäre Matrix φ_{34} auf $|\nu_3\rangle \otimes |\nu_4\rangle$ an und erhalten

$$\begin{aligned}&\sum_i \alpha_i \left(|\nu_{1i}\rangle \otimes |\nu_{2i}\rangle\right) \otimes \sum_j \beta_j \left(|\nu_{3j}\rangle \otimes |\nu_{4j}\rangle\right)\\ &= \sum_{ij} \alpha_i\beta_j \left(|\nu_{1i}\nu_{2i}\nu_{3j}\nu_{4j}\rangle\right).\end{aligned}$$

Dann wenden wir ψ_{23} auf den Teilraum $\mathcal{H}_2 \otimes \mathcal{H}_3$ und ψ_{14} auf den Teilraum $\mathcal{H}_1 \otimes \mathcal{H}_4$ an und erhalten

$$\sum_{ij} \alpha_i\beta_j \left(\psi_{14}(|\nu_{1i}\nu_{4j}\rangle) \otimes \psi_{23}(|\nu_{2i}\nu_{3j}\rangle)\right). \tag{4.14}$$

Führen wir nun die entsprechende Rechnung im operatoralgebraischen Formalismus durch. Wir wenden die inneren Automorphismen φ_{ij} und ψ_{kl} auf die reduzierten Dichtematrizen für die entsprechenden Zellpaare an.

Bei der Anwendung von φ_{ij} geschieht noch nichts Interessantes: Weil wir den Anfangszustand als separabel vorausgesetzt haben, sind die reduzierten Dichtematrizen für die ersten beiden Zellen gleich $|\nu_1\nu_2\rangle\langle\nu_1\nu_2|$ und für die beiden anderen Zellen $|\nu_3\nu_4\rangle\langle\nu_3\nu_4|$. Nach Anwendung von φ_{12} ist das Teilsystem aus den ersten beiden Zellen dann in einem Zustand, der durch den Dichteoperator $\sum_i \alpha_i|\nu_{1i}\nu_{2i}\rangle\langle\nu_{1i}\nu_{2i}|$ beschrieben wird; für das andere Teilsystem gilt der Zustand $\sum_j \beta_j|\nu_{3j}\nu_{4j}\rangle\langle\nu_{3j}\nu_{4j}|$.

Um nun ψ_{14} anzuwenden, müssen wir aus dem ersten Teilsystem den Zustand von Zelle zwei ausspuren und aus dem anderen Teilsystem den Zustand von Zelle drei.

$$\begin{aligned}\mathrm{tr}_2\left(\sum_i \alpha_i|\nu_{1i}\nu_{2i}\rangle\langle\nu_{1i}\nu_{2i}|\right) &= \sum_i |\alpha_i|^2|\nu_{1i}\rangle\langle\nu_{1i}|\\ \mathrm{tr}_3\left(\sum_j \beta_j|\nu_{3j}\nu_{4j}\rangle\langle\nu_{3j}\nu_{4j}|\right) &= \sum_j |\beta_j|^2|\nu_{4j}\rangle\langle\nu_{4j}|\end{aligned}$$

Mit Anwendung von ψ_{14} wird daraus

$$\begin{aligned}
&\psi_{14}^{\dagger}\left(\sum_{i}|\alpha_i|^2|\nu_{1i}\rangle\langle\nu_{1i}|\otimes\sum_{j}|\beta_j|^2|\nu_{4j}\rangle\langle\nu_{4j}|\right)\psi_{14}\\
&=\psi_{14}^{\dagger}\left(\sum_{ij}|\alpha_i|^2|\beta_j|^2|\nu_{1i}\rangle\langle\nu_{1i}|\otimes|\nu_{4j}\rangle\langle\nu_{4j}|\right)\psi_{14}\\
&=\sum_{ij}|\alpha_i|^2|\beta_j|^2\psi_{14}^{\dagger}\left(|\nu_{1i}\rangle\langle\nu_{1i}|\otimes|\nu_{4j}\rangle\langle|\nu_{4j}\right)\psi_{14}.
\end{aligned}$$

Für die Zellen zwei und drei verfahren wir mit ψ_{23} analog. Insgesamt erhält man für den neuen Zustand des Gesamtsystems

$$\begin{aligned}
&\sum_{ij}|\alpha_i|^2|\beta_j|^2\psi_{14}^{\dagger}\left(|\nu_{1i}\nu_{4j}\rangle\langle\nu_{1i}\nu_{4j}|\right)\psi_{14}\otimes\sum_{ij}|\alpha_i|^2|\beta_j|^2\psi_{23}^{\dagger}\left(|\nu_{2i}\nu_{3j}\rangle\langle\nu_{2i}\nu_{3j}|\right)\psi_{23}\\
&=\sum_{ij}|\alpha_i|^2|\beta_j|^2\left(\psi_{14}^{\dagger}\left(|\nu_{1i}\nu_{4j}\rangle\langle\nu_{1i}\nu_{4j}|\right)\psi_{14}\otimes\psi_{23}^{\dagger}\left(|\nu_{2i}\nu_{3j}\rangle\langle\nu_{2i}\nu_{3j}|\right)\psi_{23}\right),
\end{aligned}$$

was der Dichteoperator zu dem Zustand aus Gleichung 4.14 ist. Der Vorteil der operatorbasierten Definition wird deutlich, wenn man dieses Beispiel auf mehr Zellen verallgemeinert. Beim Hilbertraum-Ansatz muss man immer global verfahren. Wenn man aber die Zustände lokal beschreibt, braucht man für die lokale Anwendung von Blocktransformationen auch nur die reduzierten Dichtematrizen der direkt beteiligten Zellen zu kennen.

4.4.4 Quanten-Blockzellularautomaten

Wir können nun eine weitere Variante von QZA definieren, nämlich als Automorphismen von $\mathcal{C}$. Unsere Definition basiert auf Block-Zellularautomaten, weil wir diese mit Hilfe von Quanten-Blocktransformationen einfach definieren können. Wir werden zeigen, dass dies gegenüber den bisher bekannten Modellen keine Einschränkung bedeutet. Wir kürzen Quanten-Blockzellularautomaten als BQZA ab.

Definition 4.8 (BQZA)
Ein BQZA besteht aus einer endlichen Folge $B_1, B_2, \ldots, B_n$ *von Quanten-Blocktransformationen* $B_i = (N, j_i, \mathcal{B}(\mathcal{H}), \varphi_i)$.

Wir weichen hier nur insofern von der üblichen Definition ab, als wir zulassen, dass die einzelnen Blocktransformationen unterschiedliche φ_i verwenden. Für die Frage nach der Wohlgeformtheit ist dies nicht wichtig.

Einen BQZA auf eine globale Konfiguration anzuwenden bedeutet, dass die Quanten-Blocktransformationen nacheinander angewandt werden.

Lemma 4.14
BQZA definieren Automorphismen von $\mathcal{C}$.

Beweis: Dies folgt induktiv aus Lemma 4.12. □

Als nächstes zeigen wir, dass BQZA eine zu den PQZA von Watrous äquivalente Funktionenklasse beschreiben. Zunächst beobachten wir, dass wir eine Definition von QZA auf $\mathcal{C}$ auch auf Basis partitionierter ZA geben können. Sei dazu die endliche Menge Q isomorph zu $Q_1 \times Q_2 \times \ldots \times Q_N$. Der Hilbertraum zu jeder einzelnen Zelle ist dann isomorph zu $\ell_2(Q)$, also isomorph zu $\ell_2(Q_1) \otimes \ell_2(Q_2) \otimes \ldots \otimes \ell_2(Q_N)$. Die lokale Überführungsfunktion ist als unitäres Element von $\mathcal{B}(\ell_2(Q))$ gegeben und induziert (als Spezialfall einer Blocktransformation mit der Blockgröße eins) einen Automorphismus von $\mathcal{C}$. Daneben verwenden wir N partielle Quantenverschiebungen, um jeweils die i-te Komponente jeder Zelle ihrem i-ten Nachbarn zukommen zu lassen.

Definition 4.9 (PQZA auf $\mathcal{C}$)
Ein PQZA besteht aus einer Nachbarschaftsgröße $N \in \mathbb{N}$, einem kartesischen Produkt $Q_1 \times \ldots Q_N$ von N endlichen Zustandsmengen und einem inneren Automorphismus φ von $\mathcal{B}(\ell_2(Q_1) \otimes \ldots \otimes \ell_2(Q_N))$.

Ohne Beschränkung der Allgemeinheit sei N ungerade. Anwendung eines PQZA auf eine globale Konfiguration erfolgt in N Schritten. Die ersten $N-1$ Schritte sind partielle Quantenverschiebungen; für i zwischen 1 und $(N-1)/2$ verschieben wir die i-te Komponente jedes Zellzustandes um $(N-1)/2 - i + 1$ nach links und für i zwischen $(N+1)/2$ und N um $i - (N-1)/2 + 1$ nach rechts. Im letzten Schritt wird auf jede Zelle die lokale Überführungsfunktion φ angewandt. Wie BQZA sind PQZA als Hintereinanderausführung endlich vieler Automorphismen selbst Automorphismen von $\mathcal{C}$. Außerdem besteht ein Isomorphismus zwischen PQZA

auf $\mathcal{C}$ und den PQZA von Watrous, denn jede legale lokale Überführungsfunktion in der Definition von Watrous ist eine unitäre Selbstabbildung von $\ell_2(Q_1) \otimes \ldots \otimes \ell_2(Q_N)$ und entspricht daher einem inneren Automorphismus, wie er für PQZA auf $\mathcal{C}$ gefordert ist. Umgekehrt entspricht jeder innere Automorphismus einer solchen unitären Abbildung.

Außerdem können sich BQZA und PQZA in einer naheliegenden Art gegenseitig simulieren.

Lemma 4.15
Jeder PQZA kann von einem BQZA ohne Zeitverlust simuliert werden.

Beweis: Sei (Q^N, N, φ) ein PQZA. Wir simulieren eine globale Anwendung des PQZA mit zwei Blocktransformationen eines BQZA mit Zell-Algebra $\mathcal{B}(\ell_2(Q))$ und Blockgröße $N(N-1)$. Die erste Blocktransformation ψ_1 erfolgt relativ zum Ursprung N, die zweite ψ_2 relativ zum Ursprung $N(N-1)$. Wir machen also aus jeder Partition eine eigene Zelle. Wir verwenden, dass die Zustandsmengen aller Partitionen gleich Q sind; dies lässt sich durch geeignete Einbettungen immer erreichen. Wir beginnen mit einem Zustand

$$\ldots, (x_0^{(0)}, \ldots, x_{N-1}^{(0)}), (x_0^{(1)}, \ldots, x_{N-1}^{(1)}), \ldots, (x_0^{(N-1)}, \ldots, x_{N-1}^{(N-1)}), \ldots .$$

Dabei geben die höhergestellten Indizes an, zu welcher Zelle des partitionierten QZA ein Zustand gehört und die niedergestellten geben an, zu welcher Partition er gehört. Bei der ersten Einteilung in Blöcke beginnt ein Block mit der N-ten Zelle, also der mit dem Zustand $x_{N-1}^{(0)}$, und reicht bis zur $2N-1$-ten Zelle, also bis zu der mit dem Zustand $x_{N-2}^{(N-1)}$.

Auf diesem Eingabeblock erzeugt ψ_1 die Ausgabe

$$\begin{aligned} x_0^{(1)}, \ldots, x_{N-3}^{(1)}, & x_0^{(2)}, \ldots, x_{N-4}^{(2)}, \ldots, x_0^{(N-2)}, \\ & \varphi(x_{N-1}^{(0)}, x_{N-2}^{(1)}, \ldots, x_0^{(N-1)}), \\ & x_{N-1}^{(1)}, x_{N-2}^{(2)}, x_{N-1}^{(2)}, \ldots, x_1^{(N-1)}, \ldots, x_{N-2}^{(N-1)}. \end{aligned}$$

Die Blocktransformation ψ_1 berechnet für die Zelle mit dem Index $(N-1)/2+1$ des PQZA den neuen Zustand mittels φ. Links von diesem neuen Zustand in ihrer Ausgabe stehen diejenigen Daten, die Zellen links von $(N-1)/2+1$ zum Berechnen ihres neuen Zustandes benötigen; rechts davon

stehen die Daten für die Zellen rechts von $(N-1)/2+1$. Als Kombination der unitären Abbildung $\varphi : Q^N \to Q^N$ mit einer Permutation von $Q^{(N-2)N}$ ist ψ_1 ein $\star$-Automorphismus von $\mathcal{B}(\ell_2(Q^{(N-1)N}))$.

Den Ursprung für die zweite Blocktransformation ψ_2 wählen wir so, dass der Anfang eines Blockes immer auf eine Zelle fällt, deren neuer Zustand schon berechnet wurde. Wir erhalten damit als Eingabe für ψ_2

$$\begin{aligned}
&\varphi(x_{N-1}^{(0)}, x_{N-2}^{(1)}, \ldots, x_0^{(N-1)}),\\
&\quad x_{N-1}^{(1)}, x_{N-2}^{(2)}, x_{N-1}^{(2)}, \ldots, x_1^{(N-1)}, \ldots, x_{N-2}^{(N-1)},\\
&\quad x_0^{(N)}, \ldots, x_{N-3}^{(N)}, x_0^{(N+1)}, \ldots, x_{N-4}^{(N+1)}, \ldots, x_0^{(N+N-2)}
\end{aligned}$$

und definieren als Ausgabe

$$\begin{aligned}
&\varphi(x_{N-1}^{(0)}, x_{N-2}^{(1)}, \ldots, x_0^{(N-1)}),\\
&\varphi(x_{N-1}^{(1)}, x_{N-2}^{(2)}, \ldots, x_0^{(N)}),\\
&\quad \vdots\\
&\varphi(x_{N-1}^{(N-1)}, x_{N-2}^{(N)}, \ldots, x_0^{(N+N-2)}).
\end{aligned}$$

Mit dieser Festlegung ist die zweite Blocktransformation ψ_2 ebenfalls ein $\star$-Automorphismus, denn wie man sieht, erhält sie nicht mehr Eingaben, als auch φ bekommen würde, um die neuen Zustände zu berechnen. Da die Hintereinanderausführung von ψ_1 und ψ_2 das gleiche Ergebnis hat wie die globale Anwendung von φ (von der unterschiedlichen Zusammenfassung der Zellen in Blöcke einmal abgesehen), folgt hieraus die Behauptung. □

Lemma 4.16
Jeder BQZA kann von PQZA simuliert werden.

Beweis: Da wir zulassen, dass die einzelnen Blocktransformationen verschiedene lokale Überführungsfunktionen verwenden, brauchen wir für jede Blocktransformation einen eigenen PQZA. Wir fassen jeden Block bezüglich der ersten Blockeinteilung als eine Zelle auf und wenden zunächst auf jeden Block die Block-Überführungsfunktion an; sie definieren wir auch als die Überführungsfunktion des ersten PQZA.

Nun wechselt die Blockeinteilung. Da die Blöcke jeder Blocktransformation die gleiche Länge haben, muss in jeden Block genau eine neue Blockgrenze fallen (wenn ein Block keine Blockgrenze enthielte, müssten die ersten beiden Blockeinteilungen gleich sein und dann könnte man die ersten zwei Blocktransformationen zu einer zusammenfassen). Diese Blockgrenze definieren wir als die Partitionierungsgrenze für den zweiten PQZA; wir verwenden also einen PQZA mit nur zwei Partitionen. Dann definieren wir die Überführungsfunktion des zweiten PQZA wieder als diejenige der zweiten Blocktransformation.

So fortfahrend behandeln wir alle Blocktransformationen und erhalten zu einem beliebigen BQZA eine Hintereinanderausführung von PQZA. □

Aus unseren Überlegungen folgt insbesondere, dass man die Definition von PQZA nach Watrous auf unendliche Konfigurationen erweitern kann.

Außerdem können wir jeden QZA nach der Definition von van Dam mit einem BQZA simulieren und umgekehrt.

Lemma 4.17
BQZA und van Dams QZA können sich gegenseitig simulieren.

Beweis: Der Beweis orientiert sich an den bekannten Simulationsverfahren für klassische BZA und ZA, wie sie zum Beispiel Durand-Lose beschrieben hat [25, 26].

Zu jedem BQZA gibt es einen QZA nach van Dam mit äquivalenter globaler Überführungsfunktion:

Der BQZA habe die Blockgröße N und die Zell-Algebra $\mathcal{B}(\mathcal{H})$ für einen endlichdimensionalen Hilbertraum $\mathcal{H}$. Für i zwischen 1 und N bezeichne $\mathcal{H}_i$ einen zu $\mathcal{H}$ isomorphen Hilbertraum. Wir wählen eine Orthonormalbasis Q von $\bigotimes_{i=1}^{N} \mathcal{H}_i$; sie ist eine Basis des Zustandsraumes der Blöcke der Länge N und wir legen fest, dass sie die Zustandsmenge des simulierenden QZA repräsentiere.

Falls der BQZA aus nur einer Blocktransformation besteht, ist der gesuchte QZA durch $(Q, 1, \psi_1)$ gegeben und wir sind fertig. Nehmen wir an, es gäbe eine zweite Blocktransformation ψ_2. Bevor wir diese anwenden, müssen wir die Zellen ausgehend vom Ursprung der zweiten Partitionierung neu in Blöcke einteilen. Dabei fällt in jeden alten Block genau eine neue

Blockgrenze; zu $\rho \in \mathcal{B}(\mathcal{H})$ bezeichne $R(\rho)$ den Teil des Zustandes rechts und $L(\rho)$ den Teil links von der neuen Blockgrenze.

Dann erhält ψ_2 eine Eingabe, die aus dem rechten Teil $R(\rho_{i-1})$ von Block $i-1$ und dem linken Teil $L(\rho_i)$ von Block i besteht, und dies für alle $i \in \mathbb{Z}$. Damit definieren wir eine lokale Überführungsfunktion $\varphi : \mathcal{B}(\mathcal{H}_{i-1} \otimes \mathcal{H}_i) \to \mathcal{B}(\mathcal{H})_i$ durch

$$\varphi(\rho_{i-1}, \rho_i) = \psi_2(R(\psi_1(\rho_{i-1})), L(\psi_1(\rho_i))). \tag{4.15}$$

Wir behaupten nun, dass $(Q, 2, \varphi)$ ein wohlgeformter QZA nach van Dams Definition ist. Dazu betrachten wir eine globale Konfiguration, die sich als Tensorprodukt der Blockzustände darstellen lässt (van Dams QZA sind nur auf solchen Konfigurationen definiert; man kann aber wie üblich jede endliche Konfiguration in eine Überlagerung solcher Konfigurationen überführen). Entsprechend der Definition von van Dam heisse sie periodisch, wenn sich die Blockzustände periodisch wiederholen. Wir definieren $\varphi_k(\rho_1, \ldots, \rho_k)$ durch $\varphi(\rho_1, \ldots, \rho_k, \rho_1)$. Auf Wörtern der Länge k erhalten wir mit Gleichung 4.15

$$\varphi_k(\rho_1, \ldots, \rho_k) = \psi_2(R(\psi_1(\rho_1)), \psi(\rho_2), \ldots, \psi(\rho_k), L(\psi(\rho_1))). \tag{4.16}$$

Demnach ist φ_k für alle $k \in \mathbb{N}$ unitär.

Gibt es mehr als zwei Blocktransformationen, so können wir sie zu Paaren zusammenfassen (möglicherweise behält man dabei eine einzelne Blocktransformation übrig; das ist egal). Zu jedem Paar ermitteln wir einen QZA und definieren dann den simulierenden QZA als die Hintereinanderausführung dieser einzelnen QZA sowie Verschiebungen, um die unterschiedlichen Ursprünge der Blockeinteilungen auszugleichen.

Damit ist der erste Teil des Lemmas bewiesen.

Zu jedem QZA nach van Dam gibt es einen BQZA mit äquivalenter globaler Überführungsfunktion.

Sei $\mathcal{H}$ der Hilbertraum der Zell-Zustände des QZA. Wir erweitern ihn um einen neuen Zustand, den wir mit 0 bezeichnen und nennen den erweiterten Hilbertraum $\mathcal{H}'$. Ohne Einschränkung sei die Nachbarschaftsgröße des QZA und seiner Inversen gleich 3 (dies lässt sich durch geeignete Vergrößerung der Zustandsmenge immer erreichen); φ sei die lokale Überführungsfunktion.

Als Blockzustandsmenge wählen wir $(\mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H})')^4$; dabei speichert die erste Komponente den Ausgangszustand der Zelle und die zweite nimmt den neuen Zustand auf, sobald er berechnet ist. Die erste Blockeinteilung hat den Ursprung 0. Für die erste Blocktransformation legen wir fest:

$$\begin{aligned}&\psi_1((\rho_0, 0), (\rho_1, 0), (\rho_2, 0), (\rho_3, 0))\\ &\quad = ((\rho_0, 0), (\rho_1, \varphi(\rho_0, \rho_1, \rho_2)), (\rho_2, \varphi(\rho_1, \rho_2, \rho_3)), (\rho_3, 0).\end{aligned}$$

Die übrigen Funktionswerte werden so gewählt, dass ψ_1 unitär ist (das geht immer). Der Ursprung der zweiten Blockeinteilung ist 2. Für die zweite Blocktransformation legen wir fest:

$$\begin{aligned}&\psi_2((\rho_2, \rho_2'), (\rho_3, 0), (\rho_4, 0), (\rho_5, \rho_5'))\\ &\quad = ((\rho_2, \rho_2'), (\rho_3, \varphi(\rho_2, \rho_3, \rho_4)), (\rho_4, \varphi(\rho_3, \rho_4, \rho_5)), (\rho_5, \rho_5')).\end{aligned}$$

Nun müssen wir die alten Zustände der Zellen reversibel löschen. Dies geschieht mit den folgenden zwei Blocktransformationen. Die dritte Blocktransformation hat den Ursprung 2 und ist durch

$$\begin{aligned}&\psi_3((\rho_2, \rho_2'), (\rho_3, \rho_3'), (\rho_4, \rho_4'), (\rho_5, \rho_5'))\\ &\quad = ((\rho_2, \rho_2'), (\rho_3 - \varphi^{-1}(\rho_2', \rho_3', \rho_4'), \rho_3'),\\ &\quad (\rho_4 - \varphi^{-1}(\rho_3', \rho_4', \rho_5'), \rho_4'), (\rho_5, \rho_5'))\end{aligned}$$

festgelegt. Schließlich hat die vierte Blocktransformation den Ursprung 0 und bewirkt

$$\begin{aligned}&\psi_4((0, \rho_0'), (\rho_1, \rho_1'), (\rho_2, \rho_2'), (0, \rho_3'))\\ &\quad = ((\rho_0', 0), (\rho_1', \rho_1 - \varphi^{-1}(\rho_0', \rho_1', \rho_2')),\\ &\quad (\rho_2', \rho_2 - \varphi^{-1}(\rho_1', \rho_2', \rho_3')), (\rho_3', 0)).\end{aligned}$$

Jede dieser Blocktransformationen lässt sich zu einer unitären Transformation fortsetzen. Durch Projektion auf die erste Komponente jedes Zustandspaars erhält man die globale Konfiguration, die das Ergebnis der globalen Anwendung der simulierten Überführungsfunktion φ ist.

Damit ist auch der zweite Teil des Lemmas bewiesen. □

Wir haben es hier also mit drei Schreibweisen der gleichen Klasse von Abbildungen zu tun und können folglich bei der Angabe der lokalen Überführungsfunktion jede der drei Schreibweisen verwenden. Im Folgenden verstehen wir unter QZA immer die hierdurch definierte Klasse von Abbildungen. Die Neuerung gegenüber den herkömmlichen Ansätzen besteht nicht in der Angabe einer weiteren Klasse von Abbildungen, die als QZA bezeichnet werden können; sie besteht im Wechsel zu einer operatoralgebraischen Schreibweise, die eine wirklich lokale Formulierung von Begriffen wie lokalen Konfigurationen und lokaler Überführungsfunktion erst möglich macht. Mit den Simulationslemmata wurde gezeigt, dass die herkömmlichen Wohlgeformtheits-Bedingungen für QZA sich ohne Verlust in diese Schreibweise übertragen lassen.

4.5 Metriken für QZA

4.5.1 Einleitung

Wie bei SZA wollen wir nun auch für QZA Metriken einführen, um globale Konfigurationen miteinander zu vergleichen. Hiermit wollen wir ganz wie bei SZA die Auswirkungen kleiner Änderungen an der Überführungsfunktion verfolgen; dies ist ein wichtiges Thema, weil es auf die Frage nach der Simulation gewisser Amplitudenmengen mit anderen führt, aber auch auf Robustheit gegenüber kleinen Fehlern.

Wir beginnen mit Metriken auf endlichen Konfigurationen, die als Vektoren eines Hilbertraumes darstellbar sind. Hier führt der Ansatz aus Abschnitt 2.5 jedoch nur auf eine Pseudometrik. Fassen wir globale Quanten-Konfigurationen jedoch als Elemente einer C^*-Algebra auf, so erhalten wir zwei nützliche Metriken.

4.5.2 Metriken auf endlichen Konfigurationen

Bei der Entwicklung einer Metrik für globale Quanten-Konfigurationen muss man zuerst entscheiden, auf welches Modell die Metrik anwendbar

sein soll. Die Definitionen von Watrous und van Dam auf endlichen Konfigurationen stellen globale Konfigurationen als endliche Überlagerungen deterministischer Konfigurationen dar; von daher besteht eine klare Parallele zum Begriff der globalen stochastischen Konfiguration. Es liegt daher nahe, für dieses Modell ähnliche Ansätze zu versuchen wie in Abschnitt 2.5.

Aus der in Abschnitt 2.5 eingeführten Metrik für stochastische Konfigurationen erhalten wir eine Pseudometrik für endliche Konfigurationen von QZA. Die Menge der endlichen Quanten-Konfigurationen bezeichnen wir mit $\mathcal{Q}_E$. Jedes $q \in \mathcal{Q}_E$ hat die Gestalt

$$\sum_{i=1}^{k} \alpha_i |c_i\rangle$$

für $k \in \mathbb{N}$ und $c_i \in Q_E^{\mathbb{Z}}$; es gilt

$$\sum_{i=1}^{k} |\alpha_i|^2 = 1.$$

Die c_i bilden eine Orthonormalbasis von $\mathcal{Q}_E$; messen wir q bezüglich dieser Basis, so erhalten wir c_i mit der Wahrscheinlichkeit $|\alpha_i|^2$. Definieren wir also d_Q unter Zuhilfenahme der Metrik d aus Abschnitt 2.5 durch

$$d_Q\left(\sum_{i=1}^{k} \alpha_i |c_i\rangle, \sum_{i=1}^{k} \beta_i |c_i\rangle\right) = d\left(\sum_{i=1}^{k} |\alpha_i|^2 c_i, \sum_{i=1}^{k} |\beta_i|^2 c_i\right),$$

so ist d_Q eine Pseudometrik auf $\mathcal{Q}_E$. Die Beweise für Symmetrie und Dreiecksungleichung folgen denen für d; das einzige Problem gibt es bei Konfigurationen, die sich nur in relativen Phasen unterscheiden. So ist $d_Q(\alpha|c_1\rangle + \beta|c_2\rangle, \alpha|c_1\rangle - \beta|c_2\rangle) = 0$, obwohl die beiden Konfigurationen nicht gleich sind. Dies ist insofern nicht schwerwiegend, als man solche Konfigurationen nicht durch projektive Messungen unterscheiden kann.

4.5.3 Metriken auf unendlichen Konfigurationen

Die Pseudometrik aus dem vorhergehenden Abschnitt ist ein Anfang, aber sie ist keine echte Metrik und man kann etwas Besseres finden. Im Gegensatz zu der Situation bei SZA verfügen wir bei QZA über eine brauchbare

Definition von globalen Konfigurationen, die sich nicht auf eine Wahrscheinlichkeitsverteilung oder Überlagerung endlich vieler deterministischer globaler Konfigurationen stützt. Beziehen wir unsere Metrik auf diesen Begriff von globaler Quanten-Konfiguration, so vermeiden wir die Kombination von Abstandsmaßen auf Wahrscheinlichkeitsverteilungen mit solchen auf deterministischen Konfigurationen, die das Auffinden einer Metrik in Abschnitt 2.5 erschwerten.

Es gibt diverse Topologien für $C^\star$-Algebren; auf die meisten von ihnen wollen wir hier nicht eingehen, denn zum Teil sind sie nicht metrisierbar und zum Teil passen sie nicht zu unseren Zwecken. Statt dessen verwenden wir als Ausgangspunkte die Spurmetrik aus Abschnitt 3.8 und die diskrete Metrik. Sie wenden wir auf endliche Observable an und erhalten dank der Definition globaler Konfigurationen mittels endlicher Observabler eine Metrik auf globalen Quanten-Konfigurationen.

Lemma 4.18
Sei d' eine Metrik auf beschränkten Observablen. Dann ist

$$d(\widehat{q},\widehat{p}) = \sum_{i\in\mathbb{N}} 2^{-i} d'(\widehat{q}[-i\ldots i],\widehat{p}[-i\ldots i]) \tag{4.17}$$

für $\widehat{q},\widehat{p}\in\mathcal{C}$ eine Metrik auf $\mathcal{C}$.

Beweis: Für $\widehat{q}=\widehat{p}$ folgt $\widehat{q}[-i\ldots i]=\widehat{p}[-i\ldots i]$ für alle $i\in\mathbb{N}$ und damit (da d' eine Metrik ist) $d(\widehat{q},\widehat{p})=0$. Sei $\widehat{q}\neq\widehat{p}$. Dann gibt es ein endliches Intervall von Zellen, auf dem sich $\widehat{q}$ und $\widehat{p}$ unterscheiden und demnach ein $k\in\mathbb{N}$, so dass das Intervall von $-k$ bis k dieses endliche Intervall enthält. Wegen $d'(\widehat{q}[-k\ldots k],\widehat{p}[-k\ldots k])>0$ ist dann auch $d(\widehat{q},\widehat{p})>0$.

Die Symmetrie $d(\widehat{q},\widehat{p}) = d(\widehat{p},\widehat{q})$ folgt ebenfalls daraus, dass d' eine Metrik ist.

Es bleibt zu zeigen, dass d die Dreiecksungleichung erfüllt. Es ist

$$\begin{aligned}
&\sum_{i\in\mathbb{N}} 2^{-i} d'(\widehat{q}[-i\dots i],\widehat{p}[-i\dots i]) + \sum_{i\in\mathbb{N}} 2^{-i} d'(\widehat{p}[-i\dots i],\widehat{r}[-i\dots i]) \\
&\quad = \sum_{i\in\mathbb{N}} 2^{-i}\left(d'(\widehat{q}[-i\dots i],\widehat{p}[-i\dots i]) + d'(\widehat{p}[-i\dots i],\widehat{r}[-i\dots i])\right) \\
&\quad \geq \sum_{i\in\mathbb{N}} 2^{-i} d'(\widehat{q}[-i\dots i],\widehat{r}[-i\dots i]) \\
&\quad = d(\widehat{q},\widehat{r}),
\end{aligned}$$

auch diese Eigenschaft ist folglich erfüllt, wenn d' eine Metrik ist. □

Für d' kann man zum Beispiel den Spurabstand aus Kapitel 3 einsetzen; einfach den Spurabstand der kompletten Konfigurationen als Metrik einzusetzen ist für unsere Zwecke nicht sinnvoll, weil es ausgesprochen schwierig ist, den Spurabstand unendlicher Operatoren abzuschätzen.

Einen Spezialfall erhalten wir, wenn wir für d' die diskrete Metrik δ einsetzen, also $\delta(a,b) = 1$ für $a \neq b$ und $\delta(a,a) = 0$ festlegen.

Lemma 4.19
Setzt man für d' den Spurabstand oder die diskrete Metrik ein, so erzeugt d auf den deterministischen globalen Konfigurationen eine Topologie, die zur Cantor-Topologie äquivalent ist.

Beweis: Auf deterministischen Konfigurationen fallen Spurabstand und diskrete Metrik zusammen. Der Dichteoperator eines deterministischen Zellzustandes ist nämlich eine Matrix, die an genau einer Stelle auf der Diagonalen eine 1 besitzt und sonst nur aus Nullen besteht. Folglich ist der Spurabstand von zwei solchen Zuständen 1, wenn sie verschieden und 0, wenn sie gleich sind.

Seien c, e deterministische globale Konfigurationen. Der Index der ersten Zelle, in der sie sich unterscheiden, sei k; ohne Beschränkung der Allgemeinheit sei $k > 0$.

Wir erhalten

$$d(c,e) = \sum_{i=0}^{\infty} 2^{-i}\delta(c[-i\dots i], e[-i\dots i]),$$

das heisst, $d(c,e) = d_C(c,e) + \sum_{i=k+1}^{\infty} 2^{-i}$. Aus $\sum_{i=0}^{\infty} 2^{-i} = 2$ folgt $d(c,e) = 2^{-k+1}$, also $d(c,e) = 2d_C(c,e)$. □

Lemma 4.20
Setzt man für d' die diskrete Metrik ein, so ist $(\mathcal{C}, d)$ vollständig, aber nicht kompakt.

Beweis: Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $\mathcal{C}$ mit der Metrik d. Dann gibt es zu jedem $\varepsilon > 0$ ein $n_\varepsilon \in \mathbb{N}$ so dass $d(x_i, x_{i+1}) < \varepsilon$ für alle $i \geq n_\varepsilon$. Daraus folgt, dass für alle x_i mit $i \geq n_\varepsilon$ der Zellblock von $-\log 1/\varepsilon$ bis $\log 1/\varepsilon$ gleich sein muss. Wir konstruieren einen Grenzwert, indem wir den Zustand des Blockes von $-k$ bis $+k$ durch den gemeinsamen Zustand dieses Blockes in den Folgengliedern ab $n_{2^{-k}}$ definieren. So erhalten wir einen Grenzwert von $(x_n)_{n\in\mathbb{N}}$; dieser muss (weil wir in einem metrischen Raum sind) eindeutig sein und ist ein Element von $\mathcal{C}$ (nach Konstruktion).

Wäre $(\mathcal{C}, d)$ kompakt, so müsste jede offene Überdeckung eine endliche Teilüberdeckung enthalten. Für $\rho \in \mathcal{B}(\mathcal{H})$ sei $U_\rho = \{\widehat{q} \in \mathcal{C} : \widehat{q}[0] = \rho\}$. Dann ist U_ρ offen, denn mit jedem $\widehat{q}$ ist auch eine ε-Umgebung von $\widehat{q}$ in U_ρ enthalten (sie besteht aus $\widehat{q}' \in \mathcal{C}$, die in Zelle 0 mit $\widehat{q}$ übereinstimmen). Außerdem ist $\bigcup_{\rho\in\mathcal{B}(\mathcal{H})} U_\rho = \mathcal{C}$, denn jedes Element von $\mathcal{C}$ muss in Zelle 0 einen Zustand aus $\mathcal{B}(\mathcal{H})$ annehmen.

Weil $\mathcal{B}(\mathcal{H})$ unendlich viele Elemente besitzt, muss jede endliche Teilüberdeckung einige U_ρ ausschließen. Dann kann sie aber keine Überdeckung mehr sein, weil dann Konfigurationen, in deren Mitte ρ steht, nicht mehr enthalten sind. □

4.5.4 Anwendungen

Fehlerabschätzung

Wir setzen unsere Metrik ein, um abzuschätzen, wie stark sich kleine Abweichungen von der Überführungsfunktion auswirken. Dazu gehen wir wie folgt vor. Wir betrachten zwei BQZA mit der gleichen Blockgröße N und dem gleichen Zustandsalphabet Q. Ohne Einschränkung sei $N = 3$ und

beide BQZA haben die gleiche Anzahl an Blocktransformationen, die mit den gleichen Ursprüngen arbeiten (falls dies nicht der Fall ist, füllt man mit identischen Blocktransformationen auf).

Wir nehmen nun an, die jeweils ersten Blocktransformationen B_1 und B_2 unterscheiden sich. Aus einem noch zu definierenden Maß für ihre Unterschiedlichkeit entwickeln wir eine Abschätzung für den maximalen Spurabstand von $B_1(\rho)$ und $B_2(\rho)$ über alle Blockzustände ρ. Daraus wiederum gewinnen wir eine Abschätzung für den Spurabstand von $B_1(\tau)$ und $B_2(\tau)$ für globale Konfigurationen τ.

Im Gegensatz zu Kapitel 2 verfügen wir hier nicht über eine Summendarstellung aus deterministischen ZA und müssen daher erst definieren, was wir unter ähnlichen Blocktransformationen verstehen.

Eine Möglichkeit besteht darin, an Untersuchungen zu verrauschten Quantenprozessen (zum Beispiel depolarisierende Kanäle) anzuknüpfen und eine verrauschte Blocktransformation als Superoperator

$$\mathcal{U}(\tau) = p\rho_0 + (1-p)U(\tau) \tag{4.18}$$

zu schreiben. Dabei ist p eine Zahl zwischen 0 und 1, die wir als Fehlerwahrscheinlichkeit auffassen und ρ_0 ist ein fest gewählter Dichteoperator. $\mathcal{U}$ verhält sich mit Wahrscheinlichkeit $(1-p)$ so wie die unitäre Abbildung U, mit Wahrscheinlichkeit p jedoch bildet er jede Eingabe auf ρ_0 ab.

Als weitere Möglichkeit untersuchen wir Paare U_1, U_2 von unitären Transformationen auf $\ell_2(Q)^N$, für die gilt:

$$\sup_{\rho \in \mathcal{B}(\ell_2(Q))^N} D(U_1(\rho), U_2(\rho)) \leq \varepsilon \tag{4.19}$$

für ein $\varepsilon > 0$, welches als Maß für den Unterschied zwischen U_1 und U_2 dienen soll. In Anbetracht der Interpretation von D als der Wahrscheinlichkeit, bei einer Messung einen Unterschied festzustellen, wenn man die dafür optimale Observable verwendet, beschreibt Gleichung 4.19 einen sinnvollen Begriff von der Ähnlichkeit zweier Blocktransformationen. Ein für die Anschauung nützlicher Spezialfall mit $|Q| = 2$ liegt für $U_2 = R_\theta \circ U_1$ vor, wobei R_θ für die Drehung um θ steht. Weil die Abschätzungen sehr schwierig werden, wenn man Gleichung 4.19 in ihrer vollen Allgemeinheit einsetzt,

beschränken wir uns auf eine Verallgemeinerung der Kombination mit einer Drehung und nehmen an, U_2 sei in der Form $R \circ U_1$ mit einer unitären Abbildung R darstellbar.

Es gibt einen klaren Unterschied zwischen diesen Abstandsbegriffen: der erste, in Gleichung 4.18 beschriebene, ersetzt die unitäre Blocktransformation U durch einen (wahrscheinlich nicht unitären) Superoperator $\mathcal{U}$. Das suggeriert eine extern verursachte Störung der Überführungsfunktion. Der zweite Begriff, aus Gleichung 4.19, geht von einer Störung aus, die sich als unitäre Transformation schreiben lässt; damit können wir zum Beispiel den Fall erfassen, dass wir die gewünschte Überführungsfunktion unvollkommen abgebildet haben, ohne dabei aber die Unitarität zu verletzen. Ein Beispiel hierfür wäre eine Situation, wo für die Überführungsfunktion eines QZA eine gewisse Menge an Amplituden einsetzen wollen, aber nicht alle von diesen Amplituden erzeugen können (weil zum Beispiel einige von ihnen nicht berechenbaren Zahlen entsprechen, oder weil sie mit einer Präzision bestimmt sind, die unsere Apparaturen nicht erreichen können). Wir würden dann wahrscheinlich eine Überführungsfunktion implementieren, die von der gewünschten abweicht, ohne dabei die Unitarität zu verlieren.

Was auch immer die Charakteristika und Ursachen einer Abweichung von der gewünschten Überführungsfunktion sein mögen, eine Abschätzung ihrer Konsequenzen ist offenbar wichtig. Dies ist ein komplexes Thema, das wir unmöglich in seiner vollen Breite behandeln können; wir geben aber erste Abschätzungen an.

Sei $\widehat{q}$ eine globale Konfiguration. Um der Übersichtlichkeit willen nehmen wir an, $\widehat{q}$ wäre als Tensorproduktzustand der Blockzustände bezüglich der ersten Blocktransformation darstellbar; ist dies nicht der Fall, können wir zumindest für endliche $\widehat{q}$ den Gesamtzustand als endliche Überlagerung solcher separabler Zustände darstellen. Ist $\widehat{q}$ unendlich, so beobachten wir, dass wegen der Definition unserer Metrik der Einfluss der weit draußen liegenden Blöcke exponentiell mit ihrer Entfernung vom Nullpunkt abnimmt, so dass wir für Abschätzungen alle Blöcke ab einem gewissen beliebig großen aber endlichen Index ignorieren und so τ durch eine endliche Konfiguration ersetzen (wir untersuchen hier nur die ersten paar Anwendungen von B_1 und B_2; wollten wir zum Beispiel Aussagen über das

Verhalten im zeitlichen Grenzwert machen, könnten wir diese Reduktion nicht vornehmen).

Wir erhalten dann

$$B_1(\widehat{q}) = B_1\left(\bigotimes_{i=-\infty}^{\infty} \rho_i\right) = \bigotimes_{i=-\infty}^{\infty} B_1(\rho_i)$$

und entsprechendes für B_2. Dabei steht ρ_i für den Zustand des i-ten Blockes. Wir schreiben $\rho_i[j]$ für den (reduzierten) Zustand der j-ten Zelle von Block i und erinnern uns, dass wir $N = 3$ vereinbart haben. Dann ist

$$\begin{aligned} d_S(B_1(\widehat{q}), B_2(\widehat{q})) &= D(B_1(\rho_0)[1], B_2(\rho_0)[1]) \\ &\quad + \frac{1}{2} D(B_1(\rho_{-1})[3] \otimes B_1(\rho_0)[1,2], B_2(\rho_{-1})[3] \otimes B_2(\rho_0)[1,2]) \\ &\quad + \frac{1}{4} D(B_1(\rho_{-1})[2,3] \otimes B_1(\rho_0), B_2(\rho_{-1})[2,3] \otimes B_2(\rho_0)) \\ &\quad + \frac{1}{8} D(B_1(\rho_{-1}) \otimes B_1(\rho_0) \otimes B_1(\rho_1)[1], \\ &\quad B_2(\rho_{-1}) \otimes B_2(\rho_0) \otimes B_2(\rho_1)[1]) \\ &\quad + \dots \end{aligned} \tag{4.20}$$

Um $d_S(B_1(\widehat{q}), B_2(\widehat{q})$ abschätzen zu können, müssen wir wissen, wie sich D auf Tensorprodukten verhält und was für den Abstand von Teilzuständen gilt, wenn der des Gesamtzustandes bekannt ist. Zunächst gilt für D: Partielle Spurbildung kann den Abstand nie vergrößern. Das heißt, aus $D(\rho, \rho') = x$ folgt für jedes Teilsystem A: $D(\mathrm{tr}_A(\rho), \mathrm{tr}_A(\rho')) \leq x$. Damit ist insbesondere $D(B_1(\rho_i)[j], B_2(\rho_i)[j]) \leq D(B_1(\rho_i), B_2(\rho_i)$ für alle $i \in \mathbb{Z}$ und $1 \leq j \leq N$.

Für den Spurabstand $D(\mathcal{U}(\rho), U(\rho))$ gilt nach Gleichung 3.31

$$\begin{aligned} D(\mathcal{U})(\rho), U(\rho)) &= D((p\rho_0 + (1-p)U(\rho)), U(\rho)) \\ &\leq p + pD(\rho_0, U(\rho)) \\ &\leq 2p, \end{aligned}$$

wobei wir $D(\rho_0, U(\rho))$ nach oben durch 1 abgeschätzt haben. Ohne bessere Kenntnis von ρ_0 und U können wir diese Abschätzung nicht verfeinern.

Für Paare (ρ_i, ρ_{i+1}) von Blöcken erhalten wir entsprechend

$$\begin{aligned}
D(U(\rho_i) \otimes U(\rho_{i+1}), U'(\rho_i) \otimes U'(\rho_{i+1})) = D(U(\rho_i) \otimes U(\rho_{i+1}), & p^2(\rho_0 \otimes \rho_0) + \\
& p(1-p)(\rho_0 \otimes U(\rho_{i+1})) + \\
& (1-p)p(U(\rho_i) \otimes \rho_0) + \\
& (1-p)^2(U(\rho_i) \otimes U(\rho_{i+1}))) \\
& \leq 2p - p^2 + \\
& p^2 D(U(\rho_i) \otimes U(\rho_{i+1}), \rho_0 \otimes \rho_0) + \\
& p(1-p)D(U(\rho_i), \rho_0) + \\
& (1-p)pD(U(\rho_{i+1}), \rho_0) \\
& \leq 4p - 2p^2 = 2(1-(1-p)^2).
\end{aligned}$$

Induktiv erhält man für k Blöcke als obere Schranke $k(1-(1-p)^k)$. Die Nützlichkeit dieser Abschätzung lässt für große k stark nach. Genauer können wir sie aber ohne Kenntnis von U und ρ_0 nicht machen. Der Ansatz über verrauschte Operatoren scheint daher für QZA weniger geeignet zu sein, weil bei der parallelen Anwendung auf mehrere Blöcke die obere Schranke so ungenau wird, dass sie bald jede Bedeutung verliert.

Für den Abstandsbegriff nach Gleichung 4.19 gilt gemäß der Definition $D(B_1(\rho), B_2(\rho)) \leq \varepsilon$. Seien insbesondere B_1 und B_2 durch eine unitäre Abbildung R unterschieden. Für einen beliebigen reinen Zustand ρ aus $\mathcal{B}(\ell(Q))^N$ berechnen wir $D(B_1(\rho), B_2(\rho))$. Sei U die unitäre Transformation zu B_1. Dann ist $D(B_1(\rho), B_2(\rho)) = D(U(\rho), R \circ U(\rho)) = D(\rho, R(\rho))$; die letzte Gleichung gilt, weil D unter unitären Transformationen invariant ist. Im Spezialfall $R = R_\theta$ gilt $D(\rho, R_\theta(\rho)) = |\sin\theta|$ [66].

Für Tensorproduktzustände $\rho_1 \otimes \rho_2$ mit $\rho_1, \rho_2 \in \mathcal{B}(\ell(Q))^N$ gilt wegen der Dreiecksungleichung

$$\begin{aligned}
& D(\rho_1 \otimes \rho_2, R(\rho_1 \otimes \rho_2)) \\
& \quad = D(\rho_1 \otimes \rho_2, R(\rho_1) \otimes R(\rho_2)) \\
& \quad \leq D(\rho_1 \otimes \rho_2, R(\rho_1) \otimes \rho_2) + D(R_\theta(\rho_1) \otimes \rho_2, R(\rho_1) \otimes R(\rho_2)).
\end{aligned}$$

Nun kann Tensorierung beider Teile mit ρ_2 nicht zur Unterscheidbarkeit von

ρ_1 und $R(\rho_1)$ beitragen. Folglich können wir die Abschätzung fortsetzen:

$$\begin{aligned} &D(\rho_1 \otimes \rho_2 R(\rho_1 \otimes \rho_2)) \\ &\quad \leq D(\rho_1, R_\theta(\rho_1)) + D(\rho_2, R_\theta(\rho_2)) \\ &\quad = 2\varepsilon. \end{aligned}$$

Entsprechend gilt eine obere Schranke von $k\varepsilon$, wenn wir Tensorprodukte aus k Blöcken betrachten.

Eingesetzt in Gleichung 4.20 ergibt sich für den Gesamtabstand

$$\begin{aligned} d_S(B_1(\tau), B_2(\tau)) &\leq \varepsilon + 2\sum_{i=2}^{\infty} i\varepsilon 2^{-i} \\ &= \varepsilon + 3\varepsilon = 4\varepsilon, \end{aligned} \tag{4.21}$$

was noch eine relativ grobe Abschätzung ist, aber für unsere Zwecke genügt.

Nun führen wir die zweite Blocktransformation mit der unitären Abbildung V beziehungsweise $R' \circ V$ durch. Hier haben wir als Eingaben Blöcke, die durch partielle Spurbildung aus den Zuständen von Paaren von Blöcken bezüglich der ersten Blocktransformation entstehen. Wir verwenden σ_i für den i-ten Block von $B_1(\tau)$ und σ'_i für den i-ten Block von $B_2(\tau)$. Dann ist $D(\sigma_i, \sigma'_i) \leq 2\varepsilon$ für alle $i \in \mathbb{Z}$. Folglich ist

$$\begin{aligned} D(V(\sigma_i), R' \circ V(\sigma'_i)) &\leq D(\sigma_i, R'(\sigma'_i)) \\ &\leq D(\sigma_i, \sigma'_i) + D(\sigma'_i, R'(\sigma'_i)) \\ &\leq 3\varepsilon. \end{aligned}$$

Daraus erhalten wir für den Unterschied zwischen den globalen Konfigurationen nach Anwendung der zweiten Blocktransformation eine obere Schranke von 9ε.

Man kann sehen, dass bei einer Anwendung des gestörten BQZA der Unterschied zum ungestörten BQZA noch relativ klein bleibt – er ist ein Vielfaches von ε. Bei mehrfacher Anwendung des BQZA wird die Abschätzung allerdings viel schwieriger, weil gewisse Annahmen über die Separabilität der Eingaben dann nicht mehr gelten. Es ist zu vermuten, dass die Abweichung dann ähnlich schnell wächst wie die für stochastische ZA aus Abschnitt 2.5.6; ein Beweis ist allerdings bis jetzt nicht gelungen.

Es ist bei QZA auch möglich, dass Fehler mit der Zeit oszillieren. Ein einfaches Beispiel ist ein BQZA mit nur einer Blocktransformation, die durch eine Drehung gestört ist. Nach k Anwendungen des BQZA ist die Abweichung in jedem Block gerade $|\sin k\theta|$.

Insgesamt haben wir gezeigt, wie man die Ähnlichkeit von BQZA definieren kann. Für die Definition über das Supremum der Spurabstände (Ungleichung 4.19) lässt sich die Auswirkung auf globale Konfigurationen für eine Anwendung der BQZA einigermaßen abschätzen; wie sich die Unterschiede bei der weiteren Rechnung bemerkbar machen, ist jedoch unklar. Obwohl es möglich ist, dass der Abstand der globalen Konfigurationen oszilliert, ist doch zu befürchten, dass im Allgemeinen durch die parallele Anwendung der gestörten Überführungsfunktion auf viele Zellen der Fehler mit der Zeit ähnlich groß wird wie bei SZA.

Da andererseits bekannt ist, dass eine Quantenturingmaschine eine andere mit beliebiger Genauigkeit simulieren kann, deren Überführungsfunktion sich von der eigenen nur wenig unterscheidet [7] und QZA solche Quantenturingmaschinen simulieren können, können QZA in diesem Sinn durchaus Abweichungen ausgleichen; aber dies ist eben nur für die sequentielle Rechnung gezeigt.

Über eine topologische Charakterisierung der QZA

Für deterministische ZA gilt ein Charakterisierungssatz von Hedlund [37]. Er besagt, dass eine Selbstabbildung des Raumes der globalen Konfigurationen genau dann die globale Überführungsfunktion eines ZA ist, wenn sie mit der Verschiebung kommutiert und bezüglich der Cantor-Topologie stetig ist. Man könnte nun vermuten, dass eine entsprechende Aussage auch für QZA gelte; wir zeigen, an welcher Stelle der Beweis einer solchen Aussage in möglicherweise unüberwindliche Schwierigkeiten gerät. Wir verwenden die Metrik von oben und setzen dabei die diskrete Metrik auf Observablen ein.

Wir zeigen zunächst, dass QZA stetig sind, indem wir zeigen, dass Blocktransformationen stetig sind. Seien dazu $\widehat{q}, \widehat{p}$ globale Konfigurationen mit $d(\widehat{q}, \widehat{p}) \leq \varepsilon$ für ein beliebig aber fest gewähltes $\varepsilon > 0$; das heißt, die

reduzierten Dichteoperatoren unterscheiden sich zum ersten Mal bei Zelle $\pm \log \varepsilon^{-1}$. Wenden wir hierauf eine Blocktransformation mit der Blockgröße N an, so können sich die resultierenden globalen Konfigurationen frühestens bei der Zelle $\log \varepsilon^{-1} - N + 1$ beziehungsweise $-\log \varepsilon^{-1} + N - 1$ unterscheiden (das tritt ein, wenn Zelle $\pm \log \varepsilon^{-1}$ genau am rechten beziehungsweise linken Rand eines Blockes liegt). Bezeichnen wir die globale Abbildung zu unserer Blocktransformation mit Φ, so folgt $d(\Phi(\widehat{q}), \Phi(\widehat{p})) \leq 2^{N-1} d(\widehat{q}, \widehat{p})$, das heisst, der Abstand wächst höchstens um einen konstanten Faktor; damit sind QZA sogar gleichmäßig stetig.

Da ein BQZA aus endlich vielen Blocktransformationen besteht, ist er als Hintereinanderausführung endlich vieler stetiger Funktionen selbst stetig.

Blocktransformationen kommutieren nicht mit der Verschiebung, aber immerhin mit der N-ten Potenz der Verschiebung, wobei N die Blockgröße ist. Wir können sie daher mit normalen ZA simulieren, indem wir wie im Beweis von Lemma 4.17 jeden Block der ersten Partitionierung als eine Zelle auffassen; dies ändert nichts an der Stetigkeit. Dass QZA mit der Verschiebung kommutieren, wissen wir aus Lemma 4.7.

Sei nun Φ eine Selbstabbildung des Raums der globalen Quanten-Konfigurationen, die gleichmäßig stetig ist und mit der Verschiebung kommutiert. Wir entwickeln einen QZA mit der globalen Überführungsfunktion Φ; dabei orientieren wir uns zunächst am Beweis der entsprechenden Behauptung für deterministische ZA von Curtis, Hedlund und Lyndon [37].

Für $\rho \in \mathcal{B}(\mathcal{H})$ sei wie im Beweis zu Lemma 4.20 $U_\rho = \{\widehat{q} \in \mathcal{C} : \widehat{q}[0] = \rho\}$. Jede der Mengen U_ρ ist offen und abgeschlossen; sie sind offen, weil sie mit jedem $\widehat{q}$ auch eine ε-Umgebung von $\widehat{q}$ enthalten. Sie sind abgeschlossen, weil ihr Komplement als Vereinigung offener Mengen offen ist.

Definieren wir nun für ein stetiges, unitäres und mit der Verschiebung kommutierendes $\Phi : \mathcal{C} \to \mathcal{C}$ die Mengen V_ρ durch $\Phi^{-1}(U_\rho)$. Weil Φ stetig ist, sind alle V_ρ offen und abgeschlossen. Außerdem gilt $V_\rho \cap V_\tau = U_\rho \cap U_\tau = \emptyset$ für $\rho \neq \tau$, sowie $\bigcup_{\rho \in \mathcal{B}(\mathcal{H})} U_\rho = \bigcup_{\rho \in \mathcal{B}(\mathcal{H})} V_\rho = \mathcal{C}$.

Zu $\rho \neq \tau$ gibt es ein $k \in \mathbb{N}$, so dass für alle $x \in V_\rho$ und $y \in V_\tau$ gilt: $d(x, y) \geq 2^{-k}$. Wenn es nämlich kein solches k gäbe, könnte man eine Folge in V_ρ finden, deren Grenzwert in V_τ läge. Damit wäre dann aber entweder

V_ρ nicht abgeschlossen oder V_ρ und V_τ nicht disjunkt.

Wir erhalten daher ein k für jedes Paar ρ, τ. Nehmen wir an, es gebe unendlich viele k. Dann existieren für jedes solche k globale Konfigurationen $\widehat{q}, \widehat{p}$ mit $d(\widehat{q}, \widehat{p}) < 2^{-k}$ und $d(\Phi(\widehat{q}), \Phi(\widehat{p})) = 2$, so dass Φ nicht stetig wäre. Es kann daher nur endlich viele verschiedene k geben, unter denen wir ein Maximum auswählen.

Sei B_ρ die Menge aller Blöcke der Länge $2k+1$, die zentral in V_ρ vorkommen. Für $A \in B_\rho$ definieren wir $\varphi(A) = \rho$. Damit erhält man Funktionswerte von φ auf allen möglichen Blöcken der Länge $2k+1$ und es bleibt zu zeigen, dass φ die Bedingungen an eine lokale Überführungsfunktion eines van Dam-QZA erfüllt. Dies ist jedoch alles andere als offensichtlich, denn wir kennen zwar das Verhalten von φ auf allen $A \in B_\rho$ für alle ρ, aber es ist nicht klar, dass wir immer eine gemeinsame Basis der A finden können, so dass die Werte, die φ auf den Basiselementen annimmt, rein sind. Dies müssten wir aber, um einen QZA zu erhalten.

4.5.5 Zusammenfassung

Die Definition von globalen Quanten-Konfigurationen über Elemente der quasilokalen Algebra erleichtert die Definition einer brauchbaren Metrik. Genauer erhalten wir sogar eine Familie von Metriken, denn jede Metrik auf beschränkten Observablen induziert eine Metrik, wenn man sie in Gleichung 4.17 einsetzt.

Der Versuch, diese Metrik dazu einzusetzen, die Auswirkungen von kleinen Störungen an der Überführungsfunktion abzuschätzen, hat sich als schwierig herausgestellt. Immerhin ist es gelungen, für die erste Iteration eine obere Schranke für die Abweichung herzuleiten.

Wegen der Konstruktion globaler Konfigurationen als Grenzwerte, die mit der Konstruktion unendlicher klassischer Konfigurationen vergleichbar ist, können wir für Quanten-Konfigurationen Metriken definieren, die Ähnlichkeit mit der Cantor-Metrik besitzen.

4.6 Entwicklung von Verschränkung

4.6.1 Einleitung

Einer der Nachteile der Modelle von Watrous und van Dam ist das Wachstum der Anzahl Summanden, die an der globalen Konfiguration beteiligt sind. Die Schreibweise mittels lokaler Operatoren macht globale Konfigurationen leichter handhabbar; ganz kann sie das Problem jedoch nicht lösen, denn hier äußert sich gerade die Eigenschaft, die Quantensysteme mit klassischen Mitteln so schwer modellierbar macht und daher die mögliche Überlegenheit von Quantenrechnern bewirkt.

Schwierigkeiten bei der Beschreibung globaler Konfigurationen äußern sich dahingehend, dass durch die Zustände von Blöcken von Zellen bis zu einer festen Länge k die globale Quanten-Konfiguration nicht eindeutig festgelegt ist. Die Zustände der Blöcke sind durch reduzierte Dichteoperatoren beschrieben; diese heißen deswegen reduziert, weil sie nicht die volle Information über das Gesamtsystem tragen. Beim Ausspuren geht zwangsläufig Information verloren, nämlich solche, die sich auf die Verschränktheit mit Zellen des ausgespurten Teilsystems bezieht.

Daher wird die globale Beschreibung um so aufwändiger, je mehr und über je größere Distanzen hinweg Zellen in unserem System verschränkt sind. QZA unterscheiden sich darin, wie viel Verschränkung sie erzeugen. Dies zu untersuchen ist auch deswegen interessant, weil man Verschränkung als eine Ressource betrachten kann. Auf dieser Idee basiert der Einweg-Quantenrechner von Raussendorf und Briegel [72].

4.6.2 Lokal beschreibbare Konfigurationen

Kennen wir von einer globalen Quanten-Konfiguration nur die Blockzustände bis zu einer festen Blocklänge k, so ist die globale Konfiguration damit nicht eindeutig bestimmt. Als Beispiel betrachten wir ein System aus vier qubits, das sich in dem Zustand $(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)/2$ befindet. Mittels partieller Spurbildung erhalten wir für jedes einzelne qubit

die gleiche reduzierte Dichtematrix, nämlich

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}.$$

Die gleichen reduzierten Dichtematrizen für die einzelnen qubits erhalten wir auch aus dem Zustand $(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)/2$. Eine globale Konfiguration, die ein Tensorprodukt aus solchen Vier-qubit-Systemen wäre, könnte man also allein auf Basis der Zustände der einzelnen qubits nicht eindeutig identifizieren.

Es gibt jedoch Situationen, in denen der Gesamtzustand durch die reduzierten Dichtematrizen von einigen Teilzuständen bereits eindeutig festgelegt ist. Ein Beispiel hierfür sind Tensorproduktzustände; befindet sich ein bipartites System im Zustand $|\varphi\rangle \otimes |\psi\rangle$, so sind die reduzierten Dichteoperatoren der einzelnen Teile gerade $|\varphi\rangle\langle\varphi|$ und $|\psi\rangle\langle\psi|$ und enthalten die volle Information über den Systemzustand. Entsprechendes gilt für Systeme aus mehr Teilen.

Im Allgemeinen befinden sich die Zellen eines QZA nach einigen Anwendungen der globalen Überführungsfunktion nicht in einem Tensorproduktzustand; zumindest einige Zellen sind miteinander verschränkt. Wenn wir von einer vollständig unverschränkten Anfangskonfiguration ausgehen, müssen wir also damit rechnen, dass die Anwendung eines QZA die Beschreibung der Ergebniskonfiguration erschwert. Andererseits kann bei Anwendung auf eine verschränkte Anfangskonfiguration die Beschreibung auch erleichtert werden. Schließlich sind QZA reversibel; wenn einer von ihnen Verschränkung erzeugt, wird seine Inverse sie wieder reduzieren.

Wir untersuchen verschiedene QZA darauf hin, ob sie überhaupt Verschränkung erzeugen und ob es eine obere Schranke für den Abstand von Zellen gibt, die durch die Aktion des QZA mit der Zeit miteinander verschränkt werden.

4.6.3 Entwicklung von Verschränkung

Wir wollen QZA darauf hin untersuchen, wie sie die Verschränkung globaler Konfigurationen verändern. Dazu müssen wir diese Veränderung quantifi-

zieren. Zu diesem Zweck betrachten wir globale Konfigurationen, die in dem folgenden Sinn raumperiodisch sind.

Sei a eine globale Konfiguration, die als unendliches Tensorprodukt $\ldots\otimes \rho_{i-1}\otimes\rho_i\otimes\rho_{i+1}\otimes\ldots$ darstellbar ist. Dabei steht ρ_j jeweils für den Zustand eines Blocks der festen Länge k. Wir nennen a periodisch (mit der Periode l), wenn für alle j gilt: $\rho_j = \rho_{j+l}$.

Auf a wenden wir nun eine Blocktransformation B an. Ohne Einschränkung setzen wir für diese Blocktransformation eine Blockgröße $N \leq k$ voraus. Wir könnten nun so vorgehen, dass wir für jedes Paar von Blöcken die Schmidt-Zahl nach Anwendung von B berechnen; weil die Blockgrenzen von a aber nicht die von B sein müssen, würden wir dann die Schmidt-Zahlen von gemischten Zuständen berechnen. Wir vereinfachen daher die Vorgehensweise, indem wir eine zirkuläre Anwendung von B definieren.

Definition 4.10 (Zirkuläre Blocktransformation)
Seien $B = (N, Q, \varphi)$ eine Blocktransformation und ρ_1, ρ_2 Dichtematrizen reiner Quantenzustände von Blöcken der Länge N; das heißt, jeder Block besteht aus N Zellen, die jeweils einen Zustand über einem zu $\mathcal{H} = \ell_2(Q)$ isomorphen Hilbertraum einnehmen. Wir setzen $\rho = \rho_1 \otimes \rho_2$. Für $1 \leq i < k \leq 2N$ bezeichne $\rho[i \ldots k]$ die reduzierte Dichtematrix, die den Zustand der i-ten bis k-ten Zelle in ρ beschreibt.

Eine zirkuläre Anwendung von B auf $\rho_1 \otimes \rho_2$ mit Ursprung $1 \leq i < N$ ist durch

$$\varphi_z(\rho) = \varphi(\rho[i \ldots N+i]) \otimes \varphi(\rho[N+i+1 \bmod 2N \ldots 2N+i+1 \bmod 2N])$$

gegeben. Anders ausgedrückt erhalten wir φ_z für den Ursprung i, indem wir die Nte Potenz der zirkulanten Matrix mit der Identität auf $\mathcal{H}$ tensorieren und dann mit $\varphi \otimes \varphi$ multiplizieren.

Da zirkulante Matrizen als Permutationsmatrizen unitär sind, ist die zirkuläre Anwendung einer unitären Blocktransformation selbst unitär. Damit sind zirkuläre Blocktransformationen ganz ähnlich wie die periodischen Anwendungen der lokalen Überführungsfunktion bei van Dam definiert. Wir verwenden diese Definition, um die Entwicklung der Verschränktheit in einem endlichen System zu untersuchen. Damit ist sichergestellt, dass

wir bei jeder zirkulären Anwendung von B einen reinen Zustand erhalten, wenn wir mit einem reinen Zustand anfangen (denn unitäre Transformationen ändern den Mischungsgrad nicht). Da wir erst einmal nur an der prinzipiellen Fähigkeit von QZA zur Erzeugung von Verschränkung interessiert sind, ist eine solche Beschränkung auf periodische Konfigurationen zunächst sinnvoll.

Offenbar werden ρ_1 und ρ_2 nicht verschränkt, wenn man die zirkuläre Blocktransformation mit Ursprung 1 anwendet, denn dann findet keine Interaktion zwischen den Teilen statt.

Verschiebung

Einen weiteren einfachen Fall erhält man aus der Verschiebung. Zirkulär angewandt wird aus einer Verschiebung oder partiellen Verschiebung eine Permutation.

Der Ausgangszustand sei $\rho_1 \otimes \rho_2$ mit reinen Zuständen $\rho_1 = |\varphi\rangle\langle\varphi|$, $\rho_2 = |\psi\rangle\langle\psi|$ und $|\varphi\rangle = \alpha_{00}|00\rangle_A + \alpha_{01}|01\rangle_A + \alpha_{10}|10\rangle_A + \alpha_{11}|11\rangle_A$ sowie $|\psi\rangle = \beta_{00}|00\rangle_B + \beta_{01}|01\rangle_B + \beta_{10}|10\rangle_B + \beta_{11}|11\rangle_B$.

Für eine Verschiebung gibt es nun im Wesentlichen zwei Möglichkeiten: Entweder es werden alle Zellen um den gleichen Betrag verschoben oder es nehmen nicht alle Zellen an der Verschiebung teil. Beispiele für entsprechende Matrizen sind

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

(Diese Matrizen operieren nur auf zwei qubits; die entsprechenden Matrizen für vier qubits erhält man analog.) Sind $|\varphi\rangle$ und $|\psi\rangle$ selbst separabel, so kann durch Anwendung solcher Verschiebungen keine Verschränkung entstehen. Nur wenn mindestens einer der beiden Vektoren schon zu Beginn verschränkt ist, kann nach Anwendung der Verschiebung der erste Block mit dem zweiten verschränkt sein. Dabei ist an sich keine neue Verschränkung entstanden, sondern nur die bestehende verlagert worden.

Verschränkung durch „echte“ Interaktion

Die Blocktransformation mit Blocklänge zwei und der Überführungsfunktion, die durch die unitäre Matrix U_{cnot} gegeben ist, erzeugt mit Ursprung 1 auf dem Ausgangszustand $\rho_1 \otimes \rho_2$ auch dann Verschränkung, wenn die einzelnen Blöcke zu Beginn separabel sind.

Zirkuläre Anwendung von U_{cnot} mit Ursprung 1 überführt den Ausgangszustand $\rho_1 \otimes \rho_2$ in

$$\begin{aligned}
&\alpha_{00}\beta_{00}|00\rangle_A|00\rangle_B + \alpha_{10}\beta_{01}|00\rangle_A|01\rangle_B + \alpha_{00}\beta_{10}|00\rangle_A|10\rangle_B \\
&+ \alpha_{10}\beta_{11}|00\rangle_A|11\rangle_B + \alpha_{01}\beta_{10}|01\rangle_A|00\rangle_B + \alpha_{11}\beta_{11}|01\rangle_A|01\rangle_B \\
&+ \alpha_{01}\beta_{00}|01\rangle_A|10\rangle_B + \alpha_{11}\beta_{01}|01\rangle_A|11\rangle_B + \alpha_{10}\beta_{00}|10\rangle_A|00\rangle_B \\
&+ \alpha_{00}\beta_{01}|10\rangle_A|01\rangle_B + \alpha_{10}\beta_{10}|10\rangle_A|10\rangle_B + \alpha_{00}\beta_{11}|10\rangle_A|11\rangle_B \\
&+ \alpha_{11}\beta_{10}|11\rangle_A|00\rangle_B + \alpha_{01}\beta_{11}|11\rangle_A|01\rangle_B + \alpha_{11}\beta_{00}|11\rangle_A|10\rangle_B \\
&+ \alpha_{01}\beta_{01}|11\rangle_A|11\rangle_B.
\end{aligned}$$

Daraus erhalten wir

$$\begin{aligned}
&|00\rangle_A\,(\alpha_{00}\beta_{00}|00\rangle_B + \alpha_{10}\beta_{01}|01\rangle_B + \alpha_{00}\beta_{10}|10\rangle_B + \alpha_{10}\beta_{11}|11\rangle_B) \\
&+ |01\rangle_A\,(\alpha_{01}\beta_{10}|00\rangle_B + \alpha_{11}\beta_{11}|01\rangle_B + \alpha_{01}\beta_{00}|10\rangle_B + \alpha_{11}\beta_{01}|11\rangle_B) \\
&+ |10\rangle_A\,(\alpha_{10}\beta_{00}|00\rangle_B + \alpha_{00}\beta_{01}|01\rangle_B + \alpha_{10}\beta_{10}|10\rangle_B + \alpha_{00}\beta_{11}|11\rangle_B) \\
&+ |11\rangle_A\,(\alpha_{11}\beta_{10}|00\rangle_B + \alpha_{01}\beta_{10}|01\rangle_B + \alpha_{11}\beta_{00}|10\rangle_B + \alpha_{01}\beta_{01}|11\rangle_B)\,,
\end{aligned}$$

also eine Schmidt-Zahl von vier. Wiederholte Anwendung von U_{cnot} mit dem gleichen Ursprung lässt die Verschränkung oszillieren, weil U_{cnot} zu sich selbst invers ist. Verwendet man beim zweiten Mal den Ursprung 2 oder 4, so bleibt die Schmidt-Zahl vier erhalten. Dies gilt auch dann, wenn φ und ψ separabel sind. Damit erhalten wir einen Unterschied im Verhalten der Verschiebung im Vergleich zu U_{cnot}.

In unserem Beispiel muss sich allerdings nach spätestens $16!$ Anwendungen von U_{cnot} der Originalzustand mit Schmidt-Zahl eins wieder einstellen. Das liegt daran, dass wir nur die Verschränkung auf einem endlichen System betrachten. Um zu demonstrieren, dass es bei unendlichen Systemen mehr Möglichkeiten gibt, betrachten wir den folgenden BQZA A.

$$
\begin{array}{lcl}
|a,x,i,y\rangle & \mapsto & |i,x,a,x\oplus y\rangle \\
|a,x,a,y\rangle & \mapsto & |a,x,a,y\rangle \\
|i,x,i,y\rangle & \mapsto & |i,x,i,y\rangle \\
|i,x,a,y\rangle & \mapsto & |a,x,i,y\rangle
\end{array}
$$

Tabelle 4.1: Tabelle zum BQZA A

Er besteht aus zwei Blocktransformationen der Blocklänge N. Jede Zelle enthält zwei qubits, von denen das eine angibt, ob die Zelle aktiv ist. Seine Zustandsmenge ist $\{a,i\}$. Als Variablen für den Zustand des zweiten qubits verwenden wir x und y.

Beide Blocktransformationen verwenden die gleiche Überführungsfunktion, die durch Tabelle 4.1 definiert ist. Dabei steht $x\oplus y$ für das Exklusiv-Oder von x und y; auf den zweiten qubits der Blöcke verhält sich die Blocktransformation wie U_{cnot}. Der Ursprung der ersten Blocktransformation ist 0, der der zweiten 1. Wir zeigen an einem Beispiel die Wirkung von A:

$$
\begin{array}{cccccccccc}
 & i & i & a & i & i & i & i & i & \\
\ldots & x_{-1} & x_0 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & \ldots \\
 & i & i & i & a & i & i & i & i & \\
\ldots & x_{-1} & x_0 & x_1 & x_1\oplus x_2 & x_3 & x_4 & x_5 & x_6 & \ldots \\
 & i & i & i & i & a & i & i & i & \\
\ldots & x_{-1} & x_0 & x_1 & x_1\oplus x_2 & x_1\oplus x_2\oplus x_3 & x_4 & x_5 & x_6 & \ldots
\end{array}
$$

Nach dem k-ten Schritt ist für $1\le l\le k$ das zweite qubit der l-ten Zelle im Zustand $\bigoplus_{n=1}^{l} x_n$. Es ist mit den zweiten qubits der Zellen 1 bis $l-1$ verschränkt. Es handelt sich hier um einen ähnlichen QZA wie in dem zirkulären Beispiel vorhin. Zwischen nebeneinander liegenden Blöcken wird wieder nur begrenzt viel Verschränkung erzeugt. Da das System jetzt aber unendlich viele Zellen enthält, wird die Entwicklung nicht periodisch. Insbesondere kann eine Zelle durch die Aktion von A mit einer beliebig weit entfernt liegenden weiteren Zelle verschränkt werden, ohne dass dabei (wie bei der Verschiebung) an anderer Stelle Verschränkung abgebaut werden müsste.

Zusammenfassend können wir verschiedenes Verhalten hinsichtlich der Verschränkung beobachten:

1. Einige QZA erzeugen gar keine Verschränkung. Hierzu gehört die identische Abbildung. Auch die Verschiebung erzeugt keine Verschränkung, sondern verlagert sie allenfalls.

2. Einige weitere QZA erzeugen Verschränkung, diese breitet sich aber nicht über einen festen Radius hinaus aus. Beispiele hierzu sind zeitperiodische QZA, bei denen sich jede Konfiguration nach einer Zahl k von Iterationen wiederholt.

3. Schließlich gibt es QZA wie den aus dem letzten Beispiel, die mit der Zeit Verschränkung über unbegrenzte Distanzen hinweg erzeugen können.

Diese Aufzählung erinnert in mancher Hinsicht an die Beschreibung der ersten drei Klassen von ZA nach Wolfram. Ein entscheidender Unterschied ist allerdings, dass bei uns die Verschiebung ganz eindeutig in die erste Klasse gehört, während sie im klassischen Fall als chaotisch bezeichnet wird. Das liegt daran, dass Verschränkung nur durch Interaktion entstehen kann. Wenn man die Erzeugung von Verschränkung bewertet, macht man eine Aussage darüber, wie viel Interaktion stattfindet; ein QZA kann nur dann viel Verschränkung erzeugen, wenn seine Zellen miteinander interagieren.

Die Verschiebung aber bewirkt keine echte Interaktion. Klassische Klassifikationsverfahren beachten dies jedoch nicht; sie unterscheiden meist nicht zwischen der Bewegung und der Verarbeitung von Information.

4.6.4 Zusammenfassung

Globale Konfigurationen lokal zu beschreiben ist um so schwieriger, je mehr Zellen miteinander über große Entfernungen hinweg verschränkt sind. QZA unterscheiden sich darin, wie viel Verschränkung sie aufbauen. Man kann dies zum Beispiel als ein Klassifikationskriterium für QZA einsetzen; es kann eine Klassifikation nach der Komplexität der erzeugten Raum-Zeit-Diagramme, wie sie bei klassischen ZA vorgenommen wird [30, 52, 74, 86], ergänzen.

Die üblichen Klassifikationen von ZA messen eigentlich, wie schnell sich Information *bewegt*. Deshalb können sie nicht zwischen der Verschiebung und komplexeren ZA unterscheiden – sie messen nicht Komplexität im Sinne von Veränderung, die durch die Interaktion von Zellen entsteht. Verschränkung aber entsteht nicht durch die bloße Bewegung von Information, sie entsteht durch Interaktion. Von daher ist dies ein durchaus interessantes Komplexitätsmaß.

Die Erzeugung von Verschränkung ist aber auch für Rechnungen wichtig. Einerseits, weil Verschränkung als Ressource verwendet werden kann. Ein Beispiel hierfür ist der Einweg-Rechner von Raussendorf und Briegel, für den es wichtig ist, möglichst viel Verschränkung erzeugen zu können (weil sie während der anschließenden eigentlichen Rechnung schrittweise verbraucht wird).

4.7 Zusammenfassung

Nach einem Überblick über die existierenden Definitionen von QZA haben wir in diesem Kapitel ein neuartiges Modell vorgestellt. Es weicht von allen bisherigen darin ab, dass es sich aus einem operatoralgebraischen Begriff von Zustand und Konfiguration herleitet. Dies ermöglicht eine echt lokale Beschreibung von Zuständen und damit eine lokale Formulierung der Überführungsfunktion auf beliebigen (auch gemischten) Zuständen.

Neben einer Vereinfachung der Beschreibung von Konfigurationen ermöglicht dieses Modell auch eine lückenlose Erweiterung auf unendliche Konfigurationen, was vorher nicht möglich war. Darüber hinaus konnten wir zeigen, dass unser Modell in der Lage ist, diejenigen von Watrous und van Dam zu simulieren. Man kann ihre Definitionen auch auf operatoralgebraische Konfigurationen übertragen und erhält jeweils eine zu der unseren äquivalente Definition.

Für unseren Konfigurationenbegriff haben wir Metriken untersucht. Dabei stützen wir uns vor allem auf die Spurdistanz. Eine mögliche Anwendung ist wieder der Vergleich des globalen Verhaltens von QZA, deren lokale Überführungsfunktionen in einem genau definierten Sinn ähnlich sind. Hier konnten erste Ergebnisse gezeigt werden; an dieser Stelle öffnet sich

ein Weg zu weiteren interessanten Ergebnissen.

Schließlich haben wir untersucht, inwiefern sich QZA bezüglich der von ihnen erzeugten Verschränkung unterscheiden. Daraus lässt sich ein brauchbares Komplexitätsmaß ableiten, das eine Unterscheidung leistet, an der die meisten Komplexitätsmaße für deterministische ZA scheitern.

Es sollte möglich sein, den neuen Begriff von globaler Quantenkonfiguration zumindest in Ansätzen auf den stochastischen Fall zu übertragen. Ein Teil des mathematischen Reichtums würde zwar verloren gehen (weil im klassischen Fall die Theorie abelsch sein muss), aber man würde auf jeden Fall eine Möglichkeit zur lokalen Beschreibung globaler Konfigurationen gewinnen und auch die Metrik ließe sich übertragen.

Zusammenfassung und Ausblick

Wir haben ein Modell von Quantenzellularautomaten entwickelt, das die bestehenden Modelle entscheidend erweitert. Weil wir eine lokale Sicht auf Zellen und ihre Zustände einnehmen, gewinnen wir einen Begriff von globalen und lokalen Konfigurationen, der Zellularautomaten, die ja durch die Lokalität ihrer Interaktion charakterisiert sind, angemessen ist. Dank dieser lokalen Sicht ist es außerdem gelungen, die Beschränkung auf endliche Konfigurationen zu überwinden.

Neben der Entwicklung eines brauchbaren Modells haben wir Folgen der Reversibilität (die für Quantensysteme unumgänglich ist) sowie der Abweichung vom Determinismus untersucht. Da unser Modell deterministische reversible Zellularautomaten als Spezialfälle von Quantenzellularautomaten enthält, haben wir an deterministischen Zellularautomaten herausgearbeitet, wie sich die Forderung nach Reversibilität auf Verhalten und Mächtigkeit auswirkt. Aus den in Kapitel 1 zusammengefassten Simulationsergebnissen sowie der Simulation von Quantenturingmaschinen mit Quantenzellularautomaten nach Watrous [85] kann man schließen, dass reversible (und daher auch Quanten-) Zellularautomaten ein universelles Modell sind und dass der durch die Reversibilität bedingte zusätzliche Aufwand nicht so groß ist, dass er die Effizienzsteigerung der bekannten Quantenalgorithmen zunichte machen würde.

Insbesondere können nach Watrous Quantenzellularautomaten mit kon-

stantem Zeitverlust Quantenturingmaschinen simulieren. Man kann daher auch in Quantenzellularautomaten Algorithmen wie die von Grover oder Shor implementieren und erhält Geschwindigkeitssteigerungen gegenüber einer klassischen Implementierung. Neue Quantenalgorithmen zu entwickeln war allerdings nicht das Ziel dieser Arbeit – wir sind eher an Quantenzellularautomaten als Modell interessiert, zum Beispiel für die Simulation von Quantenprozessen oder wegen ihrer Relevanz als Architekturmodell für Quantenrechner.

Dafür war es wichtig, festzustellen, dass die Reversibilitätsforderung aus Zellularautomaten nicht ein uninteressantes Rechenmodell macht. Nachdem dies geklärt ist, brauchen wir Verfahren, um globale Konfigurationen zu beschreiben und zu vergleichen. Wegen der Entwicklung von Abhängigkeiten und Verschränkung zwischen den Zellen ist schon die Beschreibung viel schwieriger als im klassischen deterministischen Fall; einige der Schwierigkeiten sind aber durchaus vergleichbar mit denen, die bei stochastischen Zellularautomaten auftreten.

Daher haben wir uns in Kapitel 2 mit stochastischen Zellularautomaten auseinandergesetzt – ein Modell entwickelt, die Möglichkeit einer lokalen Sicht auf globale Konfigurationen untersucht und eine Metrik erarbeitet, die einen zweckmäßigen Abstandsbegriff auf globalen Konfigurationen begründet. Diese Themen begegnen uns bei der Beschäftigung mit Quantenzellularautomaten wieder.

Für die lokale Beschreibung von Konfigurationen haben wir bei Quantenzellularautomaten C^*-Algebren eingesetzt. Diese sind eher in der Physik- als in der Informatik-Literatur zum Quantenrechnen gebräuchlich, erweisen sich aber für unsere Zwecke als ausgesprochen nützlich. Sie ermöglichen ein Modell, das die eingeschränkte Sicht jeder Zelle auf ihren eigenen Zustand und den ihrer Umgebung reflektiert. Wir haben gezeigt, dass unser Modell eine echte Erweiterung der bestehenden Ansätze bietet. Ein Vorteil an unserer lokalen Sichtweise auf globale Zustände wird bei der Entwicklung von Metriken offensichtlich. Wir konnten eine Metrik definieren, die in ihrem Abstandsbegriff der bei deterministischen Zellularautomaten üblichen Cantor-Metrik sehr ähnlich ist.

Daneben haben wir uns mit der Frage beschäftigt, wie sehr kleine Ab-

weichungen von der lokalen Überführungsfunktion die globale Entwicklung beeinflussen. Die Motivationen für diese Frage sind vielfältig; im Fall stochastischer Zellularautomaten konnten wir (für die dort hergeleitete Metrik) nachweisen, dass die Abweichungen potentiell beträchtlich sind. Für Quantenzellularautomaten konnten wir diese Frage zwar nicht abschließend klären, die Ergebnisse weisen aber ebenfalls auf große mögliche Abweichungen hin.

Es haben sich nun durch die Bearbeitung der zu Beginn gestellten Aufgaben viele neue Fragen aufgetan. Zum Beispiel sollte sich die Beschreibung mittels lokaler Observablenalgebren, die für Quantenzellularautomaten so nützlich ist, auch auf stochastische Zellularautomaten übertragen lassen. Der Begriff der Observablen ist nicht auf die Quanten-Welt beschränkt; allerdings ist die zugehörige algebraische Theorie im klassischen Fall abelsch.

Außerdem ist es wichtig, bessere Abschätzungen dafür zu finden, wie sich Abweichungen von der lokalen Überführungsfunktion auswirken. Für Quantenturingmaschinen ist bekannt, dass sich solche Auswirkungen prinzipiell begrenzen lassen [7]; ähnliches muss für Quantenzellularautomaten gelten, die Quantenturingmaschinen simulieren. Im Allgemeinen sieht es aber so aus, als ob solche Auswirkungen sich für stochastische und Quantenzellularautomaten prinzipiell nicht begrenzen ließen; man muss daher zum Beispiel bei Geschwindigkeitsaussagen davon ausgehen, dass die konkrete Wahl der Übergangswahrscheinlichkeiten und -amplituden nicht zu vernachlässigen ist, weil es im Allgemeinen nicht möglich ist, diese Werte zu approximieren, ohne das Ergebnis der Rechnung zu gefährden.

STICHWORTVERZEICHNIS

LITERATURVERZEICHNIS

[1] Aharonov, D., Ambainis, A., Kempe, J., und Vazirani, U. Quantum walks on graphs. In *Proceedings of the 33rd STOC* (2001), S. 50–59.

[2] Ambainis, A., Bach, E., Nayak, A., Vishwanath, A., und Watrous, J. One-dimensional quantum walks. In *Proceedings of the 33rd STOC* (2001), S. 37–49.

[3] Amoroso, S., und Patt, Y. N. Decision procedures for surjectivity und injectivity of parallel maps for tessellation structures. *Journal of Computer and System Sciences 6* (1972), 448–464.

[4] Benioff, P. Quantum mechanical Hamiltonian models of Turing machines. *Journal of Statistical Physics 29* (1982), 515–546.

[5] Benioff, P. Quantum mechanical Hamiltonian models of Turing machines that dissipate no energy. *Physical Review Letters 48* (1982), 1581–1585.

[6] Bennett, C. H. Time/space trade-offs for reversible computation. *SIAM J. Computation 18*, 4 (1989), 766–776.

[7] Bernstein, E., und Vazirani, U. Quantum complexity theory. In *Proceedings of the 25th STOC* (1993), S. 11–20.

[8] Boykett, T. Efficient exhaustive listings of reversible one dimensional cellular automata. *Complex Systems 11* (1997).

[9] Bratteli, O., und Robinson, D. W. *Operator Algebras and Quantum Statistical Mechanics vol. 1/2*. Springer, 1981.

[10] Burks, A. W., Ed. *Essays on Cellular Automata*. University of Illinois Press, 1970.

[11] Cattaneo, G., Formenti, E., und Margara, L. Topological definitions of deterministic chaos. In Delorme und Mazoyer [20], ch. 8, S. 213–259.

[12] Cattaneo, G., Formenti, E., Margara, L., und Mazoyer, J. A shift-invariant metric on $S^{\mathbb{Z}}$ inducing a non-trivial topology. In Prívara und Ružička [71], S. 179–188.

[13] Childs, A. M., Farhi, E., und Gutmann, S. An example of the difference between quantum and classical random walks. Tech. Ber. quant-ph/0103020, `http://xxx.lanl.gov`, 2001.

[14] Choffrut, C., und Pighizzini, G. Distances between languages and reflexivity of relations. In Prívara und Ružička [71], S. 199–208.

[15] Culik, K., Hurd, L. P., und Yu, S. Computation theoretic aspects of cellular automata. *Physica D 45* (1990), 357–378.

[16] Culik, K., und Yu, S. Cellular automata, $\omega\omega$-regular sets, and sofic systems. *Discrete Applied Mathematics 32* (1991), 85–101.

[17] de Jong, H., und Maes, C. Extended application of constructive criteria for ergodicity of interacting particle systems. *International Journal of Modern Physics C 7* (1996), 1–18.

[18] de la Harpe, P., und Jones, V. An introduction to $C^\star$-algebras. Université de Genève, Section de Mathématiques, 1995.

[19] Delorme, M. An introduction to cellular automata. In Delorme und Mazoyer [20], ch. 1, S. 5–49.

[20] Delorme, M., und Mazoyer, J., Eds. *Cellular Automata. A Parallel Model.* Kluwer Academic Publisher, 1999.

[21] Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A 400* (1985), 97–117.

[22] Dias Barreto, S. A quantum spin system with random interactions I. *Proc. Indian Acad. Sci. (Math. Sci.) 110*, 4 (2000), 347–356.

[23] Dubacq, J.-C. How to simulate Turing machines by invertible one-dimensional cellular automata. *International Journal of Foundations of Computer Science 6*, 4 (1997), 395–402.

[24] Dür, W., Vidal, G., und Cirac, J. I. Three qubits can be entangled in two inequivalent ways. Tech. Ber. quant-ph/0005115 v2, `http://xxx.lanl.gov/`, 2000.

[25] Durand-Lose, J. Reversible cellular automaton able to simulate any other reversible one using partitioning automata. In *Proceedings of LATIN 95* (1995), Nr. 911 in LNCS, S. 230–244.

[26] Durand-Lose, J. Intrinsic universality of a 1-dimensional reversible cellular automaton. In *Proceedings of the 14th STACS* (1997), Nr. 1200 in LNCS, S. 439–450.

[27] Durand-Lose, J. Reversible space-time simulation of cellular automata. *Theoretical Computer Science 146*, 1–2 (2000), 117–129.

[28] Dürr, C., LêThanh, H., und Santha, M. A decision procedure for well–formed linear quantum cellular automata. In *Proceedings of the 13th STACS* (1996), Nr. 1046 in LNCS, Springer, S. 281–292.

[29] Dürr, C., und Santha, M. A decision procedure for unitary linear quantum cellular automata. In *Proceedings of the 37th FOCS* (1996), S. 38–45.

[30] Formenti, E. *Automates cellulaires et chaos: de la vision topologique à la vision algorithmique*. Dissertation, École normale Supérieure de Lyon, 1998.

[31] Frank, M. P. *Reversibility for efficient computing*. Dissertation, MIT, 1999.

[32] Fuchs, C. A., und van de Graaf, J. Cryptographic distinguishability measures for quantum mechanical states. Tech. Ber. quant-ph/9712042 v2, `http://xxx.lanl.gov/`, 1998.

[33] Grössing, G., und Zeilinger, A. Quantum cellular automata. *Complex Systems 2* (1988), 197–208.

[34] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th STOC* (1996), S. 212–219.

[35] Gruska, J. *Quantum Computing*. McGraw–Hill, 1999.

[36] Haller, M. Strukturuntersuchungen an eindimensionalen reversiblen Zellularautomaten. Studienarbeit, Universität Karlsruhe, 2001.

[37] Hedlund, G. A. Endomorphisms and automorphisms of the shift dynamical system. *Mathematical Systems Theory 3* (1969), 320–375.

[38] Hertling, P. Embedding cellular automata into reversible ones. Tech. Ber. CDMTCS-065, University of Auckland, 1997.

[39] Hillman, D. The structure of reversible one-dimensional cellular automata. *Physica D* (1991), 277–292.

[40] Imai, K., und Morita, K. Firing squad synchronization problem in reversible cellular automata. *Theoretical Computer Science 165*, 2 (1996), 475–482.

[41] Jänich, K. *Topologie*, vierte Aufl. Springer, 1994.

[42] KANE, B. E. A silicon–based nuclear spin quantum computer. *Nature 393* (1998), 133–137.

[43] KARI, J. *Decision Problems Concerning Cellular Automata*. Dissertation, Universität Turku, 1990.

[44] KARI, J. Representation of reversible cellular automata with block permutations. *Mathematical Systems Theory 29*, 1 (1996), 47–61.

[45] LEBOWITZ, J. L., MAES, C., UND SPEER, E. R. Statistical mechanics of probabilistic cellular automata. *Journal of Statistical Physics 59*, 1/2 (1990), 117–170.

[46] LLOYD, S. A potentially realizable quantum computer. *Science 261* (1993), 1569–1571.

[47] LLOYD, S. Programming pulse driven quantum computers. Tech. Ber. quant-ph/9912086, `http://xxx.lanl.gov/`, 1999.

[48] MAES, C., UND SHLOSMAN, S. B. Ergodicity of probabilistic cellular automata: A constructive criterion. *Communications in Mathematical Physics 135* (1991), 233–251.

[49] MAJEWSKI, A. W., UND ZEGARLINSKI, B. Quantum stochastic dynamics I : Spin systems on a lattice. *Mathematical Physics Electronic Journal 1* (1995).

[50] MARROQUÍN, J. L., UND RAMÍREZ, A. Stochastic cellular automata with Gibbsian invariant measures. *IEEE Transactions on Information Theory 37*, 3 (1991), 541–551.

[51] MAZOYER, J. A six–state minimal time solution to the firing squad synchronization problem. *Theoretical Computer Science 50*, 2 (1987), 183–238.

[52] MAZOYER, J., UND RAPAPORT, I. Inducing an order on cellular automata by a grouping operation. Tech. Ber. 97-33, Ecole Normale Supérieure de Lyon, 1997.

[53] Merkle, D. Theoretische und praktische Untersuchungen an stochastischen Zellularautomaten. Diplomarbeit, Universität Karlsruhe, 1997.

[54] Merkle, D., und Worsch, T. Formal language recognition by stochastic cellular automata. *Fundamenta Informaticae* (zur Veröffentlichung akzeptiert)

[55] Meyer, D. A. From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics 85* (1996), 551–574.

[56] Meyer, D. A. On the absence of homogeneous scalar unitary cellular automata. Tech. Ber. quant-ph/9604011, `http://xxx.lanl.gov/`, 1996.

[57] Meyer, D. A. Unitarity in one dimensional nonlinear quantum cellular automata. Tech. Ber., `http://xxx.lanl.gov/`, 1996.

[58] Meyer, D. A. Quantum lattice gases and their invariants. *International Journal of Modern Physics C 8* (1997), 717–735.

[59] Morita, K. Reversible simulation of one-dimensional irreversible cellular automata. *Theoretical Computer Science 148*, 1 (1995), 157–163.

[60] Morita, K., und Harao, M. Computation universality of one-dimensional reversible (injective) cellular automata. *Trans. IEICE Japan E72* (1989), 758–762.

[61] Morita, K., und Imai, K. Logical universality and self-reproduction in reversible cellular automata. In *Proceedings of the First International Conference on Evolvable Systems (ICES96)* (1997), LNCS, Springer.

[62] Morita, K., Shirasaki, A., und Gono, Y. A 1-tape 2-symbol reversible Turing machine. *Transactions of the IEICE J70-D*, 5 (1987), 1047–1050.

[63] Motwani, R., und Raghavan, P. *Randomized Algorithms*. Cambridge University Press, 1995.

[64] Nayak, A., und Vishwanath, A. Quantum walk on the line. Tech. Ber. quant-ph/0010117, http://xxx.lanl.gov/, 2000.

[65] Nepomechie, R. A spin chain primer. Tech. Ber. hep-th/9810032, http://xxx.lanl.gov/, 1998.

[66] Nielsen, M., und Chuang, I. L. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[67] Nishio, H. An algebraic study of information in cellular automata. In *ACRI 2000 Work in Progress presentations* (2000), Technischer Bericht 2000-22, Universität Karlsruhe.

[68] Nishio, H., und Saito, T. The information dynamics of cellular automata: Informational completeness and reversibility. In *Proceedings of IFIP 2001* (2001).

[69] Orlov, A. O., Amlani, I., Bernstein, G. H., Lent, C. S., und Snider, G. L. Realization of a functional cell for quantum-dot cellular automata. *Science 277* (1997), 928–930.

[70] Preskill, J. Lecture notes for physics 229: Quantum information and computation. http://www.theory.caltech.edu/people/preskill/ph229/, 1998.

[71] Prívara, I., und Ružička, P., Eds. *Mathematical Foundations of Computer Science* (1997), Nr. 1295 in LNCS, Springer.

[72] Raussendorf, R., und Briegel, H. Computational model underlying the one-way quantum computer. Tech. Ber. quant-ph/0108067, http://xxx.lanl.gov/, 2001.

[73] Rudin, W. *Principles of Mathematical Analysis*. McGraw-Hill, 1976.

[74] Rust, H. *Zur Komplexität von Überführungsfunktionen in Zellularräumen*. Dissertation, Universität Karlsruhe, 1993.

[75] Schöning, U. A probabilistic algorithm for k-SAT based on limited local search and restart. *Algorithmica 32* (2002), 615–623.

[76] Sears, M. The automorphisms of the shift dynamical system are relatively sparse. *Mathematical Systems Theory* (1971), 228–231.

[77] Shor, P. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of the 35th FOCS* (1994), S. 124–134.

[78] Snider, G. L., Orlov, A. O., Amlani, I., Zuo, X., Bernstein, G. H., Lent, C. S., Merz, J. L., und Porod, W. Quantum-dot cellular automata: Review and recent experiments. *Journal of applied physics 85*, 8 (1999), 4283–4285.

[79] Sutner, K. Debruijn graphs and cellular automata. *Complex Systems 5* (1991), 19–30.

[80] Toffoli, T. Computation and construction universality of reversible cellular automata. *Journal of Computer and System Sciences 15* (1977), 213–231.

[81] Toffoli, T., und Margolus, N. H. *Cellular Automata Machines*. MIT Press, 1987.

[82] Toffoli, T., und Margolus, N. H. Invertible cellular automata: a review. *Physica D 45* (1990), 229–253.

[83] van Dam, W. Quantum cellular automata. Diplomarbeit, Universität Nijmegen, Niederlande, 1996.

[84] Vollmar, R. *Algorithmen in Zellularautomaten*. Teubner, 1979.

[85] Watrous, J. On one-dimensional quantum cellular automata. In *Proceedings of the 36th FOCS* (1995), S. 528–537.

[86] Wolfram, S. Computation theory of cellular automata. *Communications in Mathematical Physics 96* (1984), 15–57.

[87] Wu, S., und Zhang, Y. Multipartite pure-state entanglement and the generalized GHZ states. Tech. Ber. quant-ph/0004020 v2, `http://xxx.lanl.gov/`, 2000.

[88] Yepez, J. Quantum computation of fluid dynamics. In *Quantum Computing and Quantum Communications. 1st NASA International Conference QCQC* (1998), C. P. Williams, Ed., Nr. 1509 in LNCS, S. 34–60.

[89] Yepez, J. Lattice-gas quantum computation. *International Journal of Modern Physics C 9*, 8 (1999), 1587–1596.

[90] Yepez, J. Lattice-gas quantum computing. In *Proceedings of the AFQSR Meeting on computational and applied mathematics* (1999).

[91] Życzkowski, K., und Słomczyński, W. Monge metric on the sphere und geometry of quantum states. *Journal of Physics A: Mathematical und General 34* (2001), 6689–6722.