Universität Leipzig

Fakultät für Mathematik und Informatik

Institut für Informatik

Quantenautomaten und das Cut-Point-Theorem für beschränkte erkennbare Potenzreihen

Bachelorarbeit

Leipzig, September 2009

Vorgelegt von — Martin Huschenbett
Studiengang Informatik (BSc.)

Betreuender Hochschullehrer — Prof. Dr. Manfred Droste
Institut für Informatik
Universität Leipzig

Inhaltsverzeichnis

1 Einleitung

> In an important milestone toward making powerful computers that exploit the mind-bending possibilities of calculating with individual atoms, scientists at the I.B.M. Almaden Research Center, in San Jose, Calif., are announcing today that they have performed the most complex such calculation yet: factoring the number 15. [10]

Wieso war es der New York Times am 20.12.2001 eine Nachricht wert, dass es Wissenschaftlern gelang, die Zahl 15 mit einem Computer zu faktorisieren, obwohl dies doch bereits mit den ersten Rechnermodellen in den 1940er Jahren möglich war? Die Antwort liefert der nächste Absatz:

> The answer itself was no surprise: 3 and 5, the numbers that divide into 15, leaving no remainder. But the exercise that led to that simple result – the first factoring of a number with an exotic device called a *quantum computer* – holds the promise of one day solving problems now considered impossible, and cracking seemingly impenetrable codes. [10]

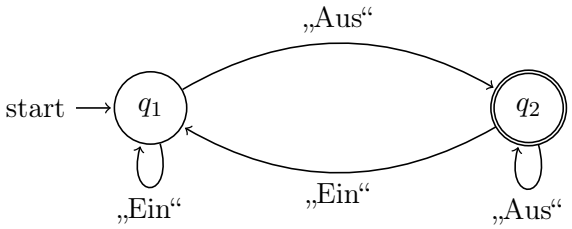
Das Interessante an dem gemeldeten Vorgang war also nicht das Ergebnis der Faktorisierung selbst, sondern das Gerät, auf dem diese durchgeführt wurde, ein sogenannter Quantencomputer. Doch worum handelt es sich bei diesen Geräten und warum interessiert man sich für sie, wenn eine derart einfache Aufgabe scheinbar schon eine große Herausforderung für sie darstellt?

Kurz gesagt: Quantenrechner sind Computer die auf quantenmechanischen Prinzipien und Phänomenen beruhen. Heutzutage handelt es sich beim Quantumcomputing um ein aktives Forschungsfeld, für Physiker wie Informatiker, das noch hauptsächlich theoretischer Art ist. Wie der zitierte Artikel aufzeigt, ist es unter Laborbedingungen jedoch bereits möglich, kleinste Quantencomputer zu bauen, und es besteht die Hoffnung eines Tages alltagstaugliche Exemplare herzustellen. Diese wären durch die Ausnutzung quantenphysikalischer Effekte in der Lage, exponentiell viele Berechnungspfade parallel abzuarbeiten und würden so bedeutend effizientere Algorithmen erlauben [9, S. 101ff]. Die Forscher von IBM haben beispielsweise Shors Faktorisierunsalgorithmus implementiert, der die Faktorisierung einer Zahl in Polynomialzeit ermöglicht [17]. Im Kontrast dazu benötigt der beste bekannte Algorithmus zur Lösung dieses Problems auf einem klassischen Computer exponentiell viel Zeit.

Der Inhalt dieser Arbeit sind jedoch nicht Quantencomputer im Allgemeinen, sondern hauptsächlich Quantenautomaten. Einen Automaten im klassischen Sinne kann man sich als eine Maschine vorstellen, die sich stets in einem von endlich vielen Zuständen befindet, von denen einige als „final“ markiert sind und unter denen es einen ausgezeichneten

Anfangszustand gibt. Aufgabe des Automaten ist die Untersuchung endlicher Symbolfolgen. Dazu geht er die Folge zeichenweise von Anfang bis Ende durch und wechselt in jedem Schritt in Abhängigkeit vom aktuellen Zustand und dem gelesenen Symbol in einen neuen Zustand. Ist der Zustand nach dem Abarbeiten des letzten Symbols mit „final“ markiert, dann „akzeptiert“ der Automat die Folge, andernfalls lehnt er sie ab. Die Sprache des Automaten ist schließlich die Menge aller Symbolfolgen, die er akzeptiert.

Beispielsweise akzeptiert der folgende, grafisch dargestellte Automat gerade diejenigen Folgen von „Ein“- und „Aus“-Ereignissen, die ein eingeschaltetes Gerät in ein ausgeschaltetes überführen:



Dabei ist q_1 der Anfangszustand und der Doppelkreis um q_2 markiert diesen Zustand als „final“. Eine formale Definition endlicher Automaten findet man z.B. in [16, S. 19].

Versieht man dieses Modell eines Automaten, das gewissermaßen auf klassischer Physik basiert, mit quantenmechanischen Grundlagen, erhält man das Konzept eines Quantenautomaten. Das Interesse an diesen beruht auf der Annahme, dass Quantencomputing in der Zukunft praktisch durchführbar sein wird. Außerdem besteht die Hoffnung, durch die Übertragung möglichst vieler Konzepte der klassischen Berechnungstheorie auf Quantenberechnungen Letztere theoretisch besser fassen zu können. Da die unterste Stufe der traditionellen Berechnungshierarchie die endlichen Automaten und regulären Sprachen bilden, bietet es sich an, diese als erste zu übertragen. Dies führt zu den Begriffen der „endlichen Quantenautomaten“ und der „quantenregulären“ oder „quantenerkennbaren Sprachen“, die Hauptgegenstand der vorliegenden Arbeit sind. Die Klasse der quantenerkennbaren Sprachen wird dabei nach ähnlichen Mustern untersucht, wie formale Sprachen oder formale Potenzreihen, insbesondere Abschlusseigenschaften spielen hierbei eine wichtige Rolle. Die Höhepunkte der Arbeit sind die Beweise eines Pumping-Lemmas (siehe [12]) und eines Cut-Point-Theorems (siehe [6]) für quantenreguläre Sprachen sowie eine darauf basierende Charakterisierung der von Quantenautomaten akzeptierten Sprachen (siehe [7]) in Kapitel 5. Neu sind die Verallgemeinerung des Cut-Point-Theorems auf beschränkte erkennbare Potenzreihen sowie einige negative Resultate hinsichtlich der Abschlusseigenschaften quantenerkennbarer Sprachen.

Die Arbeit gliedert sich folgendermaßen: Kapitel 2 stellt die notwendigen mathematischen Grundlagen bereit, die über den Inhalt der Mathematikausbildung eines Informatikstudiums hinausgehen. Die für die letzten zwei Kapitel erforderlichen Kenntnisse der Theorie der gewichteten Automaten und der (erkennbaren) formalen Potenzreihen werden in Kaptiel 3 vorgestellt. Kapitel 4 beschäftigt sich mit beschränkten Potenzreihen und beweist eine verallgemeinerte Formulierung des Cut-Point-Theorems. Abschließend hat Kapitel 5 den Hauptgegenstand der Arbeit zum Inhalt – Quantenautomaten.

Hinweise zu den verwendeten Notationen

Prinzipiell werden in dieser Arbeit Funktionsapplikationen in Postfix-Notation geschrieben, d.h. xA anstelle von $A(x)$ für $A : X \to Y$ und $x \in X$. Dementsprechend wird auch die Zusammensetzung zweier Abbildungen $A : X \to Y$ und $B : Y \to Z$ mit AB bezeichnet, so dass für $x \in X$ gerade gilt

$$x(AB) = (xA)B.$$

Da diese Form der Assoziativität zudem das Weglassen der Klammern erlaubt, wird von dieser Möglichkeit Gebrauch gemacht.

Zur Erhöhung der Übersichtlichkeit gibt es einen Ausnahmefall, in dem für die Applikation nicht die Postfix-Notation verwendet wird: Ist der Urbildbereich einer Funktion $f : M \to X$ ein allgemeines Monoid, dann wird die Anwendung von f auf $m \in M$ mit $f(m)$ notiert. Dies ist insbesondere für Monoid-Homomorphismen der Fall, weswegen die Zusammensetzung zweier derartiger Homomorphismen $h : M \to M'$ und $h' : M' \to M''$ zur Verdeutlichung des Unterschiedes mit $h' \circ h$ bezeichnet wird.

In allen verbleibenden Fällen werden die Notationen der benutzten Literatur übernommen oder Standardbezeichnungen verwendet.

2 Mathematische Grundlagen

Für das Verständnis der zentralen Gegenstände dieser Arbeit sind gute Kenntnisse der Linearen Algebra unerlässlich. Während der Inhalt eines Basiskurses für die gewichteten Automaten noch ausreichend ist, wird für die Kapitel über beschränkte Potenzreihen und Quantenautomaten darüber hinausgehendes Wissen benötigt. Als Vorbereitung auf ersteres erfolgt in Abschnitt 2.1 eine Beschäftigung mit dem Konzept der „normierten Vektorräume“, wobei das Wiedergegebene hauptsächlich [19] entnommen wurde.

Zur Formulierung der quantenmechanischen Aspekte der Quantenautomaten nehmen insbesondere die Begriffe des „unitären Vektorraums“ und der „unitären Abbildung“ einen zentralen Platz ein. Aus diesem Grund ist das Anliegen von Abschnitt 2.2, den Leser mit den nötigen Definitionen und Aussagen der Theorie der unitären Vektorräume vertraut zu machen. Solide Grundkenntnisse im Bereich der Linearen Algebra, etwa das Verständnis der Begriffe Vektorraum, Basis, lineare Abbildung, Eigenvektor, etc., werden dabei vorausgesetzt. Da sich das Vorgestellte im Wesentlichen an Kapitel 7 aus [5] orientiert, wird auf die Angabe von Beweisen verzichtet.

Abschnitt 2.3 dient der Angabe zweier Konstruktionen, die aus gegebenen Vektorräumen weitere Vektorräume erzeugen. Neben den Definitionen werden einige „Rechenregeln“ aufgelistet und die Verträglichkeit mit den Konzept der unitären Vektorräume herausgearbeitet.

Schließlich widmet sich Abschnitt 2.4 der algebraischen Struktur des „Monoides“, welche in zweierlei Hinsicht wesentlich für den Inhalt dieser Arbeit ist. Einerseits wird hier fast die komplette Theorie der formalen Potenzreihen und Quantensprachen über beliebigen Monoiden betrieben. Andererseits benötigt man insbesondere den Begriff des „Monoid-Homomorphismus“ sowie einige spezielle Monoide zur Definition der untersuchten Automatenmodelle.

2.1 Normierte Vektorräume

Dieser Abschnitt dient der Einführung der Begriffe „Norm“ und „normierter Vektorraum“, die den geometrischen Begriff der Länge eines Vektors verallgemeinern. Im Folgenden sei K dabei einer der beiden Körper $\mathbb{R}$ oder $\mathbb{C}$ und für $\lambda \in K$ bezeichne $|\lambda|$ wie üblich den reellen bzw. komplexen Betrag von λ.

Definition 2.1.1. Sei V ein K-Vektorraum. Eine *Norm auf* V ist eine Abbildung $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ die folgende Eigenschaften besitzt:

(1) Definitheit: für alle $x \in V$ gilt

$$\|x\| = 0 \Longleftrightarrow x = 0.$$

(2) Absolute Homogenität: für alle $x \in V$ und $\lambda \in K$ gilt

$$\|\lambda x\| = |\lambda| \cdot \|x\| .$$

(3) Dreiecksungleichung: für alle $x, y \in V$ gilt

$$\|x + y\| \leq \|x\| + \|y\| .$$

Ein Vektorraum V zusammen mit einer Norm $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ wird als *normierter Vektorraum* bezeichnet. Ein Vektor $x \in V$ heißt *normiert*, wenn $\|x\| = 1$ gilt.

Auf dieser Definition aufbauend, kann man den Begriff der „Beschränktheit“ von den reellen Zahlen auf normierte Vektorräume übertragen.

Definition 2.1.2. Sei V ein normierter Vektorraum. Eine Menge $X \subseteq V$ bezeichnet man als *beschränkt*, wenn es eine Konstante $c(X) > 0$ gibt, so dass für alle $x \in X$ gilt

$$\|x\| \leq c(X).$$

Eine Funktion $f : M \to V$ von einer beliebigen Menge M nach V bezeichnet man als *beschränkt*, wenn ihr Bild $\mathrm{im}(f) \subseteq V$ beschränkt ist.

Ist V ein endlich-dimensionaler Vektorraum und $\{e_i\}_{i \in I}$ eine Basis von V, dann ist für jedes $p \geq 1$ durch die Abbildung

$$\left\| \sum_{i \in I} \alpha_i e_i \right\|_p = \left(\sum_{i \in I} |\alpha_i|^p \right)^{\frac{1}{p}}$$

eine Norm $\|\cdot\|_p$ auf V definiert, die sogenannte *p-Norm*. Die durch

$$\left\| \sum_{i \in I} \alpha_i e_i \right\|_\infty = \max_{i \in I} |\alpha_i|$$

festgelegte *Maximumsnorm* $\|\cdot\|_\infty$ kann als Ergebnis der Grenzwertbildung $p \to \infty$ aufgefasst werden. Auf dem eindimensionalen Vektorraum K fallen diese Normen alle mit der Betragsabbildung $|\cdot|$ zusammen.

Definition 2.1.3. Zwei Normen $\|\cdot\|_1 : V \to \mathbb{R}_{\geq 0}$ und $\|\cdot\|_2 : V \to \mathbb{R}_{\geq 0}$ auf einem Vektorraum V werden als *äquivalent* bezeichnet, wenn $c_1, c_2 > 0$ existieren, so dass für alle $x \in V$ gilt

$$c_1 \cdot \|x\|_1 \leq \|x\|_2 \leq c_2 \cdot \|x\|_1 .$$

Folgender Satz aus der Funktionalanalysis, der hauptsächlich mithilfe des Satzes von Heine-Borel aus der Topologie metrischer Räume bewiesen wird, ist für Kapitel 4 von besonderer Bedeutung.

Satz 2.1.4. *Auf einem endlich-dimensionalen K-Vektorraum sind alle Normen äquivalent.*

Die nachstehende Behauptung lässt sich im Falle der 1-Norm auf V einfach beweisen und mit dem vorangehenden Satz zu folgender Formulierung verallgemeinern.

Korollar 2.1.5. *Seien V und W endlich-dimensionale, normierte Vektorräume und $A : V \to W$ eine lineare Abbildung. Dann existiert eine von A und den beiden Normen abhängige Konstante $c(A) > 0$, so dass für alle $x \in V$ gilt*

$$\|xA\| \leq c(A) \cdot \|x\| .$$

Mithilfe einer geometrischen Argumentation über Volumina oder eines Schubfachschlusses, kann man folgendes Lemma zeigen, welches für den Beweis des Cut-Point-Theorems in Abschnitt 4.3 benötigt wird.

Lemma 2.1.6. *Seien V ein endlich-dimensionaler, normierter Vektorraum, $X \subseteq V$ eine beschränkte Teilmenge von V und $\varepsilon > 0$, so dass für je zwei verschiedene $x, y \in X$ gilt*

$$\|x - y\| \geq \varepsilon.$$

Dann ist X endlich.

2.2 Unitäre Vektorräume

Der erste Teil dieses Abschnittes dient der Verallgemeinerung des Punktprodukts von Vektoren des $\mathbb{R}^n$ zum Skalarprodukt zweier Vektoren eines beliebigen $\mathbb{R}$- oder $\mathbb{C}$-Vektorraumes sowie der damit verbundenen Einführung unitärer Vektorräume. Anschließend wird eine Untersuchung des Zusammenspiels von Skalarprodukten und linearen Abbildungen vorgenommen, welche die Begriffe der adjungierten, unitären sowie selbstadjungierten Abbildungen hervorbringen wird. Da man diese Theorie sowohl über den reellen als auch über den komplexen Zahlen betreiben kann, sei K im Rest dieses Abschnittes einer der beiden Körper $\mathbb{R}$ oder $\mathbb{C}$. Wie üblich bezeichne $\overline{x}$ dabei die konjugiert komplexe Zahl eines $x \in \mathbb{C}$ bzw. im Falle $K = \mathbb{R}$ die Zahl x selbst.

2.2.1 Skalarprodukte und unitäre Vektorräume

Definition 2.2.1. Seien V und W K-Vektorräume. Eine *Sesquilinearform* ist eine Abbildung $\bullet : V \times W \to K$ mit folgenden Eigenschaften:

(1) $\bullet$ ist *linear im ersten Argument*, d.h. für alle $x, x' \in V$, $y \in W$ und $\lambda \in K$ gilt

$$(x + x') \bullet y = x \bullet y + x' \bullet y \qquad \text{und} \qquad (\lambda \cdot x) \bullet y = \lambda \cdot (x \bullet y).$$

(2) $\bullet$ ist *semilinear im zweiten Argument*, d.h. für alle $x \in V$, $y, y' \in W$ und $\lambda \in K$ gilt

$$x \bullet (y + y') = x \bullet y + x \bullet y' \qquad \text{und} \qquad x \bullet (\lambda \cdot y) = \overline{\lambda} \cdot (x \bullet y).$$

Sind B und C Basen von V bzw. W, dann lässt sich in Analogie zur linearen Fortsetzung jede Abbildung $B \times C \to U$ eindeutig zu einer sesquilinearen Abbildung fortsetzen.

Definition 2.2.2. Ein *Skalarprodukt* oder auch *inneres Produkt* auf einem K-Vektorraum V ist eine Sesquilinearform $\langle \cdot, \cdot \rangle : V \times V \to K$, die folgenden Bedingungen genügt:

(1) $\langle \cdot, \cdot \rangle$ ist *hermitesch*, d.h. für alle $x, y \in V$ gilt

$$\langle x, y \rangle = \overline{\langle y, x \rangle}.$$

(2) $\langle \cdot, \cdot \rangle$ ist *positiv definit*, d.h. für alle $x \in V \setminus \{0\}$ gilt

$$\langle x, x \rangle \in \mathbb{R} \qquad \text{und} \qquad \langle x, x \rangle > 0.$$

Einen Vektorraum V auf dem ein Skalarprodukt definiert ist, bezeichnet man als *Prähilbertraum*, *Innenproduktraum* oder *unitären Vektorraum*.

Bemerkung. Es ist durchaus üblich, lediglich im Falle $K = \mathbb{C}$ von einem unitären Vektorraum und für $K = \mathbb{R}$ von einem *euklidischen Vektorraum* zu sprechen, diese Unterscheidung soll hier jedoch nicht vorgenommen werden.

Offensichtlich ist jeder Unterraum U eines unitären Vektorraumes V mit der Einschränkung des Skalarproduktes auf $\langle \cdot, \cdot \rangle : U \times U \to K$ ebenfalls unitär.

Für den Spezialfall $V = K^n$ liefert die Definition

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum_{i=1}^{n} x_i \overline{y_i}$$

ein Skalarprodukt auf V. Dieses wird als *Standardskalarprodukt* oder *kanonisches Skalarprodukt* bezeichnet und im folgenden allen (Gegen-)Beispielen zugrunde liegen.

Der folgende Satz formuliert die *Schwarzsche Ungleichung*:

Satz 2.2.3. *Sei V ein unitärer Vektorraum. Dann gilt für alle $x, y \in V$:*

$$|\langle x, y \rangle|^2 \leq \langle x, x \rangle \cdot \langle y, y \rangle,$$

wobei Gleichheit genau dann eintritt, wenn x und y linear abhängig sind.

Mithilfe dieser Ungleichung kann man nachweisen, dass das Skalarprodukt eines jeden unitären Vektorraumes V durch

$$\|x\| = \sqrt{\langle x, x \rangle}$$

eine Norm $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ auf V induziert. Mit dieser Norm ist V im Sinne von Definition 2.1.1 ein normierter Vektorraum. Wird im Folgenden ein unitärer Vektorraum als normierter Vektorraum aufgefasst, dann sei die zugehörige Norm wie üblich stets die vom Skalarprodukt induzierte. Unter Verwendung dieser Norm lässt sich die Schwarzsche Ungleichung alternativ folgendermaßen formulieren:

$$|\langle x, y \rangle| \leq \|x\| \cdot \|y\|.$$

2.2.2 Orthogonalität

Von hier an sei V für den Rest von Abschnitt 2.2 stets ein endlich-dimensionaler, unitärer Vektorraum.

Definition 2.2.4. Zwei Vektoren $x, y \in V$ heißen *orthogonal* zueinander, in Zeichen $x \perp y$, wenn $\langle x, y\rangle = 0$ gilt. Zwei Mengen $X, Y \subseteq V$ heißen *orthogonal* zueinander, wenn $x \perp y$ für alle $x \in X$ und $y \in Y$ gilt.

Eine Menge $M \subseteq V \setminus \{0\}$ heißt *Orthogonalsystem*, wenn je zwei Vektoren aus M zueinander orthogonal sind. Sind außerdem alle Vektoren aus M normiert, dann nennt man M *Orthonormalsystem*. Eine *Orthonormalbasis* ist eine Basis, die ein Orthonormalsystem bildet.

Ist $e_1, \ldots, e_n$ eine Orthonormalbasis von V und sind $x = \sum_{i=1}^n \alpha_i e_i$ und $y = \sum_{i=1}^n \beta_j e_i$ zwei Vektoren, dann lässt sich das Skalarprodukt von x und y folgendermaßen berechnen:

$$\langle x, y\rangle = \langle \sum_{i=1}^n \alpha_i e_i, \sum_{j=1}^n \beta_j e_j\rangle = \sum_{i,j=1}^n \alpha_i \overline{\beta_j} \langle e_i, e_j\rangle = \sum_{i=1}^n \alpha_i \overline{\beta_i}.$$

Ist $V = K^n$ und $e_1, \ldots, e_n$ die kanonische Basis, welche eine Orthonormalbasis ist, dann liefert obige Gleichung die Definition des Standardskalarproduktes.

Fakt 2.2.5. Sei U ein Unterraum von V. Die Menge

$$U^\perp = \{x \in V \mid \forall y \in U : x \perp y\}$$

heißt *orthogonales Komplement von U in V* und ist ein Unterraum von V. Weiter gilt:

(1) U und $U \perp$ bilden eine *orthogonale Zerlegung* von V, d.h.

$$U \perp U^\perp \quad \text{und} \quad V = U \oplus U^\perp.$$

(2) Die Bildung des orthogonalen Komplements ist selbstinvers, d.h.

$$(U^\perp)^\perp = U.$$

Fakt 2.2.6. Seien V ein endlich-dimensionaler, unitärer Vektorraum und U ein Unterraum. Dann existiert genau eine lineare Abbildung $P_U : V \to U$, so dass für alle $x \in V$ und $y \in U$ gilt

$$\langle x - xP_U, y\rangle = 0.$$

Diese heißt *orthogonale Projektion auf U* und besitzt folgende Eigenschaften

(1) P_U beschränkt sich auf U zur identischen Abbildung und auf $U^\perp$ zur Nullabbildung, d.h. für alle $x \in U$ und $y \in U^\perp$ gilt

$$xP_U = x \qquad \text{und} \qquad yP_U = 0.$$

(2) Ist $P_U^\perp : V \to U^\perp$ die orthogonale Projektion auf $U^\perp$, dann bestehen für alle $x \in V$ die Gleichungen

$$x = xP_U + xP_U^\perp, \qquad \langle xP_U, xP_U^\perp \rangle = 0 \qquad \text{und} \qquad \|x\|^2 = \|xP_U\|^2 + \|xP_U^\perp\|^2.$$

Weiterhin gilt

$$\|xP_U\| \leq \|x\|,$$

d.h. P_U ist *(längen-)verkürzend*. Gleichheit tritt genau dann ein, wenn $x \in U$. Außerdem gelten folgende „Rechenregeln“ für die linearen Operatoren P_U und $P_U^\perp$:

$$\mathrm{Id} = P_U + P_U^\perp, \qquad P_U P_U^\perp = 0 \qquad \text{und} \qquad P_U^\perp P_U = 0.$$

(3) Ist $e_1, \ldots, e_k$ eine Orthonormalbasis von U, dann gilt für alle $x \in V$

$$xP_U = \sum_{i=1}^{k} \langle x, e_i \rangle e_i.$$

Eine lineare Abbildung $A : V \to V$ wird *orthogonale Projektion* genannt, wenn es einen Unterraum U von V mit $A = P_U$ gibt.

Da es zu jedem Unterraum U nur eine orthogonale Projektion auf diesen gibt und umgekehrt zu jeder orthogonalen Projektion P nur einen Unterraum auf den diese projeziert, nämlich $\mathrm{im}P$, kann man die Unterräume von V und die orthogonalen Projektionen der Gestalt $V \to V$ auf natürliche Weise miteinander identifzieren.

Schließlich kann man mithilfe des Gram-Schmidtschen Orthonormalisierungsverfahrens folgenden wichtigen Satz beweisen.

Satz 2.2.7. *Jeder endlich-dimensionale, unitäre Vektorraum V besitzt eine Orthonormalbasis. Jede Orthonormalbasis eines Unterraums U von V lässt sich zu einer Orthonormalbasis von V ergänzen.*

2.2.3 Die adjungierte Abbildung

Fakt 2.2.8. Sei $A : V \to V$ eine lineare Abbildung. Dann existiert eine eindeutig bestimmte lineare Abbildung $A^* : V \to V$, so dass für alle $x, y \in V$ gilt

$$\langle xA, y \rangle = \langle x, yA^* \rangle.$$

Diese nennt man die *zu A adjungierte Abbildung*. Sie besitzt folgende Eigenschaften

(1) Es gilt

$$\ker A^* = (\mathrm{im}A)^\perp \qquad \text{und} \qquad \mathrm{im}A^* = (\ker A)^\perp.$$

(2) A ist genau dann bijektiv, wenn A^* bijektiv ist.

(3) Der Adjunktionsoperator $^* : \mathrm{End}(V) \to \mathrm{End}(V), A \mapsto A^*$ ist semi-linear, d.h. für alle $A, B \in \mathrm{End}(V)$ und $\alpha \in K$ gilt

$$(A+B)^* = A^* + B^* \qquad \text{und} \qquad (\alpha A)^* = \overline{\alpha} A^*.$$

Definition 2.2.9. Eine lineare Abbildung $A : V \to V$ heißt *normal*, wenn sie mit ihrer adjungierten Abbildung kommutiert, d.h. wenn gilt

$$AA^* = A^*A.$$

Fakt 2.2.10. Sei $A : V \to V$ eine lineare Abbildung.

(1) A ist genau dann normal, wenn für alle $x, y \in V$ gilt

$$\langle xA, yA \rangle = \langle xA^*, yA^* \rangle.$$

(2) Sei A normal. Es ist $x \in V$ genau dann ein Eigenvektor von A zum Eigenwert $\lambda \in K$, wenn x ein Eigenvektor von A^* zum Eigenwert $\overline{\lambda}$ ist.

Der nachfolgende *Spektralsatz für normale Abbildungen* ist wesentlich für die Beweise der Sätze 2.2.13 und 2.2.15.

Satz 2.2.11. *Sei $A : V \to V$ eine lineare Abbildung, deren charakteristisches Polynom $\chi_A \in K[T]$ vollständig in Linearfaktoren zerfällt. Dann ist A genau dann normal, wenn V eine Orthonormalbasis besitzt, die aus lauter Eigenvektoren von A besteht.*

2.2.4 Isometrien und unitäre Abbildungen

Fakt 2.2.12. Sei $A : V \to V$ eine lineare Abbildung. Dann sind äquivalent:

(1) Für alle $x, y \in V$ gilt

$$\langle xA, yA \rangle = \langle x, y \rangle.$$

(2) A ist ein Isomorphismus mit

$$A^* = A^{-1}.$$

(3) A ist eine *Isometrie*, d.h. für alle $x \in V$ gilt

$$\|xA\| = \|x\|.$$

(4) Für alle Orthonormalbasen $e_1, \ldots, e_n$ von V, ist auch $e_1A, \ldots, e_nA$ eine Orthonormalbasis von V.

(5) Es existiert eine Orthonormalbasis $e_1, \ldots, e_n$ von V, für die auch $e_1A, \ldots, e_nA$ eine Orthonormalbasis von V ist.

Sind diese Bedingungen erfüllt, dann nennt man A *unitäre Abbildung*. Die Menge aller unitären Abbildungen des Vektorraumes V wird mit $\mathrm{U}(V)$ bezeichnet.

Bemerkung. Die identische Abbildung Id_V, die Zusammensetzung zweier unitärer Abbildungen sowie die Umkehrabbildung einer unitären Abbildung sind alle unitär.

Der nachstehende *Spektralsatz für unitäre Abbildungen* gilt lediglich im komplexen Fall.

Satz 2.2.13. *Seien $K = \mathbb{C}$ und $A : V \to V$ eine lineare Abbildung. Es ist A genau dann unitär, wenn $|\lambda| = 1$ für alle Eigenwerte λ von A gilt und V eine Orthonormalbasis besitzt, die aus lauter Eigenvektoren von A besteht.*

2.2.5 Selbstadjungierte Abbildungen

Definition 2.2.14. Eine lineare Abbildung $A : V \to V$ heißt *selbstadjungiert*, wenn $A^* = A$ gilt.

Der folgende *Spektralsatz für selbstadjungierte Abbildungen* ermöglicht eine Charakterisierung der orthogonalen Projektionen.

Satz 2.2.15. *Sei $A : V \to V$ eine lineare Abbildung. A ist genau dann selbstadjungiert, wenn alle Eigenwerte von A reell sind und V eine Orthonormalbasis besitzt, die aus lauter Eigenvektoren von A besteht.*

Es seien $P : V \to V$ eine orthogonale Projektion und U der Unterraum von V, auf den P projeziert. Weiter seien $e_1, \ldots, e_k$ und $e_{k+1}, \ldots, e_n$ je eine Orthonormalbasis von U bzw. $U^\perp$. Dann ist $e_1, \ldots, e_n$ eine Orthonormalbasis von V. Außerden sind $e_1, \ldots, e_k$ allesamt Eigenvektoren von P zum Eigenwert 1 und $e_{k+1}, \ldots, e_n$ Eigenvektoren zum Eigenwert 0. Weitere Eigenwerte kann es aufgrund der linearen Unabhängigkeit der e_i nicht geben, d.h. P ist eine selbstadjungierte Abbildung, die nur die Eigenwerte 0 und 1 besitzt.

Sei umgekehrt $P : V \to V$ eine selbstadjungierte Abbildung mit Eigenwerten 0 und 1 sowie U der Eigenraum zum Eigenwert 1. Dann ist P gerade die orthogonale Projektion von V auf U. Diese beiden Tatsachen ermöglichen es, orthogonale Projektionen und selbstadjungierte Abbildungen, die nur die Eigenwerte 0 und 1 besitzen, miteinander zu identifizieren.

2.3 Vektorraumkonstruktionen

2.3.1 Die direkte Summe

Definition 2.3.1. Seien V und W K-Vektorräume. Die *(konstruierte) direkte Summe von V und W* ist der K-Vektorraum

$$V \oplus W = \{(x, y) \mid x \in V, y \in W\}$$

mit komponentenweiser Addition und Multiplikation

$$(x, y) + (x', y') = (x + x', y + y') \qquad \text{und} \qquad \lambda \cdot (x, y) = (\lambda x, \lambda y).$$

Die Einbettungen $V \to V \oplus W, x \mapsto (x, 0)$ und $W \to V \oplus W, y \mapsto (0, y)$ erlauben es, V und W als Unterräume von $V \oplus W$ aufzufassen. V und W bilden so eine direkte Zerlegung von $V \oplus W$ und für $x \in V$ und $y \in W$ bezeichne $x \oplus y$ den Vektor $(x, y) \in V \oplus W$. Sind X und Y Unterräume von V bzw. W, dann ist $X \oplus Y$ ein Unterraum von $V \oplus W$.

Sind $A : V \to V'$ und $B : W \to W'$ lineare Abbildungen, dann ist durch

$$V \oplus W \to V' \oplus W', (x \oplus y) \mapsto xA \oplus yB$$

eine lineare Abbildung definiert, die mit $A \oplus B$ bezeichnet wird. Es gelten folgende „Rechenregeln“:

$$\begin{aligned}(x \oplus y)(A \oplus B) &= xA \oplus yB,\\ (A \oplus B)(A' \oplus B') &= AA' \oplus BB',\\ \mathrm{Id}_V \oplus \mathrm{Id}_W &= \mathrm{Id}_{V \oplus W}.\end{aligned}$$

Sind A und B Isomorphismen, dann ist $A \oplus B$ ebenfalls ein Isomorphismus und es gilt

$$(A \oplus B)^{-1} = A^{-1} \oplus B^{-1}.$$

Sind V und W unitäre Vektorräume, dann definiert

$$\langle x \oplus y, x' \oplus y' \rangle = \langle x, x' \rangle + \langle y, y' \rangle$$

ein Skalarprodukt auf $V \oplus W$, d.h. dieser Vektorraum ist ebenfalls unitär. Bezüglich dieses Skalarproduktes bilden V und W eine orthogonale Zerlegung von $V \oplus W$. Die orthogonalen Projektionen P_V und P_W von $V \oplus W$ auf V bzw. W sind zugleich die Projektionen auf die entsprechenden Komponenten

$$(x \oplus y)P_V = x \oplus 0 \qquad \text{und} \qquad (x \oplus y)P_W = 0 \oplus y.$$

Sind X und Y Unterräume von V und W und P_X bzw. P_Y die zugehörigen orthogonalen Projektionen, dann ist $P_X \oplus P_Y$ die orthogonale Projektion $P_{X \oplus Y}$ von $V \oplus W$ auf $X \oplus Y$:

$$P_{X \oplus Y} = P_X \oplus P_Y.$$

Sind A und B zwei Endomorphismen, dann gilt für die adjungierte Abbildung von $A \oplus B$:

$$(A \oplus B)^* = A^* \oplus B^*.$$

Also ist $A \oplus B$ unitär (bzw. selbstadjungiert), sobald A und B unitär (bzw. selbstadjungiert) sind.

2.3.2 Das Tensorprodukt

Das Tensorprodukt zweier Vektorräume definiert man üblicherweise über eine Universalitätseigenschaft, in der bilineare Abbildungen eine tragende Rolle spielen. Sind U, V

und W K-Vektorräume, dann heißt eine Abbildung $\Psi : V \times W \to U$ *bilinear*, wenn für jedes $x_0 \in V$ und $y_0 \in W$ die Abbildungen $\Phi(\cdot, y_0) : V \to U, x \mapsto \Phi(x, y_0)$ und $\Phi(x_0, \cdot) : W \to U, y \mapsto \Phi(x_0, y)$ linear sind. Im Falle $U = K$ nennt man Φ *Bilinearform.*

Definition 2.3.2. Seien V und W zwei K-Vektorräume. Ein *Tensorprodukt von V und W* ist ein K-Vektorraum $V \otimes W$ zusammen mit einer bilinearen Abbildung $\otimes : V \times W \to V \otimes W$ die folgende universelle Eigenschaft erfüllt:
Für jede bilineare Abbildung $\bullet : V \times W \to U$ gibt es genau eine lineare Abbildung $A : V \otimes W \to U$ mit

$$(x \otimes y)A = x \bullet y \qquad \text{für alle } x \in V \text{ und } y \in W. \tag{2.1}$$

Man kann zeigen, dass das Tensorprodukt zweier Vektorräume, sofern es existiert, bis auf Isomorphie eindeutig bestimmt ist. Im Allgemeinen gestaltet sich der Existenzbeweis kompliziert, wird jedoch deutlich einfacher, wenn man sich auf endlich-dimensionale Vektorräume V und W beschränkt. Der Rest dieses Abschnittes soll dazu dienen, für diesen leichteren Fall eine Konstruktion anzugeben und nachzuweisen, dass $V \otimes W$ unitär ist, wenn V und W unitär sind. Außerdem werden einige Zusammenhänge dargestellt, die für spätere Teile der Arbeit relevant sind.

Definition 2.3.3. Seien V und W endlich-dimensionale Vektorräume. $V \otimes W$ sei der Vektorraum aller Bilinearformen auf den Dualräumen von V und W, d.h.

$$V \otimes W = \{\Phi : \mathrm{Hom}(V, K) \times \mathrm{Hom}(W, K) \to K \mid \Phi \text{ ist bilinear}\}$$

zusammen mit den Operationen

$$\Phi + \Psi = (\varphi, \psi) \mapsto \Phi(\varphi, \psi) + \Psi(\varphi, \psi) \qquad \text{und} \qquad \lambda\Phi = (\varphi, \psi) \mapsto \lambda \cdot \Phi(\varphi, \psi).$$

$\otimes : V \times W \to V \otimes W$ sei die bilineare Abbildung, die jedem Paar von Vektoren $x \in V$ und $y \in W$ die Bilinearform $x \otimes y$ mit

$$x \otimes y = (\varphi, \psi) \mapsto (x\varphi) \cdot (y\psi)$$

zuordnet.

Sind $\{e_i\}_{i \in I}$ und $\{f_j\}_{j \in J}$ Basen von V und W, dann ist

$$\{e_i \otimes f_j\}_{i \in I, j \in J}$$

eine Basis von $V \otimes W$. Daraus folgt einerseits, dass $V \otimes W$ endlich-dimensional ist, genauer

$$\dim V \otimes W = \dim V \cdot \dim W,$$

und andererseits, dass die Menge

$$\{x \otimes y \mid x \in V, y \in W\}$$

ein Erzeugendensystem von $V \otimes W$ ist. Die Tensoren dieser Menge bezeichnet man als *elementare Tensoren*, $V \otimes W$ besteht jedoch im Allgemeinen aus weiteren Elementen.

Der nächste Schritt besteht darin, nachzuweisen, dass diese Konstruktion die geforderte Universalitätseigenschaft besitzt. Dazu sei $\bullet : V \times W \to U$ eine beliebige bilineare Abbildung. Es gilt zu zeigen, dass es genau eine lineare Abbildung $A : V \otimes W \to U$ gibt, die der Bedingung aus (2.1) genügt. Da diese Gleichung A auf einem Erzeugendensystem von $V \otimes W$ festlegt, ist die geforderte Eindeutigkeit gegeben.

Um die Existenz von A nachzuweisen, betrachte man die durch lineare Fortsetzung von

$$(e_i \otimes f_j)A = e_i \bullet f_j$$

definierte Abbildung $A : V \otimes W \to U$. Es lässt sich leicht überprüfen, dass diese (2.1) genügt. Mithin definiert die obige Konstruktion von $V \otimes W$ tatsächlich ein Tensorprodukt von V und W.

Sind $A : V \to V'$ und $B : B \to B'$ lineare Abbildungen, dann ist durch

$$V \otimes W \to V' \otimes W', \Phi \mapsto \big((\varphi, \psi) \mapsto \Phi(A\varphi, B\psi)\big)$$

eine lineare Abbildung definiert, die mit $A \otimes B$ bezeichnet wird. Es ergeben sich folgende „Rechenregeln“:

$$\begin{aligned}(x \otimes y)(A \otimes B) &= xA \otimes yB,\\ (A \otimes B)(A' \otimes B') &= AA' \otimes BB',\\ \mathrm{Id}_V \otimes \mathrm{Id}_W &= \mathrm{Id}_{V \otimes W}.\end{aligned}$$

Sind A und B Isomorphismen, dann ist $A \otimes B$ ebenfalls ein Ismorphismus und es gilt

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

Sind X und Y Unterräume von V bzw. W, dann ist die lineare Abbildung

$$X \otimes Y \to V \otimes W, \Phi \mapsto \big((\varphi, \psi) \mapsto \Phi(\varphi|_X, \psi|_Y)\big)$$

eine Einbettung, $X \otimes Y$ kann also als Unterraum von $V \otimes W$ aufgefasst werden.

Sind V und W unitäre Vektorräume und $\{e_i\}_{i \in I}$ bzw. $\{f_j\}_{j \in J}$ jeweils eine Basis, dann definierte die sesquilineare Fortsetzung von

$$\langle e_i \otimes f_j, e_k \otimes f_\ell \rangle = \langle e_i, e_k \rangle \cdot \langle f_j, f_\ell \rangle$$

ein Skalarprodukt auf $V \otimes W$, d.h. dieser Vektorraum ist ebenfalls unitär. Allgemeiner gilt für alle $x, x' \in V$ und $y, y' \in W$

$$\langle x \otimes y, x' \otimes y' \rangle = \langle x, x' \rangle \cdot \langle y, y' \rangle,$$

d.h. das Skalarprodukt ist unabhängig von der konkreten Wahl der Basen von V und

W. Sind A und B zwei Endomorphismen, dann gilt für die adjungierte Abbildung von $A \otimes B$:

$$(A \otimes B)^* = A^* \otimes B^*.$$

Damit folgt aus der Tatsache, dass A und B unitär (bzw. selbstadjungiert) sind, dass auch $A \otimes B$ unitär (bzw. selbstadjungiert) ist.

Sind X und Y Unterräume von V bzw. W und $P_X : V \to X$ und $P_Y : W \to Y$ die zugehörigen orthogonalen Projektionen, dann ist $P_X \otimes P_Y$ die orthogonale Projektion $P_{X \otimes Y}$ von $V \otimes W$ auf $X \otimes Y$:

$$P_{X \otimes Y} = P_X \otimes P_Y.$$

2.4 Monoide

2.4.1 Definitionen

Definition 2.4.1. Ein *Monoid* ist ein Paar $(M, \cdot)$, bestehend aus einer Menge M und einer binären Verknüpfung $\cdot : M \times M \to M$, mit folgenden Eigenschaften:

(1) $\cdot$ ist *assoziativ*, d.h. für alle $a, b, c \in M$ gilt

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(2) Es existiert ein bezüglich $\cdot$ *neutrales Element* $e \in M$, d.h. für alle $a \in M$ gilt

$$a \cdot e = a = e \cdot a.$$

Ein *Untermonoid vom* $(M, \cdot)$ ist eine Teilmenge $U \subseteq M$ mit $e \in U$, die bezüglich $\cdot$ abgeschlossen ist, d.h. es gilt $a \cdot b \in U$ für alle $a, b \in U$.

Bemerkung. Das neutrale Element eines Monoides ist eindeutig bestimmt und jedes Untermonoid eines Monoides ist selbst ein Monoid.

Wenn aus dem Kontext ersichtlich ist, welche binäre Verknüpfung auf M gemeint ist, schreibt man häufig ab statt $a \cdot b$ und bezeichnet das Monoid mit M anstelle von $(M, \cdot)$. In dieser Situation notiert man das neutrale Element als 1_M. Aufgrund der Assoziativität der Verknüpfung ist es außerdem üblich, Klammern auszulassen und abc statt $(ab)c$ oder $a(bc)$ zu schreiben, da beide Ausdrücke zum selben Wert führen.

Definition 2.4.2. Seien M ein Monoid, $X, Y \subseteq M$ und $m \in M$. Dann definiert man folgende Teilmengen von M:

$$\begin{aligned} XY &= \{mn \mid m \in X, n \in Y\}, \\ m^{-1}X &= \{n \in M \mid mn \in X\}, \\ Xm^{-1} &= \{n \in M \mid nm \in X\}. \end{aligned}$$

Man schreibt auch mX statt $\{m\}X$ und Xm statt $X\{m\}$.

Definition 2.4.3. Ein *(Monoid-)Homomorphismus* ist eine Abbildung $h : M \to M'$ zwischen Monoiden M und M', die folgenden Bedingungen genügt:

(1) h respektiert die neutralen Elemente, d.h. es gilt

$$h(1_M) = 1_{M'}.$$

(2) h ist verträglich mit den binären Verknüpfungen, d.h. für alle $a, b \in M$ gilt

$$h(ab) = h(a)h(b).$$

Ein *(Monoid-)Isomorphismus* ist ein bijektiver Monoid-Homomorphismus.

Bemerkung. Für jedes Monoid M ist die identische Abbildung Id_M ein Monoid-Isomorphismus, die Zusammensetzung zweier Monoid-Homomorphismen ist wieder ein Monoid-Homomorphismus und die Umkehrabbildung eines Monoid-Isomorphismus ist ebenfalls ein Monoid-Isomorphismus.

2.4.2 Spezielle Monoide

Definition 2.4.4. Sei Q eine beliebige Menge. $\mathrm{Abb}(Q)$ ist das Monoid aller Abbildungen von Q nach Q,

$$\mathrm{Abb}(Q) = \{f : Q \to Q \mid f \text{ ist Abildung}\},$$

zusammen mit der Nacheinanderausführung von Abbildungen

$$\mathrm{Abb}(Q) \times \mathrm{Abb}(Q) \to \mathrm{Abb}(Q), (f, g) \mapsto fg.$$

Das neutrale Element ist die identische Abbildung Id_Q.

Ist V ein beliebiger Vektorraum, dann ist die Menge $\mathrm{End}(V)$ aller linearen Abbildungen von V nach V,

$$\mathrm{End}(V) = \{A : V \to V \mid A \text{ ist lineare Abbildung}\},$$

ein Untermonoid von $\mathrm{Abb}(V)$. Ist V ein unitärer Vektorraum, dann ist die Menge $\mathrm{U}(V)$ aller unitären Abbildungen von V nach V,

$$\mathrm{U}(V) = \{A : V \to V \mid A \text{ ist unitäre Abbildung}\},$$

ein Untermonoid von $\mathrm{End}(V)$.

Definition 2.4.5. Sei Σ eine beliebige Menge. Die Menge Σ^* aller endlichen Folgen in Σ bildet zusammen mit der Konkatenation, dem Hintereinanderschreiben von Folgen, ein Monoid, welches *von* Σ *frei erzeugtes Monoid* heißt. Das neutrale Element dieses Monoids ist die leere Folge, welche mit ε bezeichnet wird.

Ist die Menge Σ endlich und nicht leer, dann bezeichnet man sie als *Alphabet* und die Elemente von Σ^* als *Worte*.

Ist $w = a_1 \dots a_n \in \Sigma^*$ ein beliebiges Wort, dann bezeichnet man n als *Länge von* w, in Zeichen $|w|$. Die Länge $|\varepsilon|$ des leeren Wortes ist 0.

Es ist leicht einzusehen, dass die Abbildung $|\cdot| : \Sigma^* \to \mathbb{N}, w \mapsto |w|$ ein Monoid-Homomorphismus von Σ^* nach $(\mathbb{N}, +)$ ist.

3 Gewichtete Automaten

Nachdem das vorangehende Kapitel die mathematischen Grundlagen dieser Arbeit gelegt hat, wird dieses darauf aufbauend die notwendigen automatentheoretischen Kenntnisse beisteuern. Es sei als eine Einführung in die Theorie der formalen Potenzreihen und gewichteten Automaten, die in gewisser Hinsicht die klassische Theorie der formalen Sprachen und endlichen Automaten verallgemeinert, verstanden. Das Hauptanliegen ist die Bereitstellung der notwendigen Begriffe und Konzepte für die nachfolgenden Kapitel. Die Darstellung orientiert sich dabei an [3] und [6].

Da gewichtete Automaten in gewisser Hinsicht eine Verallgemeinerung endlicher Automaten sind, werden Letztere in Abschnitt 3.1 kurz vorgestellt. Abschnitt 3.2 führt mit den formalen Potenzreihen die „Sprachen“ der Theorie der gewichteten Automaten ein. Direkt im Anschluss werden verschiedene Operationen auf formalen Potenzreihen definiert, die größtenteils den mengentheoretischen Operationen auf gewöhnlichen Sprachen nachempfunden sind. Die Vorstellung des zugehörigen Automatenmodells und Erkennbarkeitsbegriffs erfolgt in Abschnitt 3.3. Dort werden gewichtete Automaten sowie die Klasse der von ihnen erkennbaren Potenzreihen definiert und einige technische Aussagen bewiesen, die diese Konzepte betreffen.

Abschnitt 3.4 widmet sich der Konstruktion des Minimal-Automaten, anhand dessen man entscheiden kann, ob eine formale Potenzreihe im Sinne des vorher definierten Erkennbarkeitsbegriffs erkennbar ist. Schließlich wird in Abschnitt 3.5 untersucht, inwiefern die Klasse der erkennbaren Potenzreihen unter den im ersten Abschnitt vorgestellten Operationen abgeschlossen ist.

Da das vorliegende Kapitel einen gewissen Einführungscharakter besitzt, wird die Theorie der gewichteten Automaten weder annähernd vollständig noch in aller Allgemeinheit vorgestellt. Inbesondere werden lediglich formale Potenzreihen über Körpern statt – wie sonst üblich – über beliebigen Semiringen betrachtet. Dies ist einerseits dem Umstand geschuldet, dass die nachfolgenden Kapitel ausschließlich Automatenmodelle über Körpern untersuchen, andererseits entfällt so die Einführung einiger Begriffe. Außerdem werden Aussagen nur soweit bewiesen, wie die Beweise für den anschließenden Teil der Arbeit relevant oder zumindest ideengebend sind.

3.1 Ungewichtete Automaten über beliebigen Monoiden

An dieser Stelle erfolgt eine sehr kurze Einführung endlicher Automaten über beliebigen Monoiden, einer Verallgemeinerung gewöhnlicher endlicher Automaten, mit dem Ziel, Notationen für das Folgende bereitzustellen bzw. zu motivieren. Teilmengen $L \subseteq M$ eines Monoides M bezeichnet man als *Sprachen*. Ein *endlicher M-Automat* ist ein Quadrupel $\mathcal{A} = (Q, \delta, q_0, F)$, wobei Q eine endliche Menge von Zuständen, $\delta : M \to \mathrm{Abb}(Q)$

ein Monoid-Homomorphismus, die Transitionsabbildung, $q_0 \in Q$ der Initialzustand und $F \subseteq Q$ die Finalzustände sind. Die *von $\mathcal{A}$ akzeptierte Sprache* $L(\mathcal{A})$ ist durch

$$L(\mathcal{A}) = \{m \in M \mid q_0\delta(m) \in F\}$$

definiert. Ist $M = \Sigma^*$ ein freies Monoid, dann wird hierdurch ein vollständiger deterministischer endlicher Automat $\mathcal{A}$ definiert. Zudem handelt es sich um eine Formalisierung der informellen Beschreibung eines Automaten für Σ-Symbolfolgen in Kapitel 1.

Eine Sprache $L \subseteq M$ heißt *regulär*, wenn es einen endlichen M-Automaten $\mathcal{A}$ gibt mit

$$L = L(\mathcal{A}).$$

Ist $L \subseteq M$ eine reguläre Sprache, dann wird durch

$$Q_L = \{n^{-1}L \mid n \in M\}, \qquad (n^{-1}L)\delta_L(m) = (nm)^{-1}L \qquad \text{und} \qquad F_L = \{n^{-1}L \mid n \in L\}$$

ein endlicher M-Automat $\mathcal{A}_L = (Q_L, \delta_L, L, F_L)$ definiert. Dieser ist der zustandsminimale endliche M-Automat, der L akzeptiert, und heißt deswegen *Minimal-Automat von L*.

3.2 Formale Potenzreihen

Definition 3.2.1. Seien K ein Körper und M ein Monoid.

(1) Eine *formale M-Potenzreihe über K* ist eine Abbildung $f : M \to K$. Die Menge aller formalen M-Potenzreihen über K wird mit $K\langle\langle M\rangle\rangle$ bezeichnet,

$$K\langle\langle M\rangle\rangle = \{f : M \to K \mid f \text{ ist Abbildung}\}.$$

(2) Für eine formale Potenzreihe $f : M \to K$ heißt die Menge

$$\operatorname{supp}(f) = \{m \in M \mid f(m) \neq 0_K\}$$

Träger (engl.: support) von f.

(3) Eine formale Potenzreihe $f : M \to K$ heißt *formales M-Polynom über K*, wenn $\operatorname{supp}(f)$ endlich ist. $K\langle M\rangle$ bezeichne die Menge aller formalen M-Polynome über K,

$$K\langle M\rangle = \{f \in K\langle\langle M\rangle\rangle \mid \operatorname{supp}(f) \text{ ist endlich}\}.$$

Zusammen mit der komponentenweisen Addition $(f + g)(m) = f(m) + g(m)$ und der skalaren Multiplikation $(\lambda f)(m) = \lambda \cdot f(m)$ für $f, g \in K\langle\langle M\rangle\rangle$ und $\lambda \in K$ ist $K\langle\langle M\rangle\rangle$ ein K-Vektorraum. Aufgrund der Beziehungen

$$\operatorname{supp}(f + g) \subseteq \operatorname{supp}(f) \cup \operatorname{supp}(g) \qquad \text{und} \qquad \operatorname{supp}(\lambda f) \subseteq \operatorname{supp}(f)$$

ist $K\langle M\rangle$ ein Unterraum von $K\langle\langle M\rangle\rangle$. Die beiden Vektorräume fallen genau dann zusammen, wenn M endlich ist.

Zur Vereinfachung der Notation identifiziert man ein Monoidelement $m \in M$ häufig mit der charakteristischen Funktion $\chi_m : M \to K$ der Einpunktmenge $\{m\}$. Dadurch kann man m als formales M-Polynom mit

$$m(n) = \begin{cases} 1_K & \text{falls } n = m \\ 0_K & \text{sonst} \end{cases}$$

auffassen. Auf diese Weise kann man die Menge M in den K-Vektorraum $K\langle M\rangle$ einbetten und erhält eine Basis von $K\langle M\rangle$. Diese Tatsache wird im Folgenden häufig ohne explizite Erwähnung verwendet, um die Identität linearer Abbildungen nachzuweisen.

Der Rest dieses Abschnittes wird darauf verwendet, die wichtigsten Konstruktionen, die aus gegebenen formalen Potenzreihen neue Potenzreihen erzeugen, zu definieren.

Definition 3.2.2. Seien $f, g \in K\langle\langle M\rangle\rangle$. Die formalen Potenzreihen $f \odot g, f \cdot g \in K\langle\langle M\rangle\rangle$ mit

$$(f \odot g)(m) = f(m) \cdot g(m) \qquad \text{und} \qquad (f \cdot g)(m) = \sum_{\substack{m_1, m_2 \in M \\ m = m_1 m_2}} f(m_1) \cdot g(m_2)$$

heißen *Hadamard-Produkt* und *Cauchy-Produkt von f und g*.

Bemerkung. Bei der Definition des Cauchy-Produktes ist zu beachten, dass die Summe auf der rechten Seite im Allgemeinen nicht endlich und damit nicht definiert ist, also weitere Vorkehrungen getroffen werden müssen, um dies zu beheben. Sind f und g beide formale Polynome, dann existiert dieses Problem nicht. Anderenfalls besteht ein möglicher Ansatz in der Beschränkung auf solche Monoide M, für die sich jedes $m \in M$ nur auf endlich viele Arten in ein Produkt $m = n_1 n_2$ mit $n_1, n_2 \in M$ zerlegen lässt. Insbesondere freie Monoide besitzen diese Eigenschaft.

Für beliebige $f, g \in K\langle\langle M\rangle\rangle$ gilt (sofern $f \cdot g$ definiert ist)

$$\operatorname{supp}(f \odot g) = \operatorname{supp}(f) \cap \operatorname{supp}(g) \qquad \text{und} \qquad \operatorname{supp}(f \cdot g) \subseteq \operatorname{supp}(f) \operatorname{supp}(g),$$

der Raum $K\langle M\rangle$ ist also unter Hadamard- und Cauchy-Produkt abgeschlossen.

Definition 3.2.3. Seien $f \in K\langle\langle M\rangle\rangle$ und $n \in M$. Die Potenzreihen $n^{-1}f \in K\langle\langle M\rangle\rangle$ und $fn^{-1} \in K\langle\langle M\rangle\rangle$ mit

$$n^{-1}f(m) = f(nm) \qquad \text{und} \qquad fn^{-1}(m) = f(mn)$$

heißen *Links-* und *Rechtsableitung von f an der Stelle n*.

Für beliebige $f \in K\langle\langle M\rangle\rangle$ und $n \in M$ gilt

$$\operatorname{supp}(n^{-1}f) = n^{-1} \operatorname{supp}(f) \qquad \text{und} \qquad \operatorname{supp}(fn^{-1}) = \operatorname{supp}(f) n^{-1}.$$

Ist M ein Monoid, das den nach Definition 3.2.2 genannten Zusatzeigenschaften genügt, dann ist $K\langle M\rangle$ unter Links- und Rechtsableitung ebenfalls abgeschlossen.

Definition 3.2.4. Seien $f \in K\langle\langle M \rangle\rangle$ und $h : N \to M$ ein Monoid-Homomorphismus. Dann ist das *inverse Bild von f unter h* die formale N-Potenzreihe $h^{-1}(f) \in K\langle\langle N \rangle\rangle$ mit

$$h^{-1}(f)(n) = f(h(n)).$$

Definition 3.2.5. Seien $f \in K\langle\langle M \rangle\rangle$ und $h : M \to N$ ein Monoid-Homomorphismus. Dann ist das *homomorphe Bild von f unter h* die formale N-Potenzreihe $h(f) \in K\langle\langle N \rangle\rangle$ mit

$$h(f)(n) = \sum_{m \in h^{-1}(n)} f(m).$$

Bemerkung. Im Allgemeinen ist die Summe auf der rechten Seite unendlich und somit nicht definiert. Eine Möglichkeit der Behebung dieses Problems besteht in der Einschränkung auf solche Homorphismen, für die $h^{-1}(n)$ für jedes $n \in N$ endlich ist.

3.3 Gewichtete Automaten und Erkennbarkeit

Definition 3.3.1. Seien K ein Körper und M ein Monoid. Ein *gewichteter M-Automat über K* ist ein Quadrupel $\mathcal{A} = (A, \mu, a_0, \varphi)$ wobei

- A ein K-Vektorraum, der *Zustandsraum*,
- $\mu : M \to \mathrm{End}(K)$ ein Monoid-Homomorphismus, die *Transitionsabbildung*,
- $a_0 \in A$ der *Initialvektor* und
- $\varphi : A \to K$ eine Linearform, die *Finalabbildung* ist.

Der Automat $\mathcal{A}$ wird *endlich* genannt, wenn A endlich-dimensional ist.

Die *Erreichbarkeitsabbildung von $\mathcal{A}$* ist die Abbildung

$$r_{\mathcal{A}} : M \to A, m \mapsto a_0\mu(m).$$

Der Automat $\mathcal{A}$ wird *erreichbar* genannt, wenn $r_{\mathcal{A}}(M)$ ein Erzeugendensystem von A ist.

Das *Verhalten von $\mathcal{A}$* bzw. die *von $\mathcal{A}$ erkannte formale Potenzreihe* $|\mathcal{A}| \in K\langle\langle M \rangle\rangle$ ist durch

$$|\mathcal{A}|\,(m) = r_{\mathcal{A}}(m)\varphi$$

definiert.

Bemerkung. Ist $M = \Sigma^*$ ein freies Monoid, dann fällt diese Definition im Wesentlichen mit der einer linearen Darstellung [3, S. 10] zusammen. Dazu fixiere man eine Basis von A und fasse a_0 als $1 \times n$-Matrix, $\mu(m)$ als $n \times n$-Matrix und φ als $n \times 1$-Matrix bezüglich dieser Basis auf, wobei $n = \dim A$ sei.

Der zu diesem Automatenmodell gehörende Erkennbarkeitsbegriff ist folgender:

Definition 3.3.2. Eine formale Potenzreihe $f \in K\langle\langle M \rangle\rangle$ heißt *erkennbar*, wenn es einen endlichen gewichteten M-Automaten $\mathcal{A}$ gibt, der f erkennt, d.h.

$$f = |\mathcal{A}|\,.$$

Die Menge aller erkennbaren formalen M-Potenzreihen über K wird mit $K^{\mathrm{rec}}\langle\langle M \rangle\rangle$ bezeichnet,

$$K^{\mathrm{rec}}\langle\langle M \rangle\rangle = \{f \in K\langle\langle M \rangle\rangle \mid f \text{ ist erkennbar}\}.$$

Da eingehend erwähnt wurde, dass gewichtete Automaten das Konzept der endlichen Automaten verallgemeinern, zeigt das folgende Beispiel auf, in welcher Weise das geschieht.

Beispiel 3.3.3. Seien $L \subseteq M$ eine reguläre Sprache und $\mathcal{B} = (Q, \delta, q_0, F)$ ein endlicher M-Automat der L akzeptiert. O.B.d.A. gelte dabei $Q = \{1, \ldots, n\}$. Dann sei $\mathcal{A} = (A, \mu, a_0, \varphi)$ der folgendermaßen definierte gewichtete M-Automat:

- A ist der Vektorraum $A = K^n$ mit der kanonischen Basis $e_1, \ldots, e_n$,
- $\mu(m) : A \to A$ ist die lineare Fortsetzung von

$$e_i\mu(m) = e_{i\delta(m)},$$

- $a_0 = e_{q_0}$ und
- $\varphi : A \to K$ ist die Fortsetzung von

$$e_i\varphi = \begin{cases} 1 & \text{falls } i \in F \\ 0 & \text{sonst} \end{cases}$$

  zu einer Linearform.

Einfache Rechnungen zeigen, dass auf diese Weise tatsächlich ein Monoid-Homomorphismus μ definiert wird.

Da für alle $m \in M$ gilt

$$|\mathcal{A}|\,(m) = e_{q_0}\mu(m)\varphi = e_{q_0\delta(m)}\varphi = \begin{cases} 1 & \text{falls } q_0\delta(m) \in F \\ 0 & \text{sonst} \end{cases},$$

erkennt der gewichtete Automat $\mathcal{A}$ gerade die charakteristische Funktion χ_L von L.

Das nachstehende Lemma zeigt einen Weg auf, einen beliebigen gewichteten Automaten in einen erreichbaren gewichteten Automaten umzuformen, der dasselbe Verhalten hat und außerdem endlich ist, wenn der Ausgangsautomat endlich war. Dies ermöglicht es, im Folgenden davon auszugehen, dass gewichtete Automaten stets erreichbar sind.

Lemma 3.3.4. *Seien $f \in K\langle\langle M \rangle\rangle$ und $\mathcal{A}$ ein gewichteter Automat, der f erkennt. Dann existiert ein gewichteter Automat $\mathcal{A}'$, der f ebenfalls erkennt und dessen Zustandsraum eine höchstens so große Dimension besitzt wie derjenige von $\mathcal{A}$.*

Beweis. Sei $\mathcal{A} = (A, \mu, a_0, \varphi)$ der gewichtete Automat, der f erkennt. A' sei der von den $r_{\mathcal{A}}(m)$ erzeugte Unterraum von A

$$A' = \langle r_{\mathcal{A}}(m) \mid m \in M \rangle.$$

Wegen $a_0 = r_{\mathcal{A}}(1_M)$ gilt $a_0 \in A'$. Ist $a \in A'$, dann existierten $\lambda_1, \ldots, \lambda_k \in K$ und $m_1, \ldots, m_k \in M$ mit

$$a = \sum_{i=1}^{k} \lambda_i r_{\mathcal{A}}(m_i).$$

Daraus folgt für alle $m \in M$

$$a\mu(m) = \sum_{i=1}^{k} \lambda_i r_{\mathcal{A}}(m_i)\mu(m) = \sum_{i=1}^{k} \lambda_i r_{\mathcal{A}}(m_i m),$$

also $a\mu(m) \in A'$. Damit ist die Abbildung

$$\mu' : M \to \mathrm{End}(A'), m \mapsto \mu(m)|_{A'}$$

wohldefiniert und außerdem ein Monoid-Homomorphismus. Schließlich rechnet man leicht nach, dass das Verhalten von $\mathcal{A}' = (A', \mu', a_0, \varphi|_{A'})$ genau f ist. Da A' ein Unterraum von A ist, folgt aus der Endlichkeit von $\mathcal{A}$ die von $\mathcal{A}'$. □

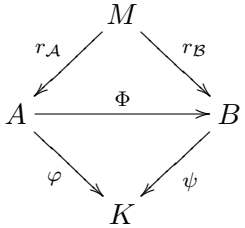
Korollar 3.3.5. *Eine formale Potenzreihe $f \in K\langle\langle M \rangle\rangle$ ist genau dann erkennbar, wenn sie von einem erreichbaren, endlichen gewichteten M-Automaten erkannt wird.*

Schließlich soll hier noch der Begriff der „Gleichheit“ zweier gewichteter Automaten eingeführt werden, der für die Konstruktion des Mininmal-Automaten im nächsten Abschnitt wichtig ist.

Definition 3.3.6. Zwei gewichtete M-Automaten $\mathcal{A} = (A, \mu, a_0, \varphi)$ und $\mathcal{B} = (B, \nu, b_0, \psi)$ über K heißen *isomorph*, in Zeichen

$$\mathcal{A} \cong \mathcal{B},$$

wenn es einen K-Vektorraum-Isomorphismus $\Phi : A \to B$ gibt, so dass folgendes Diagramm kommutiert:



Bemerkung. Isomorphe gewichtete Automaten haben offensichtlich dasselbe Verhalten. Ist einer der beiden Automaten erreichbar, dann ist es der andere auch, und der Vek-

torraum-Isomorphismus Φ ist in dieser Situation eindeutig bestimmt, da er durch das Diagramm auf einem Erzeugendensystem festgelegt wird.

3.4 Der Minimal-Automat

Für eine gegebene formale Potenzreihe $f \in K\langle\langle M \rangle\rangle$ konstruiert man den gewichteten Automaten mit Verhalten f, für den die Dimension des Zustandsraumes minimal ist – ähnlich wie für reguläre Sprachen – mithilfe der Linksableitungen von f.

Konstruktion 3.4.1. Sei $f \in K\langle\langle M \rangle\rangle$ eine formale Potenzreihe. Den gewichteten M-Automaten $\mathcal{A}_f = (A_f, \mu_f, f, \varphi_f)$ mit

- A_f ist der von den Linksableitungen von f erzeugte Unterraum von $K\langle\langle M \rangle\rangle$

$$A_f = \langle m^{-1}f \mid m \in M \rangle,$$

- $\mu_f : M \to \mathrm{End}(A_f)$ ist der wie folgt definierte Monoid-Homomorphismus

$$g\mu_f(m) = m^{-1}g,$$

- $\varphi_f : A_f \to K$ ist die wie folgt definierte Linearform

$$g\varphi_f = g(1_M),$$

bezeichnet man als *den Minimal-Automaten von f.*

Der Rest dieses Abschnitts dient dem Nachweis, dass der Begriff „der Minimal-Automat von f“ berechtigt ist. Zunächst rechnet man leicht nach, dass es sich bei $\mathcal{A}_f$ um einen gewichteten M-Automaten handelt. Dass das Verhalten von $\mathcal{A}_f$ genau f ist, zeigt folgendes Lemma:

Lemma 3.4.2. *Sei $f \in K\langle\langle M \rangle\rangle$ eine formale Potenzreihe. Dann ist $\mathcal{A}_f$ ein erreichbarer gewichteter M-Automat, der f erkennt.*

Beweis. Die Erreichbarkeit von $\mathcal{A}_f$ folgt aus $r_{\mathcal{A}_f}(m) = m^{-1}f$ und der Wahl von A_f. Weiter gilt für $m \in M$

$$|\mathcal{A}_f|\,(m) = r_{\mathcal{A}_f}(m)\varphi_f = (m^{-1}f)\varphi_f = (m^{-1}f)(1_M) = f(m). \qquad \square$$

Der nächste Schritt des Beweises besteht in der Angabe einer Konstruktion, die aus einem gegebenen gewichteten Automaten einen reduzierten gewichteten Automaten mit demselben Verhalten erzeugt.

Konstruktion 3.4.3. Sei $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein gewichteter M-Automat. Der *Reduktionsautomat von $\mathcal{A}$* ist der gewichtete M-Automat $\mathrm{red}(\mathcal{A}) = (A/B, \mu', a_0\rho, \varphi')$ mit:

- B ist der Unterraum

$$B = \{a \in A \mid \forall m \in M : a\mu(m)\varphi = 0\}$$

  von A und $\rho : A \to A/B$ die natürliche Abbildung in den Faktorraum.

- $\mu' : M \to \mathrm{End}(A/B)$ ist der Monoid-Homomorphismus mit

$$(a + B)\mu'(m) = a\mu(m) + B.$$

- $\varphi' : A/B \to K$ ist die Linearform mit

$$(a + B)\varphi' = a\varphi. \tag{3.1}$$

Zunächst gilt es nachzuweisen, dass diese Konstruktion wohldefiniert ist und einen gewichteten M-Automaten liefert. Da

$$B = \bigcap_{m \in M} \ker(\mu(m)\varphi)$$

gilt, ist B tatsächlich ein Unterraum von A. Für $a, a' \in A$ und $m \in M$ gilt:

$$\begin{aligned} a + B = a' + B &\Longrightarrow a - a' \in B \\ &\Longrightarrow \forall n \in M : (a\mu(m) - a'\mu(m))\mu(n)\varphi = (a - a')\mu(mn)\varphi = 0 \\ &\Longrightarrow a\mu(m) - a'\mu(m) \in B \\ &\Longrightarrow a\mu(m) + B = a'\mu(m) + B, \end{aligned}$$

d.h. die Abbildung $\mu'(m) : A/B \to A/B$ ist wohldefiniert. Dass μ' sogar ein Monoid-Homomorphismus ist, rechnet man leicht nach. Schließlich gilt $B \subseteq \ker(\mu(1_M)\varphi) = \ker\varphi$, also ist φ' wohldefiniert und eine Linearform.

Der so konstruierte gewichtete M-Automat $\mathrm{red}(\mathcal{A})$ hat dasselbe Verhalten wie $\mathcal{A}$:

Lemma 3.4.4. *Sei $\mathcal{A}$ ein gewichteter M-Automat. Dann gilt*

$$|\mathrm{red}(\mathcal{A})| = |\mathcal{A}|.$$

Ist $\mathcal{A}$ erreichbar, dann ist auch $\mathrm{red}(\mathcal{A})$ erreichbar.

Beweis. Seien die Bezeichnungen wie in Konstruktion 3.4.3. Es gilt für alle $m \in M$

$$r_{\mathrm{red}(\mathcal{A})}(m) = (a_0 + B)\mu'(m) = (a_0\mu(m) + B) = r_{\mathcal{A}}(m)\rho \tag{3.2}$$

und damit

$$|\mathrm{red}(\mathcal{A})|(m) = r_{\mathrm{red}(\mathcal{A})}(m)\varphi' = r_{\mathcal{A}}(m)\rho\varphi' = r_{\mathcal{A}}(m)\varphi = |\mathcal{A}|(m).$$

Wenn die Vektoren $r_{\mathcal{A}}(m)$ ein Erzeugendensystem von A bilden, dann erzeugen die

$r_{\mathrm{red}(\mathcal{A})}(m)$ aufgrund von Gleichung (3.2) den Faktorraum A/B, d.h. aus der Erreichbarkeit von $\mathcal{A}$ folgt diejenige von $\mathrm{red}(\mathcal{A})$. □

Proposition 3.4.5. *Seien $f \in K\langle\langle M\rangle\rangle$ und $\mathcal{A}$ ein erreichbarer gewichteter M-Automat, der f erkennt. Dann gilt*

$$\mathrm{red}(\mathcal{A}) \cong \mathcal{A}_f.$$

Beweis. Die Bezeichnungen seien wie in den Konstruktionen 3.4.1 und 3.4.3 gewählt. Weiter sei für jedes $a \in A$ eine formale Potenzreihe $f_a \in K\langle\langle M\rangle\rangle$ durch

$$f_a(m) = a\mu(m)\varphi$$

definiert. Einfache Rechnungen zeigen, dass $\Psi : A \to K\langle\langle M\rangle\rangle, a \mapsto f_a$ ein Vektorraumhomomorphismus mit $\ker\Psi = B$ ist. Für alle $n \in M$ gilt

$$(m^{-1}f)(n) = f(mn) = r_{\mathcal{A}}(mn)\varphi = r_{\mathcal{A}}(m)\mu(n)\varphi = f_{r_{\mathcal{A}}(m)}(n),$$

also

$$m^{-1}f = f_{r_{\mathcal{A}}(m)} = r_{\mathcal{A}}(m)\Psi.$$

Da $\mathcal{A}$ erreichbar ist, bilden die $r_{\mathcal{A}}(m)$ ein Erzeugendensystem von A und somit die $r_{\mathcal{A}}(m)\Psi$ eines von $\mathrm{im}\Psi$. Es gilt also

$$\mathrm{im}\Psi = \langle r_{\mathcal{A}}(m)\Psi \mid m \in M\rangle = \langle m^{-1}f \mid m \in M\rangle = A_f.$$

Laut Isomorphiesatz für Vektorräume existiert damit ein Vektorraum-Isomorphismus $\Phi : A/B \to A_f$ mit $\rho\Phi = \Psi$.

Wie folgende zwei Gleichungen zeigen, kommutiert das Diagramm aus Definition 3.3.6 für $\mathrm{red}(\mathcal{A}) \cong \mathcal{A}_f$ mit dieser Wahl von Φ:

$$r_{\mathrm{red}(\mathcal{A})}(m)\Phi = r_{\mathcal{A}}(m)\rho\Phi = r_{\mathcal{A}}(m)\Psi = m^{-1}f = r_{\mathcal{A}_f}(m)$$

und

$$a\rho\Phi\varphi_f = a\Psi\varphi_f = f_a\varphi_f = f_a(1_M) = a\mu(1_M)\varphi = a\rho\varphi'.$$ □

Ist $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein gewichteter Automat, der eine formale Potenzreihe $f \in K\langle\langle M\rangle\rangle$ erkennt, dann folgt aus Lemma 3.3.4 und Proposition 3.4.5, dass $\dim A_f \leq \dim A$, d.h. die Dimension von $\mathcal{A}_f$ ist tatsächlich minimal. Es gilt also folgender Satz:

Satz 3.4.6. *Eine formale Potenzreihe $f \in K\langle\langle M\rangle\rangle$ ist genau dann erkennbar, wenn $\mathcal{A}_f$ endlich ist.*

Der letzte Schritt der Rechtfertigung des Begriffs „der Minimal-Automat von f“ besteht im Beweis der Eindeutigkeit des minimalen Automaten bis auf Isomorphie.

Proposition 3.4.7. *Seien $f \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$ eine erkennbare Potenzreihe und $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein gewichteter M-Automat, der f erkennt, mit $\dim A = \dim A_f$. Dann gilt*

$$\mathcal{A} \cong \mathcal{A}_f.$$

Beweis. Aufgrund von Lemma 3.3.4 ist $\mathcal{A}$ erreichbar. Nach Proposition 3.4.5 gilt demnach $\mathrm{red}(\mathcal{A}) \cong \mathcal{A}_f$, also insbesondere

$$\dim A/B = \dim A_f = \dim A,$$

d.h. die natürliche Abbildung $\rho : A \to A/B$ ist ein Vektorraum-Isomorphismus. Die Gleichungen (3.1) und (3.2) zeigen, dass die Wahl $\Phi = \rho$ das Diagram aus Definition 3.3.6 für $\mathcal{A} \cong \mathrm{red}(\mathcal{A})$ kommutativ macht. Zusammensetzen der Diagramme für $\mathcal{A} \cong \mathrm{red}(\mathcal{A})$ und $\mathrm{red}(\mathcal{A}) \cong \mathcal{A}_f$ liefert die Behauptung. □

3.5 Abschlusseigenschaften

Lemma 3.5.1. *Sei $\lambda \in K$. Dann ist die formale Potenzreihe $f_\lambda \in K\langle\langle M\rangle\rangle$ mit $f_\lambda(m) = \lambda$ erkennbar.*

Beweis. Sei $\mathcal{A} = (K, \mu, \lambda, \mathrm{Id})$ der endliche gewichtete Automat mit $\mu(m) = \mathrm{Id}$ für alle $m \in M$. Dann gilt

$$|\mathcal{A}|(m) = \lambda\mu(m)\varphi = \lambda = f_\lambda(m). \qquad \square$$

Lemma 3.5.2. *Seien $f \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$ und $n \in M$. Dann gilt $n^{-1}f \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$ und $fn^{-1} \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$.*

Beweis. Sei $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein endlicher gewichteter Automat der f erkennt. Dann gilt für die Automaten $\mathcal{A}_1 = (A, \mu, a_0\mu(n), \varphi)$ und $\mathcal{A}_2 = (A, \mu, a_0, \mu(n)\varphi)$

$$\begin{aligned} |\mathcal{A}_1|(m) &= a_0\mu(n)\mu(m)\varphi = a_0\mu(nm)\varphi = f(nm) = (n^{-1}f)(m) \quad \text{und} \\ |\mathcal{A}_2|(m) &= a_0\mu(m)\mu(n)\varphi = a_0\mu(mn)\varphi = f(mn) = (fn^{-1})(m). \end{aligned} \qquad \square$$

Lemma 3.5.3. *Für $f_1, f_2 \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$ gilt $f_1 + f_2 \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$.*

Beweis. Seien $\mathcal{A}_i = (A_i, \mu_i, a_{0i}, \varphi_i)$ endliche gewichtete Automaten mit $|\mathcal{A}_i| = f_i$ für $i = 1, 2$. Dann gilt für den Automaten $\mathcal{A} = (A_1 \oplus A_2, \mu, a_{01} \oplus a_{02}, \varphi)$ mit $\mu(m) = \mu_1(m) \oplus \mu_2(m)$ und $(a_1 \oplus a_2)\varphi = a_1\varphi_1 + a_2\varphi_2$:

$$|\mathcal{A}|(m) = (a_{01} \oplus a_{02})\mu(m)\varphi = a_{01}\mu_1(m)\varphi_1 + a_{02}\mu_2(m)\varphi_2 = f_1(m) + f_2(m). \qquad \square$$

Lemma 3.5.4. *Für $f_1, f_2 \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$ gilt $f_1 \odot f_2 \in K^{\mathrm{rec}}\langle\langle M\rangle\rangle$.*

Beweis. Seien $\mathcal{A}_i = (A_i, \mu_i, a_{0i}, \varphi_i)$ endliche gewichtete Automaten mit $|\mathcal{A}_i| = f_i$ für $i = 1, 2$. Dann ist die Abbildung $A_1 \times A_2 \to K, (a_1, a_2) \mapsto (a_1\varphi_2) \cdot (a_2\varphi_2)$ bilinear und aufgrund der Universalitätseigenschaft des Tensorproduktes existiert eine lineare

Abbildung $\varphi : A_1 \otimes A_2 \to K$ mit $(a_1 \otimes a_2)\varphi = (a_1\varphi_1) \cdot (a_2\varphi_2)$. Dann gilt für den gewichteten Automaten $\mathcal{A} = (A_1 \otimes A_2, \mu, a_{01} \otimes a_{02}, \varphi)$ mit $\mu(m) = \mu_1(m) \otimes \mu_2(m)$:

$$|\mathcal{A}|(m) = (a_{01} \otimes a_{02})\mu(m)\varphi = (a_{01}\mu_1(m)\varphi_1) \cdot (a_{02}\mu_2(m)\varphi_2) = f_1(m) \cdot f_2(m). \qquad \square$$

Aus den Lemmata 3.5.1 und 3.5.4 folgt direkt:

Korollar 3.5.5. *Für $f \in K^{\mathrm{rec}}\langle\langle M \rangle\rangle$ und $\lambda \in K$ gilt $\lambda f \in K^{\mathrm{rec}}\langle\langle M \rangle\rangle$.*

Aus den letzten fünf Aussagen folgt insgesamt:

Satz 3.5.6. *$K^{\mathrm{rec}}\langle\langle M \rangle\rangle$ ist ein Unterraum von $K\langle\langle M \rangle\rangle$, der die konstanten formalen Potenzreihen enthält und unter Hadamard-Produkt sowie Links- und Rechtsableitungen abgeschlossen ist.*

Satz 3.5.7. *Seien $f \in K^{\mathrm{rec}}\langle\langle M \rangle\rangle$ und $h : N \to M$ ein Monoid-Homomorphismus. Dann gilt $h^{-1}(f) \in K^{\mathrm{rec}}\langle\langle N \rangle\rangle$.*

Beweis. Sei $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein endlicher gewichteter Automat der f erkennt. Dann gilt für den Automaten $\mathcal{A}' = (A, \mu \circ h, a_0, \varphi)$

$$\left|\mathcal{A}'\right|(m) = a_0\mu(h(m))\varphi = f(h(m)). \qquad \square$$

Beweise für die beiden folgenden Sätze findet man beispielsweise in [3].

Satz 3.5.8. *Seien Σ und Γ Alphabete, $f \in K^{\mathrm{rec}}\langle\langle \Sigma^* \rangle\rangle$ und $h : \Sigma^* \to \Gamma^*$ ein* längenerhaltender *Monoid-Homomorphismus, d.h. es gilt*

$$|h(w)| = |w| \text{ für alle } w \in \Sigma^*.$$

Dann gilt $h(f) \in K^{\mathrm{rec}}\langle\langle \Gamma^* \rangle\rangle$.

Satz 3.5.9. *Seien Σ ein Alphabet und $f, g \in K^{\mathrm{rec}}\langle\langle \Sigma^* \rangle\rangle$. Dann ist $f \cdot g$ wohldefiniert und es gilt $f \cdot g \in K^{\mathrm{rec}}\langle\langle \Sigma^* \rangle\rangle$.*

4 Beschränkte Potenzreihen

Ausgangspunkt für Bozapalidis' Untersuchungen in [6] zu stochastischen Funktionen (siehe [15]) und quantenerkennbaren Sprachen (siehe Kapitel 5) war die Tatsache, dass für beide ein Cut-Point-Theorem gilt. Sein Ziel war es, eine größtmögliche Klasse von formalen Potenzreihen zu finden, die drei Anforderungen erfüllt:

1. es gilt ein Cut-Point-Theorem,
2. sie enthält die beiden genannten Klassen formaler Potenzreihen als Spezialfälle und
3. sie verfügt über gute Abschlusseigenschaften.

Dazu hat er das Konzept der *beschränkten Moduln* eingeführt, mit deren Hilfe die Klasse der *beschränkt-erkennbaren Potenzreihen* definiert und nachgewiesen, dass sie alle drei Eigenschaften besitzt. Weiterhin hat er festgestellt, dass beschränkt-erkennbare Potenzreihen sowohl beschränkt als auch erkennbar sind, sich jedoch nicht mit der umgekehrten Fragestellung beschäftigt.

Dieses Kapitel widmet sich daher, neben der Darstellung von Bozapalidis' Resultaten, auch der Beanwortung der noch offenen Frage nach der Umkehrung. Das Konzept der beschränkten Moduln wird dabei einerseits in die Sprache der Automatentheorie übersetzt und andererseits so verallgemeinert, dass die Handhabung einfacher wird, sich die Klasse der von ihnen erkannten Sprachen jedoch nicht ändert. Die Ergebnisse des Kapitels sind eine Charakterisierung der beschränkt-erkennbaren Potenzreihen sowie der Beweis des zugehörigen Cut-Point-Theorems.

Da im Folgenden sowohl Beschränktheit als auch normierte Vektorräume eine Rolle spielen, sei K für den Rest des Kapitels einer der Körper $\mathbb{R}$ oder $\mathbb{C}$.

4.1 Beschränkte Potenzreihen

Eine formale Potenzreihe $f \in K\langle\langle M \rangle\rangle$ heißt im Sinne von Definition 2.1.2 *beschränkt*, wenn es eine Konstante $C > 0$ gibt, so dass für alle $m \in M$ gilt

$$|f(m)| \leq C.$$

Definition 4.1.1. Die Menge der beschränkten erkennbaren Potenzreihen wird mit $K^{\mathrm{brec}}\langle\langle M \rangle\rangle$ bezeichnet,

$$K^{\mathrm{brec}}\langle\langle M \rangle\rangle = \{f \in K^{\mathrm{rec}}\langle\langle M \rangle\rangle \mid f \text{ ist beschränkt}\}.$$

In Anlehnung an Satz 3.5.6 über erkennbare Potenzreihen kann man folgenden Satz über beschränkte erkennbare Potenzreihen formulieren:

Satz 4.1.2. *$K^{\mathrm{brec}}\langle\langle M\rangle\rangle$ ist ein Unterraum von $K\langle\langle M\rangle\rangle$, der die konstanten formalen Potenzreihen enthält und unter Hadamard-Produkt sowie Links- und Rechtsableitungen abgeschlossen ist.*

Beweis. Laut Satz 3.5.6 erhalten die oben genannten Operationen die Erkennbarkeit, es reicht also zu zeigen, dass sie auch die Beschränktheit erhalten. Dazu seien $f, g \in K^{\mathrm{brec}}\langle\langle M\rangle\rangle$ Potenzreihen, die durch C bzw. D beschränkt sind, d.h. für alle $m \in M$ gelte

$$|f(m)| \leq C \qquad \text{und} \qquad |g(m)| \leq D.$$

Dann ist λf für $\lambda \in K$ durch $|\lambda| \cdot C$ beschränkt, $f+g$ durch $C+D$, $f \odot g$ durch $C \cdot D$ sowie $n^{-1}f$ und fn^{-1} für $n \in M$ durch C. Außerdem ist die konstante formale Potenzreihe $f_c(m) = c$ durch $|c|$ beschränkt. □

Auch Satz 3.5.7 lässt sich auf den Fall beschränkter erkennbarer Potenzreihen übertragen.

Satz 4.1.3. *Seien $f \in K^{\mathrm{brec}}\langle\langle M\rangle\rangle$ und $h : N \to M$ ein Monoid-Homomorphismus. Dann gilt $h^{-1}(f) \in K^{\mathrm{brec}}\langle\langle N\rangle\rangle$.*

Beweis. Die Erkennbarkeit von $h^{-1}(f)$ wurde bereits in Satz 3.5.7 gezeigt, es reicht also, die Beschränktheit nachzuweisen. Ist $C > 0$ eine Konstante, die f beschränkt, dann gilt für alle $m \in M$

$$\left|h^{-1}(f)(m)\right| = |f(h(m))| \leq C,$$

d.h. $h^{-1}(f)$ ist tatsächlich beschränkt. □

Die Frage, ob sich auch die Sätze 3.5.8 und 3.5.9 auf den Fall beschränkter erkennbarer Potenzreihen übertragen lassen, hat eine negative Antwort. Dazu betrachte man die Alphabete $\Sigma = \{a, b\}$ und $\Gamma = \{c\}$, die beschränkte erkennbare formale Potenzreihe $f \in K^{\mathrm{brec}}\langle\langle \Sigma^*\rangle\rangle$ mit $f(w) = 1$ für alle $w \in \Sigma^*$ und den längenerhaltenden Monoid-Homomorphismus $h : \Sigma^* \to \Gamma^*, x \mapsto c^{|x|}$. Dann gilt für alle $n \in \mathbb{N}$

$$h(f)(c^n) = \sum_{w \in h^{-1}(c^n)} f(w) = \sum_{w \in \Sigma^n} 1 = 2^n$$

und

$$(f \cdot f)(a^n) = \sum_{\substack{u,v \in \Sigma^* \\ uv = a^n}} f(u) \cdot f(v) = \sum_{k=0}^{n} f\left(a^k\right) \cdot f\left(a^{n-k}\right) = n + 1,$$

d.h. $h(f)$ und $f \cdot f$ sind beide nicht beschränkt.

4.2 Beschränkte Automaten

Als nächstes wird ein Automatenmodell eingeführt, von dem sich herausstellen wird, dass es gerade die beschränkten erkennbaren Potenzreihen erkennt. Diese sogenannten *beschränkten gewichteten Automaten* sind die bereits erwähnte Übertragung von Bozapalidis' beschränkten Moduln in die Sprache der Automatentheorie.

Definition 4.2.1. Ein gewichteter Automat $\mathcal{A} = (A, \mu, a_0, \varphi)$ heißt *beschränkt*, wenn A ein normierter Vektorraum und die Erreichbarkeitsabbildung $r_\mathcal{A}$ bezüglich der Norm auf A beschränkt ist.

Bemerkung. Aufgrund von Satz 2.1.4 ist es im Falle endlicher gewichteter Automaten unerheblich, welche Norm auf dem Zustandsraum betrachtet wird, da die Erreichbarkeitsabbildung entweder bezüglich aller oder gar keiner Norm beschränkt ist.

Ist $\mathcal{A} = (A, \mu, a_0, \varphi)$ ein endlicher beschänkter Automat, $f = |\mathcal{A}| \in K^{\mathrm{rec}}\langle\langle M \rangle\rangle$ die von ihm erkannte Potenzreihe und $c(\mathcal{A}) > 0$ eine Konstante, die $r_\mathcal{A}$ beschränkt, dann gilt für alle $m \in M$

$$|f(m)| = |r_\mathcal{A}(m)\varphi| \leq c(\varphi) \cdot \|r_\mathcal{A}(m)\| \leq c(\varphi) \cdot c(\mathcal{A}), \tag{4.1}$$

wobei $c(\varphi)$ die Konstante sei, deren Existenz Korollar 2.1.5 garantiert. Von endlichen beschränkten Automaten erkannte Potenzreihen sind also stets beschränkt. Umgekehrt stellt sich nun die Frage, ob jede beschränkte erkennbare Potenzreihe von einem endlichen beschränkten Automaten erkannt wird. Die Antwort liefert das nachstehende Lemma.

Lemma 4.2.2. *Für $f \in K^{\mathrm{brec}}\langle\langle M \rangle\rangle$ ist $\mathcal{A}_f$ beschränkt.*

Beweis. Aufgrund von Satz 4.1.2 gilt zunächst

$$\{m^{-1}f \mid m \in M\} \subseteq K^{\mathrm{brec}}\langle\langle M \rangle\rangle$$

und schließlich

$$A_f = \langle m^{-1}f \mid m \in M \rangle \subseteq K^{\mathrm{brec}}\langle\langle M \rangle\rangle,$$

d.h. alle Potenzreihen aus A_f sind beschränkt. Dies ermöglicht die Definition einer Abbildung

$$\|\cdot\| : A_f \to \mathbb{R}_{\geq 0}, g \mapsto \sup_{m \in M} |g(m)|\,.$$

Bei dieser handelt es sich um eine Norm auf A_f, wie die folgenden Überlegungen zeigen. Für alle $g \in A_f$ gilt

$$\begin{aligned} \|g\| = 0 \quad &\iff \quad \sup_{m \in M} |g(m)| = 0 \quad &&\iff \quad \forall m \in M : |g(m)| = 0 \\ &\iff \quad \forall m \in M : g(m) = 0 \quad &&\iff \quad g = 0. \end{aligned}$$

Weiterhin gilt für $\lambda \in K$ und $g \in A_f$

$$\|\lambda g\| = \sup_{m \in M} |\lambda g(m)| = \sup_{m \in M} \big(|\lambda| \cdot |g(m)|\big) = |\lambda| \cdot \sup_{m \in M} |g(m)| = |\lambda| \cdot \|g\|$$

sowie für $g, h \in A_f$

$$\begin{aligned}\|g+h\| &= \sup_{m\in M} |g(m)+h(m)| \\ &\leq \sup_{m\in M} \big(|g(m)|+|h(m)|\big) \leq \sup_{m\in M} |g(m)| + \sup_{m\in M} |h(m)| = \|g\| + \|h\|\,.\end{aligned}$$

Damit ist gezeigt, dass A_f ein normierter Vektorraum ist. Schließlich gilt für alle $m \in M$

$$\big\|r_{\mathcal{A}_f}(m)\big\| = \big\|m^{-1}f\big\| = \sup_{n\in M} \big|m^{-1}f(n)\big| = \sup_{n\in M} |f(mn)| \leq \sup_{n\in M} |f(n)| = \|f\|\,,$$

d.h. $r_{\mathcal{A}_f}$ ist beschränkt und $\mathcal{A}_f$ somit ein beschränkter Automat. □

Daraus folgt schlussendlich die nachstehende Charakterisierung der Menge $K^{\mathrm{brec}}\langle\langle M\rangle\rangle$:

Satz 4.2.3. *Für $f \in K\langle\langle M\rangle\rangle$ sind äquivalent:*

(1) f ist erkennbar und beschränkt, also $f \in K^{\mathrm{brec}}\langle\langle M\rangle\rangle$,

(2) $\mathcal{A}_f$ ist endlich und beschränkt sowie

(3) es existiert ein endlicher beschränkter Automat $\mathcal{A}$ mit $f = |\mathcal{A}|$.

Beweis. Die Implikation (1) $\Longrightarrow$ (2) ergibt sich aus 3.4.6 und 4.2.2, (2) $\Longrightarrow$ (3) ist trivial und (3) $\Longrightarrow$ (1) folgt aus Gleichung 4.1. □

4.3 Cut-Point-Theorem

Im Rahmen eines Cut-Point-Theorems interessiert man sich für sogenannte *Cut-Point-Sprachen*, das sind Sprachen der Form

$$L_\lambda(f) = \{m \in M \mid |f(m)| > \lambda\},$$

wobei $\lambda \in \mathbb{R}_{\geq 0}$ der *Schnittpunkt* und $f \in K\langle\langle M\rangle\rangle$ eine formale Potenzreihe sind. Der Schnittpunkt λ von f heißt *isoliert*, wenn in einer Umgebung λ kein absoluter Wert von f liegt, d.h. es existiert ein $\varepsilon > 0$, so dass für alle $m \in M$ gilt

$$|f(m)| \notin (\lambda - \varepsilon, \lambda + \varepsilon).$$

Das Ziel dieses Abschnitts ist die Angabe einer hinreichenden Bedingung für die Regularität einer Cut-Point-Sprache. Den Großteil des zugehörigen Beweises übernimmt das folgende Lemma:

Lemma 4.3.1. *Seien $\varepsilon > 0$ und $f, g \in K^{\mathrm{brec}}\langle\langle M\rangle\rangle$ beschränkte erkennbare Potenzreihen, so dass für alle $m \in M$ mit $|f(m)| \neq |g(m)|$ gilt*

$$\big||f(m)| - |g(m)|\big| \geq \varepsilon.$$

Dann sind die Sprachen $L\big(|f| < |g|\big), L\big(|f| = |g|\big), L\big(|f| > |g|\big)$

$$\begin{aligned} L\big(|f| < |g|\big) &= \{m \in M \mid |f(m)| < |g(m)|\}, \\ L\big(|f| = |g|\big) &= \{m \in M \mid |f(m)| = |g(m)|\} \text{ und} \\ L\big(|f| > |g|\big) &= \{m \in M \mid |f(m)| > |g(m)|\} \end{aligned}$$

allesamt regulär.

Beweis. Es reicht zu zeigen, dass $L\big(|f| < |g|\big)$ regulär ist, denn dann sind $L\big(|f| > |g|\big)$ aus Symmetriegründen und $L\big(|f| = |g|\big)$ wegen

$$L\big(|f| = |g|\big) = M \setminus \big(L\big(|f| < |g|\big) \cup L\big(|f| > |g|\big)\big)$$

ebenfalls regulär. Ein bekanntes Resultat aus der Automatentheorie über beliebigen Monoiden besagt, dass $L\big(|f| < |g|\big)$ genau dann regulär ist, wenn die Menge

$$\mathfrak{L} = \big\{m^{-1}L\big(|f| < |g|\big) \mid m \in M\big\}$$

der Linksableitungen von $L\big(|f| < |g|\big)$ endlich ist. Der Rest des Beweises besteht darin, die Endlichkeit von $\mathfrak{L}$ zu zeigen.

Seien also $\mathcal{A} = (A, \mu, a_0, \varphi)$ und $\mathcal{B} = (B, \nu, b_0, \psi)$ endliche beschränkte Automaten, die f und g erkennen sowie $c(\mathcal{A})$ und $c(\mathcal{B})$ Schranken für $r_{\mathcal{A}}$ und $r_{\mathcal{B}}$. Wie man leicht nachrechnet, wird durch

$$\|a \oplus b\| = \|a\| + \|b\|$$

eine Norm auf $A \oplus B$ definiert. Weiter seien eine Abbildung $r : M \to A \oplus B$ und Linearformen $\varphi', \psi' : A \oplus B \to K$ wie folgt definiert:

$$r(m) = (a_0 \oplus b_0)(\mu(m) \oplus \nu(m)), \qquad (a \oplus b)\varphi' = a\varphi \qquad \text{und} \qquad (a \oplus b)\psi' = b\psi.$$

Nach Konstruktion gilt für alle $m \in M$

$$f(m) = r(m)\varphi' \qquad \text{und} \qquad g(m) = r(m)\psi'.$$

Außerdem wird r durch $c(\mathcal{A}) + c(\mathcal{B})$ beschränkt.

Sind $m_1, m_2 \in M$, so dass

$$m_1^{-1}L\big(|f| < |g|\big) \neq m_2^{-1}L\big(|f| < |g|\big)$$

gilt, dann existiert o.B.d.A. ein $n \in M$ mit

$$n \in m_1^{-1}L\big(|f| < |g|\big) \text{ und } n \notin m_2^{-1}L\big(|f| < |g|\big)$$

bzw.

$$m_1 n \in L\big(|f| < |g|\big) \text{ und } m_2 n \notin L\big(|f| < |g|\big).$$

Es gilt also

$$|f(m_1n)| < |g(m_1n)| \qquad \text{und} \qquad |f(m_2n)| \geq |g(m_2n)|\,.$$

Wegen der eingangs gestellten Bedingung an f und g gilt dann auch

$$\varepsilon \leq |g(m_1n)| - |f(m_1n)| \qquad \text{und trivialerweise} \qquad 0 \leq |f(m_2n)| - |g(m_2n)|\,.$$

Schließlich folgt

$$\begin{aligned}
\varepsilon &\leq |f(m_2n)| - |f(m_1n)| + |g(m_1n)| - |g(m_2n)| \\
&\leq |f(m_2n) - f(m_1n)| + |g(m_1n) - g(m_2n)| \\
&= \big|r(m_2n)\varphi' - r(m_1n)\varphi'\big| + \big|r(m_1n)\psi' - r(m_2n)\psi'\big| \\
&= \big|(r(m_2) - r(m_1))(\mu(n) \oplus \nu(n))\varphi'\big| + \big|(r(m_1) - r(m_2))(\mu(n) \oplus \nu(n))\psi'\big| \\
&\leq c(\varphi') \cdot \|(r(m_2) - r(m_1))(\mu(n) \oplus \nu(n))\| + c(\psi') \cdot \|(r(m_1) - r(m_2))(\mu(n) \oplus \nu(n))\| \\
&= (c(\varphi') + c(\psi')) \cdot \|(r(m_1) - r(m_2))(\mu(n) \oplus \nu(n))\| \\
&\leq (c(\varphi') + c(\psi')) \cdot c(\mu(n) \oplus \nu(n)) \cdot \|r(m_1) - r(m_2)\|\,,
\end{aligned}$$

wobei $c(\varphi')$, $c(\psi')$ und $c(\mu(n) \oplus \nu(n))$ die Konstanten seien, deren Existenz in Korollar 2.1.5 garantiert wird. Insgesamt gilt also

$$\|r(m_1) - r(m_2)\| \geq \frac{\varepsilon}{(c(\varphi') + c(\psi')) \cdot c(\mu(n) \oplus \nu(n))} = \delta > 0.$$

Nun sei $X \subseteq M$ eine Menge, so dass für jedes $L \in \mathfrak{L}$ genau ein $m \in X$ existiert mit $m^{-1}L\big(|f| < |g|\big) = L$. Inbesondere sind $\mathfrak{L}$ und X gleichmächtig. Für $m_1, m_2 \in X$ mit $m_1 \neq m_2$ gilt also $m_1^{-1}L\big(|f| < |g|\big) \neq m_2^{-1}L\big(|f| < |g|\big)$ und somit $\|r(m_1) - r(m_2)\| \geq \delta$, also $r(m_1) \neq r(m_2)$. Die Mengen X und $r(X)$ sind damit ebenfalls gleichmächtig.

Nach Konstruktion ist r beschränkt und somit ist auch $r(X) \subseteq r(M)$ beschränkt. Da für alle $x_1, x_2 \in r(X)$ mit $x_1 \neq x_2$ zudem $\|x_1 - x_2\| \geq \delta$ gilt, ist die Menge $r(X)$ nach Lemma 2.1.6 endlich. Damit sind auch die gleichmächtigen Mengen X und $\mathfrak{L}$ endlich. □

Der nachstehende Satz ist schließlich das angestrebte *Cut-Point-Theorem für beschränkte erkennbare Potenzreihen* und somit das Hauptresultat des Kapitels.

Satz 4.3.2. *Seien $f \in K^{\mathrm{brec}}\langle\langle M\rangle\rangle$ eine beschränkte erkennbare Potenzreihe und $\lambda \in \mathbb{R}_{\geq 0}$ ein isolierter Schnittpunkt von f. Dann ist die Cut-Point-Sprache*

$$L_\lambda(f) = \{m \in M \mid |f(m)| > \lambda\}$$

regulär.

Beweis. Laut Satz 4.1.2 ist die konstante Potenzreihe $f_\lambda(m) = \lambda$ beschränkt und erkennbar. Da λ ein isolierter Schnittpunkt ist, existiert ein $\varepsilon > 0$, so dass für alle $m \in M$ gilt

$$\big||f(m)| - |f_\lambda(m)|\big| \geq \varepsilon.$$

Nach dem vorangegangenen Lemma ist $L_\lambda(f) = L\big(|f| > |f_\lambda|\big)$ also regulär. □

5 Quantenautomaten

Das in der Einleitung begründete Interesse an Quantenautomaten hat dazu geführt, dass in der Literatur verschiedene quantenmechanisch inspirierte Autmatenmodelle vorgeschlagen und untersucht wurden. Der historisch erste Ansatz waren die (measure-once) „quantum finite-state automata“ von Moore und Crutchfield [12]. Später folgten (measure-many) „1-way and 2-way quantum finite state automata“ [11], „1-way quantum finite automata with control language“ [4] und „multi-letter quantum finite automata“ [2], um nur einige zu nennen. Gegenstand dieses Kapitels sind die erstgenannten „quantum finite-state automata“.

Zum einen werden hier die bereits von Moore und Crutchfield vorgenommenen Untersuchungen zu den Abschlusseigenschaften sowie der Beweis des Pumping-Lemmas wiedergegeben. Zum anderen werden spätere Ergebnisse vorgestellt: ein Cut-Point-Theorem für quantenerkennbare Sprachen [6] und eine Charakterisierung der von Quantenautomaten akzeptierten klassischen Sprachen [7]. Außerdem werden zwei negative Resultate bezüglich der Abgeschlossenheit quantenerkennbarer Sprachen nachgewiesen, die in der Literatur noch keine Erwähnung fanden.

Das Kapitel ist dabei folgendermaßen aufgebaut: Abschnitt 5.1 gibt eine kurze Einführung in die notwendigen physikalischen Grundlagen. Darauf aufbauend werden in Abschnitt 5.2 Quantenautomaten sowie die Klasse der quantenerkennbaren Sprachen definiert, um direkt im Anschluss (5.3) verschiedene Operationen auf Quantensprachen hinsichtlich ihrer Abschlusseigenschaften zu untersuchen. Abschnitt 5.4 dient der Formulierung und dem Beweis des Pumping-Lemmas, aus dem anschließend (5.5) zwei negative Abschlussresultate gefolgert werden. Abschnitt 5.6 hat die Übertragung des Cut-Point-Theorems auf quantenerkennbare Sprachen zum Gegenstand und abschließend wird in Abschnitt 5.7 die Charakterisierung der von Quantenautomaten akzeptierten Sprachen vorgenommen.

5.1 Quantenmechanische Grundlagen

Die folgende Einführung in die Prinzipien der Quantenmechanik verwendet einen deduktiven Ansatz und gibt die wichtigsten Axiome und Postulate dieser Disziplin wieder. Die sogenannte „Dirac-Formulierung der Quantenmechanik“ wurde im Wesentlichen [14, S. 127ff] entnommen.

Jedem quantenmechanischen System ist ein Zustandsraum H zugeordnet. Bei diesem handelt es sich um einen Hilbertraum, d.h. einen vollständigen, unitären Vektorraum. Die Elemente $\psi \in H$ dieses Raumes werden als Zustandsvektoren bezeichnet und repräsentieren die Zustände des Systems. Sie besitzen keine reale Bedeutung im Sinne

einer Messbarkeit, sondern ermöglichen lediglich die Beschreibung experimenteller Abläufe. Ein Zustandsvektor ψ und seine komplexen Vielfachen $c\psi$ sollen dabei denselben Zustand repräsentieren, es ist also zweckmäßig ausschließlich Zustandsvektoren ψ mit $\|\psi\| = 1$ zu betrachten. Im hier verwendeten Schrödinger-Bild ist der Systemzustand ψ im Allgemeinen zeitlichen Änderungen unterworfen, $\psi = \psi(t)$ also von der Zeit t abhängig.

Im Gegensatz zur klassischen Physik sind die Wechselwirkungen eines quantenmechanischen Systems mit einer eingeschalteten Messapparatur nicht vernachlässigbar, d.h. eine Messung führt in der Regel zu einer Änderung des Systemzustandes. Messbare Größen werden dabei als Observable bezeichnet und durch selbstadjungierte lineare Operatoren $A : H \to H$ beschrieben. Wird im Zustand ψ eine Messung der Observablen A vorgenommen, ist das Ergebnis einer der Eigenwerte λ von A, die allesamt reell sind. Außerdem befindet sich das System nach der Messung im Zustand ψP_λ, wobei P_λ die orthogonale Projektion auf den zu λ gehörenden Eigenraum bezeichnet. Wiederholte Messungen im selben Zustand ψ können dabei verschiedene Resultate liefern. Jeder Eigenwert λ von A wird mit der Wahrscheinlichkeit

$$P(\lambda) = \|\psi P_\lambda\|^2$$

gemessen. Besitzt A genau die Eigenwerte $\lambda_1, \ldots, \lambda_k$ und sind $P_{\lambda_1}, \ldots, P_{\lambda_k}$ die Projektionen auf die zugehörigen Eigenräume, dann gilt

$$\sum_{i=1}^{k} P(\lambda_i) = \sum_{i=1}^{k} \|xP_{\lambda_i}\|^2 = \left\| \sum_{i=1}^{k} xP_{\lambda_i} \right\|^2 = \|x\|^2 = 1.$$

Es wird also mit Sicherheit einer der Eigenwerte von A gemessen.

Zur Beschreibung der Dynamik eines quantenmechanischen Systems wählt man folgenden Ansatz: der Zusammenhang zwischen den Systemzuständen $\psi(t_0)$ und $\psi(t)$ zu den Zeitpunkten t_0 und $t > t_0$ soll sich durch eine Gleichung der Form

$$\psi(t) = \psi(t_0)U(t, t_0) \tag{5.1}$$

beschreiben lassen, wobei $U(t, t_0)$ als Zeitentwicklungsoperator bezeichnet wird. Eine offensichtliche Anforderung an den zeitabhängigen Operator U ist, dass er die Gesamtwahrscheinlichkeit des Systems erhält. Es muss also

$$\|\psi(t)\| = \|\psi(t_0)\|$$

gelten, was genau dann der Fall ist, wenn $U(t, t_0)$ unitär ist.

Über mehrere Zwischenschritte kann man aus (5.1) schließlich die *zeitabhängige Schrödinger-Gleichung*

$$\mathfrak{i}\hbar \frac{\partial \psi(t)}{\partial t} = \psi(t)H(t)$$

herleiten. Dabei ist H der sogenannte Hamilton-Operator, der die Gesamtenergie des

Systems beschreibt.

5.2 Quantenautomaten und Quantensprachen

Aufbauend auf diesen physikalischen Grundlagen wird nun folgendermaßen ein Automatenmodell definiert: Ein Quantenautomat ist ein quantenmechanisches System, das sich zu Beginn in einem präparierten Initialzustand befindet. Für jeden Buchstaben eines zu untersuchenden Wortes findet ein Zustandsübergang mithilfe eines unitären Operators statt, wobei für jedes Vorkommen des gleichen Buchstabens derselbe Operator verwendet wird. Abschließend wird eine Messung vorgenommen, die ausschließlich die Ergebnisse 0 und 1 für „abgelehnt“ und „akzeptiert“ liefern darf. Da sich selbstadjungierte Operatoren, die nur die Eigenwerte 0 und 1 besitzen, mit den orthogonalen Projektionen identifizieren lassen, kann man den Operator bereits durch die Angabe eines Unterraumes des Zustandsraumes festlegen. Dieses Modell führt zu folgender formaler Definition [12]:

Definition 5.2.1. Ein *endlicher Quantenautomat* (QFA) über einem Monoid M ist ein 4-Tupel $\mathcal{Q} = (H, \delta, s_0, H_F)$ wobei

- H ein endlich-dimensionaler, unitärer $\mathbb{C}$-Vektorraum, der *Zustandsraum*,
- $\delta : M \to U(H)$ ein Monoid-Homomorphismus, die *Transitionsabbildung*,
- $s_0 \in H$ mit $\|s_0\| = 1$ der *Initialzustand* und
- $H_F \subseteq H$ der *akzeptierende Unterraum* von H ist.

Sei $P_F : H \to H_F$ die orthogonale Projektion auf H_F. Dann ist das *Verhalten von* $\mathcal{Q}$ die wie folgt definierte Funktion $|\mathcal{Q}| : M \to [0, 1]$

$$|\mathcal{Q}|(m) = \|s_0 \delta(m) P_F\|^2 .$$

Der Wert $|\mathcal{Q}|(m)$ wird dabei als die Wahrscheinlichkeit des Ereignisses interpretiert, dass $\mathcal{Q}$ das Wort $m \in M$ akzeptiert. Es gibt also zwei mögliche Arten von Objekten, die ein Quantenautomat erkennen kann. Zum einen kann man Quantensprachen als Abbildungen $M \to [0, 1]$, die jedem Wort eine Wahrscheinlichkeit zuordnen, definieren und festlegen, dass $\mathcal{Q}$ gerade die Quantensprache $|\mathcal{Q}|$ akzeptiert. Dies ist der Ansatz, der im ersten Teil des Kapitels verfolgt wird. Zum anderen könnte man als die von $\mathcal{Q}$ akzeptierte Sprache $L \subseteq M$ auch die Menge aller Wörte betrachten, deren Akzeptanzwahrscheinlichkeit eine bestimmte Grenze überschreitet. Dieser Idee wird im letzten Abschnitt des Kapitels nachgegangen.

Als *Quantensprachen* werden also Abbildungen $f : M \to [0, 1]$ bezeichnet. Der Wert $f(m)$ soll dabei als Wahrscheinlichkeit des Ereignisses, dass das Wort m zur Quantensprache f gehört, interpretiert werden. Schließlich soll der Begriff der „Quantenerkennbarkeit“ definiert werden:

Definition 5.2.2. Eine Quantensprache $f : M \to [0,1]$ heißt *quantenerkennbar*, wenn es einen QFA $\mathcal{Q}$ über M gibt mit

$$f = |\mathcal{Q}|\,.$$

Die Menge aller quantenerkennbaren Quantensprachen $M \to [0,1]$ wird $\mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ bezeichnet,

$$\mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle = \{f : M \to [0,1] \mid f \text{ ist quantenerkennbar}\}.$$

Wenn im Folgenden von „quantenerkennbaren Sprachen“ die Rede ist, dann sind stets „quantenerkennbare Quantensprachen“ gemeint. Weiterhin stellt die Bezeichung $\mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ darauf ab, dass Quantensprachen auch als formale M-Potenzreihen über $\mathbb{C}$ aufgefasst werden können und die Klasse der quantenerkennbaren Quantensprachen somit eine Teilmenge von $\mathbb{C}\langle\langle M\rangle\rangle$ ist.

5.3 Abschlusseigenschaften

In den Kapiteln 3 und 4 wurde gezeigt, dass (beschränkte) erkennbare Potenzreihen unter verschiedenen Operationen abgeschlossen sind. Es stellt sich also die Frage, ob es auch für quantenerkennbare Sprachen möglich ist, derartige Abschlusseigenschaften nachzuweisen. Bevor diese beantwortet werden kann, müssen zunächst geeignete Operationen gefunden werden, für welche sich die Abgeschlossenheit untersuchen lässt.

Für die Suche wurden bereits zwei mögliche Ansätze angedeutet: Einerseits kann man Quantensprachen als Abbildungen auffassen, die Worten Wahrscheinlichkeiten zuordnen, und versuchen, diese Wahrscheinlichkeiten mithilfe stochastischer Operationen zu kombinieren. Andererseits kann man sie als formale Potenzreihen über $\mathbb{C}$ betrachten und die zugehörigen Operationen betrachten. In den meisten Fällen führen beide Ansätze zu denselben Definitionen, in einigen jedoch zu unterschiedlichen. Aus diesem Grund werden im Rest des Abschnitts beide Wege parallel verfolgt, geeignete Operationen definiert und die jeweilige Abgeschlossenheit gezeigt. Die vorgestellten Resultate, mit Ausnahme der Lemmata 5.3.5 und 5.3.7, stammen aus [12].

5.3.1 Konstante Quantensprachen

Analog zu Lemma 3.5.1, in dem gezeigt wurde, dass konstante formale Potenzreihen erkennbar sind, gilt folgende Aussage für konstante Quantensprachen:

Lemma 5.3.1. *Sei $c \in [0,1]$. Dann ist die Quantensprache $f_c : M \to [0,1]$ mit $f_c(m) = c$ quantenerkennbar.*

Beweis. Sei $\mathcal{Q} = (\mathbb{C}^2, \delta, s_0, H_F)$ der QFA mit

$$\delta(m) = \mathrm{Id}, \qquad s_0 = (\sqrt{c}, \sqrt{1-c}) \qquad \text{und} \qquad H_F = \langle (1,0)\rangle.$$

Die orthogonale Projektion von H auf H_F ist gerade die Projektion auf die erste Koordinate, es gilt also

$$|\mathcal{Q}|(m) = \|s_0\delta(m)P_F\|^2 = \left\|(\sqrt{c}, \sqrt{1-c})\mathrm{Id}P_F\right\|^2 = \left\|(\sqrt{c}, 0)\right\|^2 = c. \qquad \square$$

5.3.2 Komplement

In der Stochastik betrachtet man zu einem Ereignis E das komplementäre Ereignis $\overline{E}$, dass genau dann eintritt, wenn E nicht eintritt. Für die zugehörigen Wahrscheinlichkeiten gilt $P(\overline{E}) = 1 - P(E)$. Überträgt man dies auf Quantensprachen $f : M \to [0,1]$, dann wird durch

$$\overline{f}(m) = 1 - f(m)$$

eine Quantensprache $\overline{f}\ M \to [0,1]$ definiert.

Lemma 5.3.2. *Für $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ gilt $\overline{f} \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$.*

Beweis. Da f quantenerkennbar ist, existiert ein QFA $\mathcal{Q} = (H, \delta, s_0, H_F)$ mit $f = |\mathcal{Q}|$. $\mathcal{Q}' = (H, \delta, s_0, H_F^{\perp})$ sei der QFA mit dem komplementären akzeptierenden Unterraum. Für alle $m \in M$ gilt dann:

$$|\mathcal{Q}|(m) + \left|\mathcal{Q}'\right|(m) = \|s_0\delta(m)P_F\|^2 + \left\|s_0\delta(m)P_F^{\perp}\right\|^2 = \|s_0\delta(m)\|^2 = \|s_0\|^2 = 1$$

und somit

$$\left|\mathcal{Q}'\right|(m) = 1 - |\mathcal{Q}|(m) = 1 - f(m). \qquad \square$$

5.3.3 Hadamard-Produkt und Durchschnitt

Das Hadamard-Produkt $f \odot g$ zweier Quantensprachen $f, g : M \to [0,1]$ ist wie im Falle der formalen Potenzreihen durch

$$(f \odot g)(m) = f(m) \cdot g(m)$$

definiert. Diese Gleichung lässt sich außerdem stochastisch interpretieren: angenommen, die Ereignisse „m gehört zu f“ und „m gehört zu g“ sind stochastisch unabhängig und treten mit den Wahrscheinlichkeiten $f(m)$ und $g(m)$ ein, dann tritt das Ereignis „m gehört zu f und g“ mit Wahrscheinlichkeit $f(m) \cdot g(m)$ ein. Die Quantensprache $f \odot g$ lässt sich also als Durchschnitt von f und g auffassen und wird daher auch mit $f \cap g$ bezeichnet.

Lemma 5.3.3. *Für $f_1, f_2 \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ gilt $f_1 \odot f_2 \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$.*

Beweis. Da f_1 und f_2 quantenerkennbar sind, existieren QFAs $\mathcal{Q}^i = (H^i, \delta^i, s_0^i, H_F^i)$ mit $f_i = \left|\mathcal{Q}^i\right|$ für $i = 1, 2$. Weiter sei $\mathcal{Q} = (H, \delta, s_0, H_F)$ der durch

$$H = H^1 \otimes H^2, \qquad \delta(m) = \delta^1(m) \otimes \delta^2(m), \qquad s_0 = s_0^1 \otimes s_0^2 \qquad \text{und} \qquad H_F = H_F^1 \otimes H_F^2$$

definierte QFA. Dann gilt $P_F = P_F^1 \otimes P_F^2$ sowie für alle $m \in M$

$$\begin{aligned}
|\mathcal{Q}|(m) &= \|s_0\delta(m)P_F\|^2 \\
&= \left\|(s_0^1\delta^1(m)P_F^1) \otimes (s_0^2\delta^2(m)P_F^2)\right\|^2 \\
&= \langle (s_0^1\delta^1(m)P_F^1) \otimes (s_0^2\delta^2(m)P_F^2), (s_0^1\delta^1(m)P_F^1) \otimes (s_0^2\delta^2(m)P_F^2)\rangle \\
&= \langle s_0^1\delta^1(m)P_F^1, s_0^1\delta^1(m)P_F^1\rangle \cdot \langle s_0^2\delta^2(m)P_F^2, s_0^2\delta^2(m)P_F^2\rangle \\
&= \left\|s_0^1\delta^1(m)P_F^1\right\|^2 \cdot \left\|s_0^2\delta^2(m)P_F\right\|^2 \\
&= f_1(m) \cdot f_2(m).
\end{aligned}$$

□

5.3.4 Summe und Vereinigung

Will man die Summe zweier Quantensprachen $f, g : M \to [0,1]$ im Sinne formaler Potenzreihen bilden, tritt das Problem auf, dass die resultierende formale Potenzreihe im Allgemeinen keine Quantensprache ist, da es $m \in M$ mit $f(m) + g(m) > 1$ geben kann. Eine Möglichkeit, dieses Problem zu beheben, besteht darin, durch eine Wichtung der Summe sicherzustellen, dass die entstehende Potenzreihe lediglich Werte aus dem Intervall $[0,1]$ annimmt. Deshalb betrachtet man für $f, g : M \to [0,1]$ und $\alpha, \beta \in [0,1]$ mit $\alpha + \beta = 1$ die durch

$$(\alpha f + \beta g)(m) = \alpha \cdot f(m) + \beta \cdot g(m)$$

definierte Quantensprache $\alpha f + \beta g$, welche als *gewichtete Summe von f und g* bezeichnet wird.

Lemma 5.3.4. *Seien $f_1, f_2 \in \mathbb{C}^{\text{qrec}}\langle\langle M\rangle\rangle$ und $\alpha_1, \alpha_2 \in [0,1]$ mit $\alpha_1 + \alpha_2 = 1$. Dann gilt $\alpha_1 f_1 + \alpha_2 f_2 \in \mathbb{C}^{\text{qrec}}\langle\langle M\rangle\rangle$.*

Beweis. Da f_1 und f_2 quantenerkennbar sind, existieren QFAs $\mathcal{Q}^i = (H^i, \delta^i, s_0^i, H_F^i)$ mit $f_i = |\mathcal{Q}_i|$ für $i = 1, 2$. Weiter sei $Q = (H, \delta, s_0, H_F)$ der durch

$$H = H^1 \oplus H^2, \quad \delta(m) = \delta^1(m) \oplus \delta^2(m), \quad s_0 = \sqrt{\alpha_1}s_0^1 \oplus \sqrt{\alpha_2}s_0^2 \quad \text{und} \quad H_F = H_F^1 \oplus H_F^2$$

definierte QFA. Dann gilt $P_F = P_F^1 \oplus P_F^2$ sowie für alle $m \in M$

$$\begin{aligned}
|\mathcal{Q}|(m) &= \|s_0\delta(m)P_F\|^2 \\
&= \left\|\left(\sqrt{\alpha_1}s_0^1\delta^1(m)P_F^1\right) \oplus \left(\sqrt{\alpha_2}s_0^2\delta^2(m)P_F^2\right)\right\|^2 \\
&= \left\|\sqrt{\alpha_1}s_0^1\delta^1(m)P_F^1\right\|^2 + \left\|\sqrt{\alpha_2}s_0^2\delta^2(m)P_F^2\right\|^2 \\
&= \alpha_1 \cdot \left\|s_0^1\delta^1(m)P_F^1\right\|^2 + \alpha_2 \cdot \left\|s_0^2\delta^2(m)P_F^2\right\|^2 \\
&= \alpha_1 \cdot f_1(m) + \alpha_2 \cdot f_2(m).
\end{aligned}$$

□

Eine weitere Möglichkeit die „Summe“ zweier Quantensprachen zu bilden, liefert ein stochastischer Ansatz. In Anlehnung an die Siebformel kann man eine Quantensprache $f \cup g$ durch

$$(f \cup g)(m) = f(m) + g(m) - (f \cap g)(m)$$

definieren. Diese lässt sich ähnlich wie im Falle des Durchschnitts als Vereinigung der beiden Quantensprachen f und g interpretieren. Außerdem gilt mit

$$\overline{f \cup g} = \overline{f} \cap \overline{g}$$

eine Entsprechung der De Morgan'schen Regeln, die diese Interpretation zusätzlich unterstützt.

Lemma 5.3.5. *Für $f_1, f_2 \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$ gilt $f_1 \cup f_2 \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$.*

Beweis. Wie bereits angedeutet wurde, gilt

$$f_1 \cup f_2 = \overline{\overline{f_1} \cap \overline{f_2}}.$$

Nach Lemma 5.3.2 sind $\overline{f_1}$ und $\overline{f_2}$ quantenerkennbar und $\overline{f_1} \cap \overline{f_2}$ somit nach Lemma 5.3.3 ebenfalls. Schließlich folgt erneut aus Lemma 5.3.2 die Quantenerkennbarkeit von $f_1 \cup f_2$. □

5.3.5 Skalare Multiplikation

Korollar 3.5.5 besagt, dass die Multiplikation einer erkennbaren Potenzreihe mit einem Skalar die Erkennbarkeit erhält. Will man das Produkt cf einer Quantensprache $f : M \to [0, 1]$ mit einem Skalar c als

$$(cf)(m) = c \cdot f(m)$$

definieren, muss man sich aufgrund der Eigenschaften von Quantensprachen auf Skalare $c \in [0, 1]$ beschränken. Aus den Lemmata 5.3.1 und 5.3.3 folgt direkt:

Korollar 5.3.6. *Seien $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$ und $c \in [0, 1]$. Dann gilt $cf \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$.*

5.3.6 Links- und Rechtsableitungen

Die Links- und Rechtsableitung $n^{-1}f$ und fn^{-1} einer Quantensprache $f : M \to [0, 1]$ an der Stelle $n \in M$ sind wie für formale Potenzreihen durch

$$n^{-1}f(m) = f(nm) \qquad \text{und} \qquad fn^{-1}(m) = f(mn)$$

definiert.

Lemma 5.3.7. *Sei $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$ und $n \in M$. Dann gilt $n^{-1}f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$ und $fn^{-1} \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M \rangle\rangle$.*

Beweis. Da f quantenerkennbar ist, existiert ein QFA $\mathcal{Q} = (H, \delta, s_0, H_F)$ mit $f = |\mathcal{Q}|$. Dann gilt für den QFA $\mathcal{Q}'' = (H, \delta, s_0\delta(n), H_F)$ für alle $m \in M$

$$\left|\mathcal{Q}''\right|(m) = \|s_0\delta(n)\delta(m)P_F\|^2 = \|s_0\delta(nm)P_F\|^2 = f(nm).$$

Weiter sei $\mathcal{Q}' = (H, \delta', s_0\delta(n), H_F)$ der QFA mit

$$\delta'(m) = \delta(n)^{-1}\delta(m)\delta(n).$$

Dass δ' ein Monoid-Homomorphismus ist, rechnet man leicht nach. Für alle $m \in M$ gilt

$$\left|\mathcal{Q}'\right|(m) = \left\|s_0\delta(n)\delta'(m)P_F\right\|^2 = \|s_0\delta(m)\delta(n)P_F\|^2 = \|s_0\delta(mn)P_F\|^2 = f(mn). \qquad \square$$

5.3.7 Inverse Homomorphismen

Auch das inverse Bild $h^{-1}(f) : N \to [0,1]$ einer Quantensprache $f : M \to [0,1]$ unter einem Monoid-Homomorphismus $h : N \to M$ ist wie für formale Potenzreihen durch

$$h^{-1}(f)(n) = f(h(n))$$

definiert.

Lemma 5.3.8. *Seien $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ und $h : N \to M$ ein Monoid-Homomorphismus. Dann gilt $h^{-1}(f) \in \mathbb{C}^{\mathrm{qrec}}\langle\langle N\rangle\rangle$.*

Beweis. Da f quantenerkennbar ist, existiert ein QFA $\mathcal{Q} = (H, \delta, s_0, H_F)$ mit $|\mathcal{Q}| = f$. Dann gilt für den QFA $\mathcal{Q}' = (H, \delta \circ h, s_0, H_F)$ für alle $n \in N$

$$\left|\mathcal{Q}'\right|(m) = \|s_0(\delta \circ h)(m)P_F\|^2 = \|s_0\delta(h(m))P_F\|^2 = f(h(m)). \qquad \square$$

5.4 Pumping-Lemma

Um nachzuweisen, dass eine Sprache $L \subseteq \Sigma^*$ nicht regulär ist, verwendet man häufig das Pumping-Lemma für reguläre Sprachen, das eine notwendige Bedingung an die Regularität einer Sprache angibt [16, S. 31]:

Satz (Pumping-Lemma)**.** *Sei L eine reguläre Sprache. Dann gibt es eine Zahl n, so dass sich alle Wörter $x \in L$ mit $|x| \geq n$ zerlegen lassen in $x = uvw$, so dass folgende Eigenschaften erfüllt sind:*

(1) $|v| \geq 1$,

(2) $|uv| \leq n$,

(3) für alle $i = 0, 1, 2, \ldots$ gilt: $uv^iw \in L$.

Erstaunlicherweise ist es möglich, etwas Ähnliches für quantenerkennbare Sprachen zu formulieren.

Satz 5.4.1 (Pumping-Lemma für Quantensprachen)**.** *Seien $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$, $m \in M$ und $\varepsilon > 0$. Dann existiert ein $k > 0$, so dass für alle $n_1, n_2 \in M$ gilt:*

$$|f(n_1m^kn_2) - f(n_1n_2)| < \varepsilon.$$

Es kann $k \leq \left(\frac{6\pi+1}{\varepsilon}\right)^n$ gewählt werden, wenn f von einem n-dimensionalen QFA erkannt wird.

Beweis. Für $\varepsilon > 1$ ist die Behauptung offensichtlich bereits für $k = 1$ erfüllt. Sei also $\varepsilon \leq 1$. Da f quantenerkennbar ist, existiert ein QFA $\mathcal{Q} = (H, \delta, s_0, H_F)$ mit $f = |\mathcal{Q}|$. Es seien $n = \dim H$ und $\alpha = \frac{\varepsilon}{3} \in (0, 1)$.

Da die Abbildung $\delta(m)$ unitär ist, existiert laut Satz 2.2.13 eine Orthonormalbasis $x_1, \ldots, x_n$ von H, die aus lauter Eigenvektoren von $\delta(m)$ besteht. Da die zugehörigen Eigenwerte alle den Betrag 1 haben, existieren außerdem Winkel $\omega_1, \ldots, \omega_n$, so dass $e^{\omega_j \mathrm{i}}$ der Eigenwert zum Eigenvektor x_j ist. Für alle $k \in \mathbb{N}$ und $1 \leq j \leq n$ gilt dann

$$x_j \delta(m^k) = e^{k\omega_j \mathrm{i}} x_j.$$

Weiterhin seien

$$N = \left\lceil \frac{2\pi}{\alpha} \right\rceil \qquad \text{und} \qquad B_\ell = \left\{ e^{\frac{2\pi t \mathrm{i}}{N}} \mid t \in [\ell - 1, \ell) \right\}$$

für $\ell = 1, \ldots, N$. Die B_ℓ bilden eine disjunkte Zerlegung des komplexen Einheitskreises in N Bögen der Länge $\frac{2\pi}{N}$. Damit existiert für jedes $k \in \mathbb{N}$ ein n-Tupel

$$(\ell_1(k), \ldots, \ell_n(k)) \in \{1, \ldots, N\}^n$$

mit $e^{k\omega_j \mathrm{i}} \in B_{\ell_j(k)}$ für $1 \leq j \leq n$. Da es nur $K = N^n$ derartige n-Tupel gibt, existieren $1 \leq k_1 < k_2 \leq K + 1$ mit $\ell_j(k_1) = \ell_j(k_2)$ für $1 \leq j \leq n$. Mit $k = k_2 - k_1 \leq K$ gilt dann

$$e^{k\omega_j \mathrm{i}} = \frac{e^{k_2 \omega_j \mathrm{i}}}{e^{k_1 \omega_j \mathrm{i}}} \in \left\{ e^{\frac{2\pi t \mathrm{i}}{N}} \mid t \in (-1, 1) \right\},$$

und da die Sehne zwischen zwei Punkten kürzer ist als die zugehörigen Bögen, somit

$$\left| e^{k\omega_j \mathrm{i}} - 1 \right| \leq \frac{2\pi}{N} \leq \alpha.$$

Sei $A : H \to H$ die durch

$$A = \frac{1}{\alpha} \left(\delta(m^k) - \mathrm{Id} \right)$$

definierte lineare Abbildung. Eine einfache Rechnung zeigt, dass die x_j auch Eigenvektoren von A sind, mit den zugehörigen Eigenwerten

$$\lambda_j = \frac{1}{\alpha} \cdot \left(e^{k\omega_j \mathrm{i}} - 1 \right).$$

Nach Konstruktion gilt $|\lambda_j| \leq 1$ für alle $1 \leq j \leq n$.

Aufgrund der Eigenschaften eines Skalarproduktes und der von ihm induzierten Norm gilt für $x, y \in H$

$$\|x + y\|^2 - \|x\|^2 = \|y\|^2 + \langle x, y \rangle + \langle y, x \rangle.$$

Durch Anwendung der Dreiecksungleichung des komplexen Betrages sowie der Schwarz-

schen Ungleichung folgt daraus

$$\left|\|x+y\|^2 - \|x\|^2\right| \leq \|y\|^2 + |\langle x,y\rangle| + |\langle y,x\rangle| \leq \|y\|^2 + 2\cdot\|x\|\cdot\|y\|\,.$$

Seien $n_1, n_2 \in M$. Für $x = s_0\delta(n_1)\delta(n_2)P_F$ und $y = \alpha s_0\delta(n_1)A\delta(n_2)P_F$ erhält man

$$\|x+y\|^2 = \|s_0\delta(n_1)(\mathrm{Id}+\alpha A)\delta(n_2)P_F\|^2 = \left\|s_0\delta(n_1)\delta(m^k)\delta(n_2)P_F\right\|^2 = f(n_1m^kn_2)$$

sowie

$$\|x\|^2 = \|s_0\delta(n_1n_2)P_F\|^2 = f(n_1n_2) \leq 1$$

und $\|x\| \leq 1$. Zusammengenommen ergibt sich

$$\left|f(n_1m^kn_2) - f(n_1n_2)\right| \leq \|y\|^2 + 2\,\|y\|\,.$$

Könnte man zeigen, dass $\|y\| \leq \alpha$ gilt, würde der erste Teil der Behauptung folgen:

$$\left|f(n_1m^kn_2) - f(n_1n_2)\right| \leq \|y\|^2 + 2\,\|y\| \leq \alpha^2 + 2\alpha < 3\alpha = \varepsilon.$$

Weiterhin wurde k so gewählt, dass

$$k \leq K = N^n = \left\lceil\frac{2\pi}{\alpha}\right\rceil^n = \left\lceil\frac{6\pi}{\varepsilon}\right\rceil^n \leq \left(\frac{6\pi+1}{\varepsilon}\right)^n.$$

Es bleibt zu zeigen, dass $\|y\| \leq \alpha$ gilt. Da $\|s_0\| = 1$ und $\delta(n_1)$ unitär ist, gilt $\|\alpha s_0\delta(n_1)\| = \alpha$. Weil $x_1, \ldots, x_n$ eine Basis von H ist, existieren $c_1, \ldots, c_n \in \mathbb{C}$ mit

$$\alpha s_0\delta(n_1) = \sum_{j=1}^{n} c_j x_j.$$

Daraus folgt

$$\alpha s_0\delta(n_1)A = \sum_{j=1}^{n} c_j\lambda_j x_j$$

und somit

$$\|\alpha s_0\delta(n_1)A\|^2 = \sum_{j=1}^{n}|c_j\lambda_j|^2 = \sum_{j=1}^{n}|c_j|^2|\lambda_j|^2 \leq \sum_{j=1}^{n}|c_j|^2 = \|\alpha s_0\delta(n_1)\|^2 = \alpha^2$$

bzw. $\|s_0\delta(n_1)A\| \leq \alpha$. Da $\delta(n_2)$ ebenfalls unitär, mithin längenerhaltend, und P_F als Projektion längenverkürzend ist, folgt

$$\|y\| = \|\alpha s_0\delta(n_1)A\delta(n_2)P_F\| \leq \|\alpha s_0\delta(n_1)A\delta(n_2)\| = \|\alpha s_0\delta(n_1)A\| \leq \alpha. \qquad \square$$

Die nachstehende unmittelbare Schlussfolgerung aus dem Pumping-Lemma gibt ein einfa-

cheres Kriterium an, um nachzuweisen, dass eine Quantensprache nicht quantenerkennbar ist und wird für die Beweise im nächsten Abschnitt von Bedeutung sein.

Korollar 5.4.2. *Seien $f : M \to [0,1]$ eine Quantensprache und $m, n_1, n_2 \in M$, so dass die Folge $\big(f\big(n_1 m^k n_2\big)\big)_{k\in\mathbb{N}}$ monoton wachsend oder fallend aber nicht konstant ist. Dann ist f nicht quantenerkennbar.*

Beweis. Da f genau dann quantenerkennbar ist, wenn $\overline{f}$ quantenerkennbar ist, und $\overline{f}$ monoton wächst wenn f monoton fällt, sei die Folge o.B.d.A. monoton wachsend. Da die Folge nicht konstant ist, existiert ein $\ell \in \mathbb{N}$ mit $f\big(n_1 m^{\ell+1} n_2\big) > f\big(n_1 m^{\ell} n_2\big)$. Es sei $\varepsilon := f(n_1 m^{\ell+1} n_2) - f(n_1 m^{\ell} n_2) > 0$, dann gilt auf Grund der Monotonie für alle $k \geq 1$

$$f\big((n_1 m^{\ell}) m^k n_2\big) - f\big((n_1 m^{\ell}) n_2\big) \geq \varepsilon,$$

was offensichtlich im Widerspruch zum Pumping-Lemma steht. □

5.5 Negative Abschlusseigenschaften

5.5.1 Homomorphe Bilder

Satz 3.5.8 besagt, dass im Falle freier Monoide das homomorphe Bild einer erkennbaren Potenzreihe unter einem längenerhaltenden Monoid-Homomorphismus ebenfalls erkennbar ist. Es stellt sich also die Frage, ob sich ein ähnlicher Satz für quantenerkennbare Sprachen formulieren und beweisen lässt. Bevor darauf eine Antwort gegeben werden kann, muss zunächst eine Definition für das homomorphe Bild einer Quantensprache gefunden werden. Da es wie im Falle von gewichteter Summe und Vereinigung von Quantensprachen zwei mögliche Ansätze gibt, soll zunächst derjenige untersucht werden, der sich an der entsprechenden Definition für formale Potenzreihen orientiert.

Seien also $f : M \to [0,1]$ eine Quantensprache und $h : M \to N$ ein Monoid-Homomorphismus. Eine direkte Übertragung der Definition

$$h(f)(n) = \sum_{m \in h^{-1}(n)} f(m)$$

für formale Potenzreihen ist nicht möglich, da die Summe 1 überschreiten kann. Wie bereits bei der Summe zweier Quantensprachen lässt sich dieses Problem durch eine Wichtung der Summanden beheben. Da kein Summand gegenüber einem anderen ausgezeichnet ist, sollten alle dasselbe Gewicht bekommen, was zu folgender Definition führt

$$h(f)(n) = \frac{1}{|h^{-1}(n)|} \sum_{m \in h^{-1}(n)} f(m).$$

Eine notwendige Voraussetzung dafür ist, dass jedes $n \in N$ nur endlich viele h-Urbilder, jedoch mindestens eines, besitzt.

Das nachstehende Beispiel wird jedoch zeigen, dass man Alphabete Σ und Γ, eine quantenerkennbare Sprache $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle \Sigma^* \rangle\rangle$ und einen längenerhaltenden Monoid-

Homomorphismus $h : \Sigma^* \to \Gamma^*$ so wählen kann, dass $h(f)$ nach obiger Definition nicht quantenerkennbar ist.

Beispiel 5.5.1. Es seien $\Sigma = \{0,1\}$, $\Gamma = \{a\}$ und $h : \Sigma^* \to \Gamma^*$ die eindeutige Fortsetzung von $h(0) = h(1) = a$ zu einem Monoid-Homomorphismus. Weiterhin sei $\mathcal{Q} = (\mathbb{C}^2, \delta, (1,0), H_F)$ der Quantenautomat mit $H_F = \langle (0,1) \rangle$ und

$$\delta(w) = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}^{|w|_1} \qquad \text{mit } \alpha = \frac{\pi}{4},$$

wobei $|w|_1$ die Anzahl der Vorkommen des Symbols 1 in w bezeichne. Schließlich sei $f = |\mathcal{Q}|$ das Verhalten von $\mathcal{Q}$. Da P_F die Projektion auf die zweite Komponente ist, gilt mit $k = |w|_1$

$$f(w) = \left\| (1,0) \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}^k P_F \right\|^2 = \sin^2(k\alpha) = \frac{1}{2} \cdot \mathrm{Re}(1 - \mathfrak{i}^k).$$

Nun sei $g : \Gamma^* \to [0,1]$ die durch

$$g(a^n) = \frac{1}{2^n} \sum_{w \in \Sigma^n} f(w)$$

definierte Quantensprache, also nach obigem Definitionsversuch genau das homomorphe Bild von f unter h. Es gilt für $n \in \mathbb{N}$

$$\begin{aligned} g(a^n) &= \frac{1}{2^n} \cdot \sum_{w \in \Sigma^n} f(w) \\ &= \frac{1}{2^n} \cdot \sum_{k=0}^{n} \left[\binom{n}{k} \cdot \frac{1}{2} \cdot \mathrm{Re}(1 - \mathfrak{i}^k) \right] \\ &= \frac{1}{2^{n+1}} \cdot \mathrm{Re} \left[\sum_{k=0}^{n} \binom{n}{k} - \sum_{k=0}^{n} \binom{n}{k} \cdot \mathfrak{i}^k \right] \\ &= \frac{1}{2} \cdot \left[1 - \frac{1}{\sqrt{2}^n} \cdot \mathrm{Re} \left(\left(\frac{1+i}{\sqrt{2}} \right)^n \right) \right] \\ &= \frac{1}{2} \cdot \left(1 - \frac{\cos\frac{n\pi}{4}}{\sqrt{2}^n} \right) \end{aligned}$$

Mit $w = a^8$ folgt für $k \in \mathbb{N}$

$$g\big(w^k\big) = \frac{1}{2} \cdot \left(1 - \frac{\cos(2k\pi)}{16^k} \right) = \frac{1}{2} \cdot \left(1 - \frac{1}{16^k} \right).$$

Die Folge $\big(g\big(w^k\big)\big)_{k \in \mathbb{N}}$ ist also streng monoton wachsend und g nach Korollar 5.4.2 somit nicht quantenerkennbar.

Damit ist gezeigt, dass der erste Ansatz zur Definition des homomorphen Bildes einer Quantensprache die Quantenerkennbarkeit nicht erhält.

Der zweite Definitionsversuch ist stochastischer Natur. Ist $L \subseteq M$ eine Sprache und $h : M \to N$ ein Monoid-Homomorphismus, dann gilt $n \in h(L)$ genau dann, wenn es ein $m \in h^{-1}(n)$ mit $m \in L$ gibt. Eine Übertragung auf den Fall einer Quantensprache $f : M \to [0, 1]$ liefert, dass das Ereignis „n gehört zu $h(f)$“ genau dann eintreten soll, wenn es ein $m \in h^{-1}(n)$ gibt, für dass das Ereignis „m gehört zu f“ eintritt. Geht man in dieser Beziehung zu den komplementären Ereignissen bzw. Quantensprachen über, erhält man – unter Annahme einer stochastischen Unabhängigkeit – folgenden Zusammenhang:

$$\overline{h(f)}(n) = \prod_{m \in h^{-1}(n)} \overline{f}(m).$$

Als Definition von $h(f) : N \to [0, 1]$ würde sich daraus ableiten:

$$h(f)(n) = 1 - \prod_{m \in h^{-1}(n)} (1 - f(m)).$$

Das folgende Beispiel zeigt, dass auch diese Definition die Quantenerkennbarkeit nicht erhält.

Beispiel 5.5.2. Seien Σ, Γ und h wie im vorangegangenen Beispiel gewählt. Weiter seien $f : \Sigma^* \to [0, 1]$ die quantenerkennbare Sprache mit $f(w) = \frac{1}{2}$ für alle $w \in \Sigma^*$ und $g : \Gamma^* \to [0, 1]$ die durch

$$g(a^n) = 1 - \prod_{w \in \Sigma^n} (1 - f(w))$$

definierte Quantensprache. Dann gilt für alle $n \in N$

$$g(a^n) = 1 - \left(\frac{1}{2}\right)^{2^n},$$

d.h. die Folge $\left(g\left(a^k\right)\right)_{k \in \mathbb{N}}$ ist streng monoton wachsend und g somit nicht quantenerkennbar.

Damit ist gezeigt, dass auch der zweite Ansatz zur Definition des homomorphen Bildes einer Quantensprache keine guten Abschlusseigenschaften besitzt.

5.5.2 Cauchy-Produkt

Dass erkennbare formale Potenzreihen im Falle freier Monoide unter Cauchy-Produkt abgeschlossen sind, ist die Behauptung von Satz 3.5.9. Erneut ergibt sich die Frage, ob eine ähnliche Aussage auch für die Quantenerkennbarkeit gilt. Wie im vorangegangenen Abschnitt zum Abschluss unter homomorphen Bildern gibt es auch hier wieder zwei Möglichkeiten, dass Cauchy-Produkt zweier Quantensprachen $f, g \in \Sigma^* \to [0, 1]$ zu definieren.

Der Weg über die Wichtung der Definition für formale Potenzreihen führt zu

$$(f \cdot g)(w) = \frac{1}{|w|+1} \sum_{\substack{u,v \in \Sigma^* \\ w=uv}} f(u) \cdot g(v),$$

während der stochastische Ansatz

$$(f \cdot g)(w) = 1 - \prod_{\substack{u,v \in \Sigma^* \\ w=uv}} (1 - f(u) \cdot g(v))$$

liefert.

Dass der zweite Ansatz die Quantenerkennbarkeit nicht erhält, kann man mithilfe des bereits mehrfach vorgeführten Monotonieargumentes nachweisen, wenn man die quantenerkennbaren Sprachen $f, g : \Sigma^* \to [0,1]$ mit $f(w) = g(w) = \frac{1}{2}$ für alle $w \in \Sigma^*$ bei beliebigem Alphabet Σ betrachtet. Dass auch die andere Definitionsmöglichkeit keine guten Abschlusseigenschaften besitzt, zeigt folgendes Beispiel:

Beispiel 5.5.3. Sei $\Sigma = \{a\}$ und $\mathcal{Q} = (\mathbb{C}^2, \delta, (1,0), H_F)$ der QFA mit $H_F = \langle (0,1) \rangle$ und

$$\delta(a^n) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^n$$

sowie $f = |\mathcal{Q}|$ die von $\mathcal{Q}$ akzeptierte Quantensprache. Einfache Rechnungen zeigen, dass

$$f(a^n) = n \bmod 2$$

gilt. Definiert man eine Quantensprache $g : \Sigma^* \to [0,1]$ durch

$$g(a^n) = \frac{1}{n+1} \sum_{k=0}^{n} f(a^k) \cdot f(a^{n-k}),$$

entspricht diese gerade dem Cauchy-Produkt von f und f nach dem ersten Definitionsansatz.

Somit gilt für alle $k \in \mathbb{N}$

$$g\big(a^{2k}\big) = \frac{1}{2k+1} \sum_{\ell=0}^{2k} (\ell \bmod 2) \cdot ((2k-\ell) \bmod 2) = \frac{1}{2k+1} \sum_{\ell=0}^{2k} (\ell^2 \bmod 2) = \frac{k}{2k+1}$$

Die Folge $\big(g\big((aa)^k\big)\big)_{k \in \mathbb{N}}$ ist also streng monoton wachsend und g damit nicht quantenerkennbar.

5.6 Cut-Point-Theorem

In Kapitel 4 wurde ein Cut-Point-Theorem für beschränkte erkennbare Potenzreihen nachgewiesen. Dieser Abschnitt wird zeigen, dass quantenerkennbare Sprachen auch im

Sinne der gewichteten Automaten erkennbar sind, und schließlich das Cut-Point-Theorem auf Quantensprachen übertragen. Der erste Schritt besteht im Beweis der Abgeschlossenheit erkennbarer komplexer Potenzreihen unter komplexer Konjugation.

Lemma 5.6.1. *Seien $f \in \mathbb{C}^{\mathrm{rec}}\langle\langle M\rangle\rangle$ und $\overline{f} \in \mathbb{C}\langle\langle M\rangle\rangle$ die durch*

$$\overline{f}(m) = \overline{f(m)}$$

definierte Potenzreihe. Dann gilt $\overline{f} \in \mathbb{C}^{\mathrm{rec}}\langle\langle M\rangle\rangle$.

Beweis. Da f erkennbar ist, ist A_f endlich-dimensional, es existieren also $n \in \mathbb{N}$ und $m_1, \ldots, m_n \in M$ mit

$$A_f = \langle m_1^{-1} f, \ldots, m_n^{-1} f\rangle.$$

Könnte man zeigen, dass

$$A_{\overline{f}} = \langle m_1^{-1}\overline{f}, \ldots, m_n^{-1}\overline{f}\rangle \tag{5.2}$$

gilt, dann wäre $A_{\overline{f}}$ ebenfalls endlich-dimensional und $\overline{f}$ somit erkennbar.

Wegen

$$A_{\overline{f}} = \langle m^{-1}\overline{f} \mid m \in M\rangle$$

gilt in (5.2) offensichtlich die „$\supseteq$“-Inklusion. Zum Beweis der umgekehrten Inklusion sei $g \in A_{\overline{f}}$. Dann existieren $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$ und $x_1, \ldots, x_k \in M$ mit

$$g = \sum_{i=1}^{k} \alpha_i x_i^{-1}\overline{f}.$$

Für alle $m \in M$ gilt

$$\overline{g}(m) = \sum_{i=1}^{k} \overline{\alpha_i} \cdot \overline{\overline{f}(x_i m)} = \sum_{i=1}^{k} \overline{\alpha_i} x_i^{-1} f(m),$$

also

$$\overline{g} = \sum_{i=1}^{k} \overline{\alpha_i} x_i^{-1} f$$

und somit $\overline{g} \in A_f$. Es existieren also $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ mit

$$\overline{g} = \sum_{i=1}^{n} \lambda_i m_i^{-1} f.$$

Ähnlich wie eben folgt daraus

$$g = \overline{\overline{g}} = \sum_{i=1}^{n} \overline{\lambda_i} m_i^{-1}\overline{f},$$

also $g \in \langle m_1^{-1}\overline{f}, \ldots, m_n^{-1}\overline{f}\rangle$. □

Im vorangehenden Beweis hätte man zusätzlich zeigen können, dass die $m_i^{-1}\overline{f}$ eine Basis von $A_{\overline{f}}$ bilden, wenn $m_1^{-1}f, \ldots, m_n^{-1}f$ eine Basis von A_f ist, also $\dim A_{\overline{f}} = \dim A_f$ gilt.

Proposition 5.6.2. *Es gilt*

$$\mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle \subseteq \mathbb{C}^{\mathrm{brec}}\langle\langle M\rangle\rangle.$$

Beweis. Da Quantensprachen offensichtlich beschränkt sind, reicht es, die Erkennbarkeit nachzuweisen. Dazu seien $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$, $\mathcal{Q} = (H, \delta, s_0, H_F)$ ein QFA mit $|\mathcal{Q}| = f$ und $e_1, \ldots, e_k$ eine Orthonormalbasis von H_F. Weiter seien für $1 \leq i \leq k$ Linearformen $\varphi_i : H \to \mathbb{C}, x \mapsto \langle x, e_i\rangle$, gewichtete Automaten $\mathcal{A}_i = (H, \delta, s_0, \varphi_i)$ und erkennbare Potenzreihen $f_i = |\mathcal{A}_i|$ definiert. Dann gilt für alle $m \in M$

$$f(m) = \|s_0\delta(m)P_F\|^2 = \left\|\sum_{i=1}^{k}\langle s_0\delta(m), e_i\rangle e_i\right\|^2 = \left\|\sum_{i=1}^{k}(s_0\delta(m)\varphi_i)e_i\right\|^2 = \left\|\sum_{i=1}^{k} f_i(m)\cdot e_i\right\|^2$$
$$= \langle\sum_{i=1}^{k} f_i(m)\cdot e_i, \sum_{i=1}^{k} f_i(m)\cdot e_i\rangle = \sum_{i,j=1}^{k} f_i(m)\cdot\overline{f_j(m)}\cdot\langle e_i, e_j\rangle = \sum_{i=1}^{k} f_i(m)\cdot\overline{f_i}(m)$$

und somit

$$f = \sum_{i=1}^{k} f_i \odot \overline{f_i}.$$

Nach Satz 3.5.6 und Lemma 5.6.1 ist f also erkennbar. □

Aus den Sätzen 4.3.2 und 5.6.2 folgt unmittelbar das Hauptresultat dieses Abschnittes:

Satz 5.6.3 (Cut-Point-Theorem für Quantensprachen)**.** *Seien $f \in \mathbb{C}^{\mathrm{qrec}}\langle\langle M\rangle\rangle$ eine quantenerkennbare Sprache und $\lambda \in [0, 1]$ ein isolierter Schnittpunkt von f. Dann ist die Cut-Point-Sprache*

$$L_\lambda(f) = \{m \in M \mid f(m) > \lambda\}$$

regulär.

5.7 Quantenautomaten und Sprachen

Nachdem in den vorangegangenen Abschnitten des Kapitels hauptsächlich der Zusammenhang von Quantenautomaten und Quantensprachen untersucht wurde, sollen Quantenautomaten in diesem Abschnitt klassische Sprachen, also Teilmengen eines Monoides M, akzeptieren. Da die Implementation eines Quantenautomaten für jedes Wort entweder „akzeptiert“ oder „abgelehnt“ liefert, kann man Quantenautomaten gewissermaßen als randomisierte Algorithmen auffassen (siehe z.B. [13]). Es bietet sich also an, die Akzeptanzbedingung so zu wählen, dass man Methoden aus diesem Bereich der Algorithmentheorie verwenden kann. Da sich insbesondere die Begrenzung der Fehlerwahrscheinlichkeit als hilfreich erweist, wird die Akzeptanz eines Quantenautomaten wie folgt definiert:

Definition 5.7.1. Seien $\mathcal{Q}$ ein Quantenautomat über M, $L \subseteq M$ eine Sprache und $\lambda \in (0,1)$ ein Schnittpunkt. *$\mathcal{Q}$ akzeptiert L mit Schnittpunkt λ und begrenztem Fehler*, wenn es ein $\varepsilon > 0$ gibt, so dass für alle $m \in M$ gilt:

$$m \in L \Longrightarrow |\mathcal{Q}|(m) > \lambda + \varepsilon \qquad \text{und} \qquad m \notin L \Longrightarrow |\mathcal{Q}|(m) < \lambda - \varepsilon.$$

Damit diese Definition mit den Methoden für randomisierte Algorithmen verträglich ist, muss $\lambda = \frac{1}{2}$ gelten. Dass diese Bedingung die Klasse der akzeptierten Sprachen nicht einschränkt, zeigt folgendes Lemma:

Lemma 5.7.2. *Sei $\mathcal{Q}$ ein QFA der $L \subseteq M$ mit Schnittpunkt $\lambda \in (0,1)$ und begrenztem Fehler akzeptiert. Dann kann man aus $\mathcal{Q}$ effektiv einen QFA $\mathcal{Q}'$ konstruieren, der L mit Schnittpunkt $\frac{1}{2}$ und begrenztem Fehler akzeptiert.*

Beweis. Gilt $\lambda = \frac{1}{2}$, dann ist nichts zu zeigen. Im Falle $\lambda > \frac{1}{2}$ zeigen einfache Rechnungen, dass der in Korollar 5.3.6 konstruierte QFA $\mathcal{Q}'$ mit $|\mathcal{Q}'| = \frac{1}{2\lambda}|\mathcal{Q}|$ die Sprache L mit Schnittpunkt $\frac{1}{2}$ akzeptiert. Im Falle $\lambda < \frac{1}{2}$ eignet sich der in Lemma 5.3.2 und Korollar 5.3.6 konstruierte Quantenautomat für $\frac{1}{2(1-\lambda)}|\overline{\overline{\mathcal{Q}}}|$ als $\mathcal{Q}'$. □

Der Rest dieses Abschnittes hat die Charakterisierung der von Quantenautomaten mit begrenztem Fehler akzeptierten Sprachen zum Ziel. Dafür spielen Gruppenautomaten eine entscheidende Rollen, die man in Anlehnung an [7] folgendermaßen definieren kann:

Definition 5.7.3. Ein endlicher M-Automat $\mathcal{A} = (Q, \delta, q_0, F)$ heißt *Gruppenautomat*, wenn die Abbildung $\delta(m)$ für jedes $m \in M$ eine Bijektion ist. Eine reguläre Sprache $L \subseteq M$ heißt *Gruppensprache*, wenn es einen Gruppenautomaten gibt, der L akzeptiert.

Der nächste Satz liefert schließlich die gewünschte Charakterisierung:

Satz 5.7.4. *Eine Sprache $L \subseteq M$ wird genau dann von einem Quantenautomaten mit begrenztem Fehler akzeptiert, wenn es einen Gruppenautomaten gibt, der L akzeptiert.*

Beweis. Zunächst sei $\mathcal{B} = (Q, \delta, q_0, F)$ ein Gruppenautomat, der L akzeptiert. O.B.d.A. gelte $Q = \{1, \ldots, n\}$ und $\mathcal{A} = (A, \mu, a_0, \varphi)$ sei der in Beispiel 3.3.3 aus $\mathcal{B}$ konstruierte gewichtete M-Automat über $\mathbb{C}$ mit $|\mathcal{A}| = \chi_L$. Aus $\mathcal{A}$ wird nun ein Quantenautomat $\mathcal{Q}$ mit $|\mathcal{Q}| = \chi_L$ konstruiert, der L mit – nicht vorhandenem und damit – begrenztem Fehler akzeptiert.

Der Vektorraum $A = \mathbb{C}^n$ wird durch das Standardskalarprodukt ein unitärer Vektorraum. Für jedes $m \in M$ ist $\delta(m)$ eine Bijektion und $\mu(m)$ somit eine Permutation auf der kanonischen Orthonormalbasis $e_1, \ldots, e_n$ von A, d.h. $\mu(m)$ ist unitär. Außerdem gilt $\|a_0\| = \|e_{q_0}\| = 1$. Weiter seien A_F der von den e_i mit $i \in F$ erzeugte Unterraum von A,

$$A_F = \langle e_i \mid i \in F \rangle,$$

und $P_F : A \to A_F$ die orthogonale Projektion auf A_F. Offensichtlich gilt für $i \in Q$:

$$e_i P_F = \begin{cases} e_i & \text{falls } i \in F \\ 0 & \text{sonst} \end{cases}.$$

Schließlich zeigen einfache Rechnungen, dass für den QFA $\mathcal{Q} = (A, \mu, a_0, A_F)$ gilt:

$$|\mathcal{Q}| = \chi_L.$$

Der Beweis der umgekehrten Richtung folgt im Wesentlichen aus dem Pumping-Lemma und dem Cut-Point-Theorem. Dazu sei $\mathcal{Q}$ ein QFA der L mit Schnittpunkt λ und begrenztem Fehler akzeptiert sowie $\varepsilon > 0$ die Konstante aus der Definition der Akzeptanz. Dann gilt einerseits $L = L_\lambda(|\mathcal{Q}|)$ und andererseits ist λ ein isolierter Schnittpunkt von $|\mathcal{Q}|$. Die Sprache L ist also regulär und es reicht zu zeigen, dass der Minimalautomat $\mathcal{A}_L$ von L ein Gruppenautomat ist.

Es gilt also nachzuweisen, dass $\delta_L(m)$ für $m \in M$ eine Bijektion ist. Dazu sei $k > 0$ die Zahl aus dem Pumping-Lemma, so dass für alle $n_1, n_2 \in N$ gilt:

$$\left| |\mathcal{Q}|\,(n_1 m^k n_2) - |\mathcal{Q}|\,(n_1 n_2) \right| < \varepsilon. \tag{5.3}$$

Dann gilt für alle $n \in M$

$$x \in n^{-1}L \iff |\mathcal{Q}|\,(nx) > \lambda + \varepsilon \overset{(*)}{\iff} |\mathcal{Q}|\,(nm^k x) > \lambda + \varepsilon \iff x \in \left(nm^k\right)^{-1} L,$$

wobei die mit $(*)$ gekennzeichnete Äquivalenz Ungleichung (5.3) und die Tatsache, dass sich im Intervall $(\lambda - \varepsilon, \lambda + \varepsilon)$ kein Funktionswert von $|\mathcal{Q}|$ befindet, ausnutzt. Es besteht also die Gleichung

$$n^{-1}L = \left(nm^k\right)^{-1} L = \delta_L\big(m^k\big)\big(n^{-1}L\big),$$

d.h. $\mathrm{Id} = \delta_L\big(m^k\big)$. Da δ_L ein Monoid-Homomorphismus ist, folgt $\mathrm{Id} = \delta_L(m)^k$ und somit die Bijektivität von $\delta_L(m)$. □

Die hier untersuchten Quantenautomaten und Gruppenautomaten besitzen also dieselbe Mächtigkeit. Da erstere nur unsichere Aussagen treffen und zudem auf nicht-klassischer Physik beruhen, scheint es, als besäßen sie ausschließlich entscheidende Nachteile gegenüber letzteren. Dass dies nicht der Fall ist, wurde in [1] nachgewiesen: für beliebig große n existieren Gruppensprachen, die von einem Quantenautomaten der Dimension n erkannt werden, deren Minimalautomat jedoch $2^{O(n)}$ Zustände besitzt.

6 Zusammenfassung und Ausblick

Die ersten beiden Kapitel der Arbeit dienten ausschließlich der Bereitstellung der mathematischen und automatentheoretischen Grundlagen für die nachfolgenden Untersuchungen. Diese hatten zwei Hauptgegenstände: beschränkte erkennbare Potenzreihen und Quantenautomaten.

Von Ersteren konnte gezeigt werden, dass sie genau die Klasse der Potenzreihen bilden, die von beschränkten Automaten erkannt werden. Dies ermöglichte einerseits einfacherere Beweise der Abschlusseigenschaften als in [6]. Andererseits konnte das aus der selben Arbeit stammende Cut-Point-Theorem zu einem Cut-Point-Theorem für beschränkte erkennbare Potenzreihen verallgemeinert werden.

Das Kapitel über Quantenautomaten widmete sich zum einen der Vorstellung bereits bekannter Ergebnisse. Dazu zählen der Großteil der Abschlusseigenschaften, das Pumping-Lemma, das Cut-Point-Theorem und die Charakterisierung der von Quantenautomaten akzeptierten Sprachen. Zum anderen wurden dem weitere positive Abschlussresultate hinzugefügt sowie Untersuchungen hinsichtlich der Abgeschlossenheit unter Cauchy-Produkt und homomorphen Bildern vorgenommen. Diese war jedoch nachgewiesenermaßen für keine der vorgeschlagenen Definitionen gegeben.

Dies ist bedauerlich, da es sonst eventuell möglich wäre, mithilfe der Techniken aus [8] eine MSO-Logik für Quantensprachen zu definieren und ein Analogon zum Satz von Büchi (siehe z.B. [18]) zu beweisen. Ein möglicher Anknüpfungspunkt an diese Arbeit besteht also in der Suche einer geeigneteren Definition für das homomorphe Bild sowie der anschließenden Betrachtung einer Quantenlogik. Ähnlich dazu könnten passende Definitionen des Cauchy-Produktes und des – hier nicht betrachteten – Stern-Operators zu einer Entsprechung des Satzes von Schützenberger (siehe z.B. [3]) führen. Vorstellbar wären auch vergleichbare Untersuchungen an anderen Modellen für Quantenautomaten.

Weiterhin könnte es lohnenswert sein, zu untersuchen, inwiefern sich das Cut-Point-Theorem auf andere Quantenautomatenmodelle anwenden lässt. Allen diesen Modellen ist außerdem in gewisser Hinsicht eine Unitarität ihrer Transitionen gemein. Da diese der Kernaspekt beim Nachweis des Pumping-Lemmas war, ist es vorstellbar, dass sich der Beweis leicht an andere Definitionen eines Quantenautomaten anpassen lässt.

Die letzte Frage, die hier aufgeworfen werden soll, ist die nach einer weiteren Verallgemeinerung des Cut-Point-Theorems. Statt sich auf die Körper $\mathbb{R}$ und $\mathbb{C}$ zu beschränken, könnte man der Betrachtung beliebige Körper – oder darüberhinaus unitäre Ringe – mit Betrag zugrunde legen. Die Erfolgsaussichten darauf, dass dies lediglich mit unbeträchtlichen Änderungen des Beweises möglich ist, sind jedoch gering. Der Nachweis beruht explizit auf der Voraussetzung, dass alle Normen auf einem endlich-dimensionalen Vektorraum äquivalent sind, und somit implizit auf dem Satz von Heine-Borel. Letzterer gilt jedoch ausschließlich für $\mathbb{R}$-Vektorräume.

7 Literaturverzeichnis

[1] Andris Ambainis and Rusins Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 332–341, 1998.

[2] Aleksandrs Belovs, Ansis Rosmanis, and Juris Smotrovs. Multi-letter reversible and quantum finite automata. In *Proceedings of the 11th International Conference on Developments in Language Theory*, pages 60–71, 2007.

[3] Jean Berstel and Christophe Reutenauer. *Rational Series and their Languages*. Texts in Theoretical Computer Science. An EATCS Series. Springer, 1988.

[4] Alberto Bertoni, Carlo Mereghetti, and Beatrice Palano. Quantum computing: 1-way quantum automata. In *Proceedings of the 7th International Conference on Developments in Language Theory*, pages 1–20, 2003.

[5] Siegfried Bosch. *Lineare Algebra*. Springer, 4th edition, 2008.

[6] Simeon Bozapalidis. Extending stochastic and quantum functions. *Theory of Computing Systems*, 36(2):183–197, 2003.

[7] Alex Brodsky and Nicholas Pippenger. Characterizations of 1-way quantum finite automata. *SIAM Journal on Computing*, 31(5):1456–1478, 2002.

[8] Manfred Droste and Paul Gastin. Weighted automata and weighted logics. *Theoretical Computer Science*, 380(1-2):69–86, 2007.

[9] Jozef Gruska. *Quantum Computing*. Advanced Topics in Computer Science Series. McGraw-Hill, 1999.

[10] George Johnson. Efforts to transform computers reach milestone. *New York Times*, 20.12.2001.

[11] Attila Kondacs and John Watrous. On the power of quantum finite state automata. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Scient*, pages 66–75, 1997.

[12] Christopher Moore and James P. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, 2000.

[13] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.

[14] Wolfgang Nolting. *Grundkurs Theoretische Physik 5/1.* Springer, 6th edition, 2004.

[15] Azaria Paz. *Introduction to Probabilistic Automata.* Academic Press, 1971.

[16] Uwe Schöning. *Theoretische Informatik – kurz gefasst.* Spektrum Akademischer Verlag, 5 edition, 2008.

[17] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[18] Wolfgang Thomas. Languages, automata and logic. In Grzegorz Rozenberg and Arto Salomaa, editors, *Handbook of Formal Languages*, volume 3, pages 389–485. Springer, 1997.

[19] Dirk Werner. *Funktionalanalysis.* Springer, 6th edition, 2007.

Selbstständigkeitserklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe, insbesondere sind wörtliche oder sinngemäße Zitate als solche gekennzeichnet. Mir ist bekannt, dass Zuwiderhandlung auch nachträglich zur Aberkennung des Abschlusses führen kann.

Ort, Datum	Unterschrift