Verschiedene Varianten endlicher Quanten-Automaten

Stephan Sigg

17. Dezember 2004

1. Motivation
   - Interessante Arbeiten
   - Quantenautomaten
2. Problemstellung
   - Problemstellung
   - Ergebnisse

Vielversprechende Ergebnisse

Quantencomputer

- Faktorisieren großer Zahlen in Polynimialzeit (P.W. Shor).
- Suchen in ungeordneten Datenbanken (L.K. Grover).

Endliche Quantenautomaten

- Die ersten Quantencomputer werden nur über kleines Register an Qubits verfügen.
- Quantenregister hat konstante Größe.
- Wächst die Mächtigkeit von Automaten durch die Verwendung von Qubits?

Vielversprechende Ergebnisse

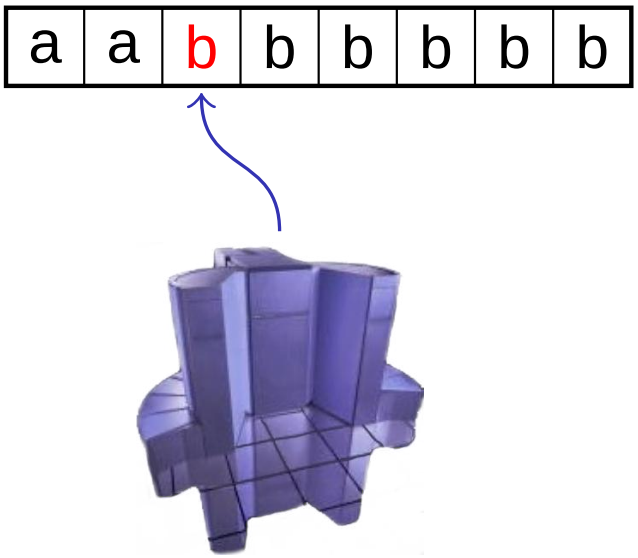
Quantencomputer

- Faktorisieren großer Zahlen in Polynimialzeit (P.W. Shor).
- Suchen in ungeordneten Datenbanken (L.K. Grover).

Endliche Quantenautomaten

- Die ersten Quantencomputer werden nur über kleines Register an Qubits verfügen.
- Quantenregister hat konstante Größe.
- Wächst die Mächtigkeit von Automaten durch die Verwendung von Qubits?

Quantenautomaten



Zustand: $q_0 = (1, 0)$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$.
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$.

Quantenautomaten

Zustandsvektoren

- Basiszustände: Einheitsvektoren $(v_1, \ldots, v_{|Q|})$.
- Überlagerung:
  - $v_i \in C$
  - $\sum_{i=1}^{n} |v_i|^2 = 1$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$

Quantenautomaten

Zustandsvektoren

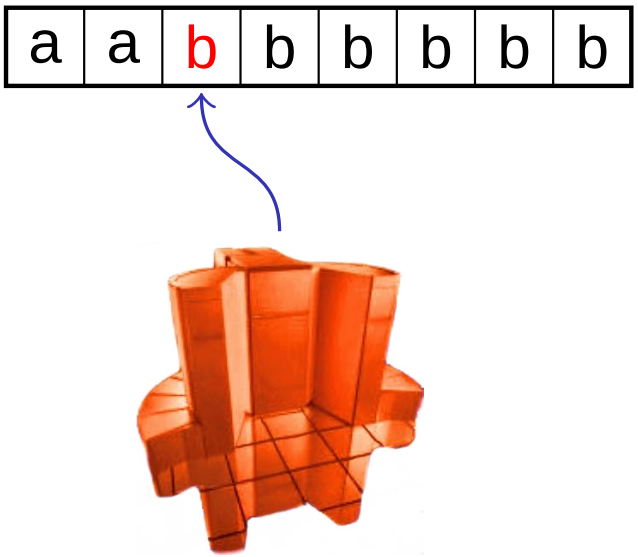
- Basiszustände: Einheitsvektoren $(v_1, \ldots, v_{|Q|})$.
- Überlagerung:
  - $v_i \in C$
  - $\sum_{i=1}^{n} |v_i|^2 = 1$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$

Quantenautomaten



Zustand: $q_0 = (1, 0)$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$

Quantenautomaten

Unitäre Matrix

Eine Matrix M ist unitär, wenn $M \times M^{-1} = I$ gilt. Es ist M^{-1} die adjungierte Matrix zu M.

$$M = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$$

$$M^{-1} = \begin{bmatrix} m_{11}^{\dagger} & m_{21}^{\dagger} \\ m_{12}^{\dagger} & m_{22}^{\dagger} \end{bmatrix}$$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$

Quantenautomaten

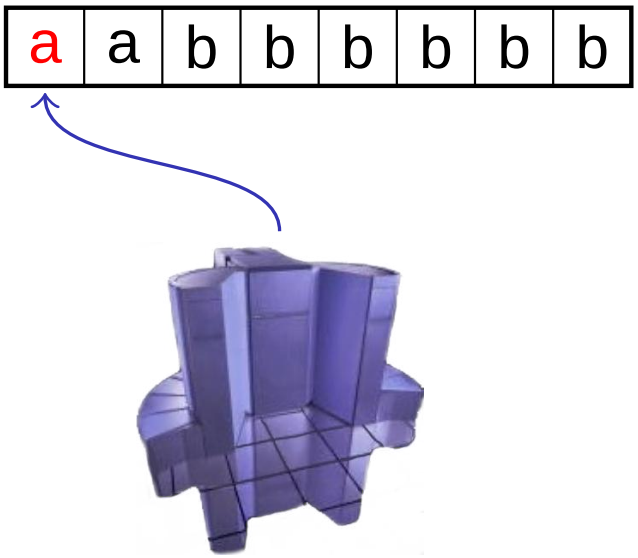
Zustandsüberführung

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

1-QFA

- Endliche Zustandsmenge: Q.
- Endliches Eingabealphabet: Σ.
- Überführungsfunktion: unitäre Matrix.
- Akzeptierende Zustände: $Q_{acc} \subseteq (Q \setminus Q_{rej})$
- Verwerfende Zustände: $Q_{rej} \subseteq (Q \setminus Q_{acc})$

Quantenautomaten

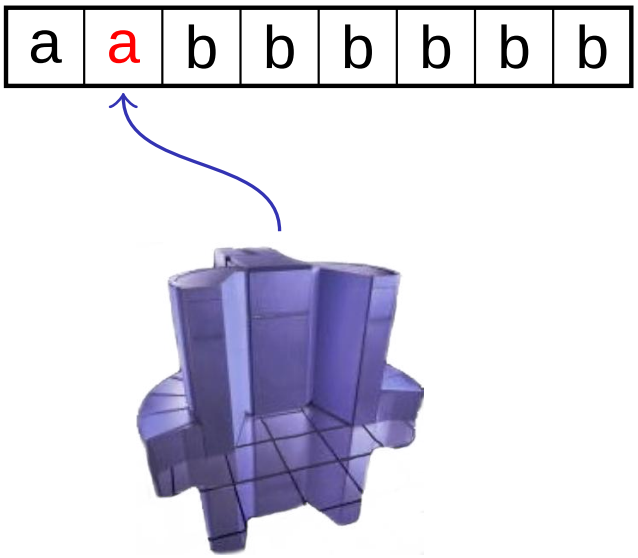


Zustand: $(1, 0)$

Erkennen der Sprache $L = \{a^*b^*\}$

- $$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
- $$M_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Quantenautomaten

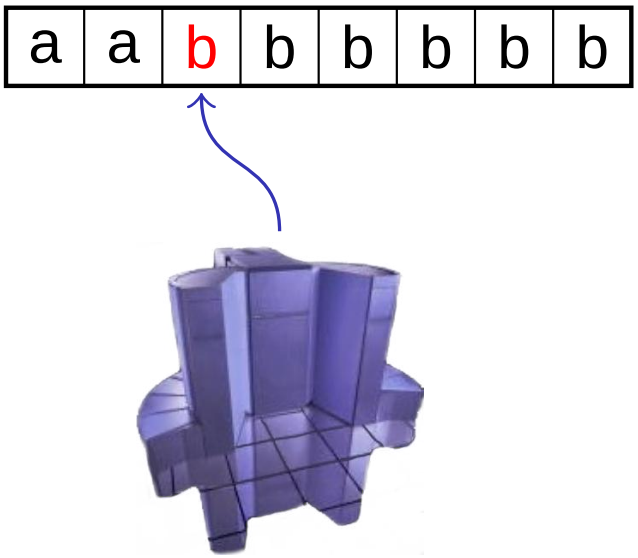


Zustand: $(1, 0)$

Erkennen der Sprache $L = \{a^* b^*\}$

- $$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
- $$M_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Quantenautomaten

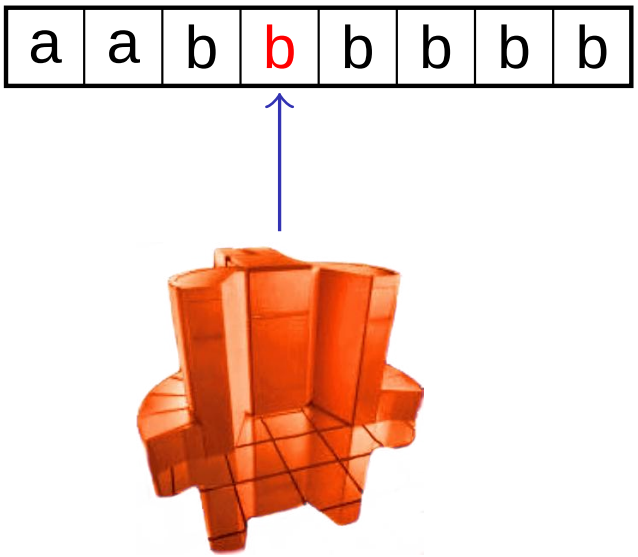


Zustand: $(1, 0)$

Erkennen der Sprache $L = \{a^* b^*\}$

- $$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
- $$M_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Quantenautomaten

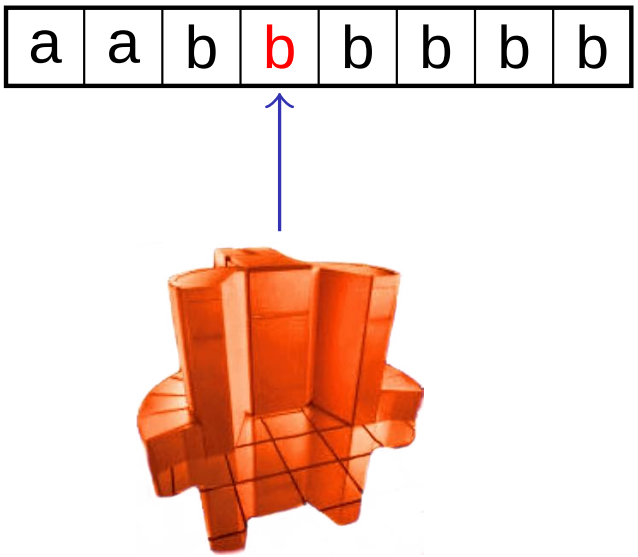


Zustand: $(0, 1)$

Erkennen der Sprache $L = \{a^* b^*\}$

- $$M_a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
- $$M_b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Quantenautomaten

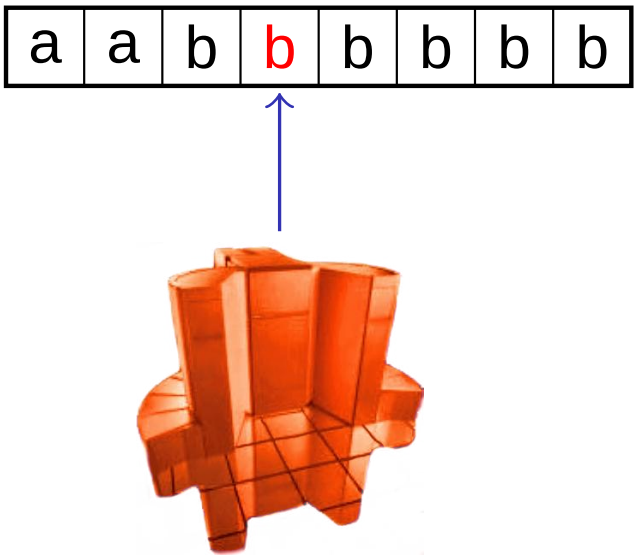


Zustand: $(0, 1)$

bekannte Quantenautomaten

- 1-QFA (A.Kondacs und J.Watrous - 1997)
  - erkennt nur eine Teilmenge der regulären sprachen.
- 2-QFA (A.Kondacs und J.Watrous - 1997)
  - erkennt alle regulären sprachen.
  - erkennt einige nicht-regulären Sprachen.
  - Quantenteil nicht konstant.

Quantenautomaten



Zustand: $(0, 1)$

bekannte Quantenautomaten

- 1-QFA (A.Kondacs und J.Watrous - 1997)
  - erkennt nur eine Teilmenge der regulären sprachen.
- 2-QFA (A.Kondacs und J.Watrous - 1997)
  - erkennt alle regulären sprachen.
  - erkennt einige nicht-regulären Sprachen.
  - Quantenteil nicht konstant.

Modifikationen

Fragestellung in der Diplomarbeit

Gibt es Quantenautomaten, die mehr als nur eine Teilmenge der regulären Sprachen erkennen und über ein konstant großes Quantenregister verfügen?

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Variationen, Ergebnisse und Ausblick

Varianten von 1-QFAs

- Zyklisches Eingabeband.
  - Erkennt nicht-reguläre Sprache.
  - Weitere Modifikationen notwendig.
- Verallgemeinerte Zustandsüberführung.
  - Kann *1-DFA* simulieren.
  - Simulation in anderer Richtung eventuell möglich.
- Preprocessing durch einen klassischen Automaten.
  - Erkennt auch nicht-reguläre Sprachen.
  - Abgrenzung zu dem *2-QFA* nicht klar.

Dankeschön!

Dankeschön!

Vielen Dank für Ihre Aufmerksamkeit.

Literatur

- A.Kondaks und J.Watrous: *On the Power of Quantum Finite State Automata.* FOCS, 66-75, 1997.
- A.Ambainis und R.Freivalds: *1-Way Quantum Finite Automata.* STOC, 368-375, 1999.
- M.Hirvensalo: *Some Open Problems Related to Quantum Computing.* EATCS, 74:154-170, 2001.
- R.Freivalds: *Probabilistic Two-Way Machines.* LNCS, 118:33-45, 1981.
- P.W.Shor: *Polynomial-Time Algorithms für Prome Factorizations and Discrete Logarithms on a Quantum computer.* SIAM, 26(5):1474-1483, 1997.
- L.K. Grover: *A Fast Quantum Mechanical Algorithm for Database Search.* STOC, 212-219, 1996.