1- und 2-Wege QFAs

Stephan Sigg

09.12.2003

1. Einleitung und Überblick
2. Quantentheoretische Grundlagen
3. DFAs und QFAs
4. Einige bekannte Ergebnisse
5. Offene Fragen
6. Schluß

Qubits

- Qubit als Analogon zum klassischen Bit
  - Basiszustände $|0\rangle$ und $|1\rangle$ als Parallele zu 0 und 1
  - $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
  - Aber auch ‘Zwischenzustände’ möglich:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

  - $|\alpha|^2 + |\beta|^2 = 1$ und $\alpha, \beta \in \mathbb{C}$
  - $|||\psi\rangle|| = 1$
- Punkt in komplexem Vektorraum mit innerem Produkt

Mehrere Qubits

Verallgemeinerung auf mehrere Qubits:

Für $\alpha_{ij} \in \mathbb{C}$:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

mit $|||\psi\rangle|| = 1$

Bemerkungen und Schwierigkeiten

- Beobachtung:

  – Die Anzahl der Basiszustände verdoppelt sich mit jedem weiteren Qubit

- Messungen:

  $\rightarrow$ Sei $|\psi\rangle = \sum_{i=0}^{n} \alpha_i |q_i\rangle$

  – Erste Messung liefert $|q_i\rangle$ mit Wahrscheinlichkeit $|\alpha_i|^2$

  Neuer Zustand ist $|q_i\rangle$

  – Jede weitere Messung liefert $|q_i\rangle$ mit Wahrscheinlichkeit 1

Bausteine in Quantenschaltkreisen

- Bedingungen an die Bausteine
  - Quadratische Matrix
  - Unitarität : $U^\dagger U = I$
  - Alle Einträge aus $\mathbb{C}$
  - Noch weitere Einschränkungen, aber hier nicht wichtig

Bausteine in Quantenschaltkreisen

- Bedingungen an die Bausteine
  - Quadratische Matrix
  - Unitarität : $U^\dagger U = I$
  - Alle Einträge aus $\mathbb{C}$
  - Noch weitere Einschränkungen, aber hier nicht wichtig
- Hadamard Gate als Beispiel für einen ein - Qubit Baustein:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Quantenbausteine

- Beispiel

$$H(\alpha|0\rangle + \beta|1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}$$

$$= \frac{(\alpha + \beta)}{\sqrt{2}}|0\rangle + \frac{(\alpha - \beta)}{\sqrt{2}}|1\rangle$$

DFAs

- $M = (Q, \Sigma, q_0, \delta, F)$
  - Endmarkierungen: $\dashv \quad ; \quad \vdash$
- Unterscheidung zwischen 1-DFAs und 2-DFAs
  - 1-DFA: Kopf darf nur in eine Richtung wandern

$$\delta_d : Q \times \Gamma \rightarrow Q$$

  - 2-DFA: $\delta_d^2 : Q \times \Gamma \rightarrow Q \times \{-1, 0, 1\}$
- Erkennen genau die regulären Sprachen

DFAs

- Zustandsüberführung in Matrizenschreibweise
  - Zustände werden durch Einheitsvektoren beschrieben
  - Quadratische Matrizen
  - Alle Matrixeinträge aus $\{0, 1\}$
  - Jede Spalte darf nur maximal eine ’1’ enthalten

Beispiel

$\delta(q_0, \sigma) = q_1$ und $\delta(q_1, \sigma) = q_1$

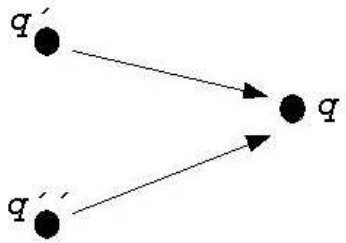
$$q_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad q_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$V_\sigma(q_0) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = q_1$$

$$V_\sigma(q_1) = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = q_1$$

RFAs

- Reversible Automaten
  - Spezieller DFA
  - Verboten:
    - $\delta_r(q', \sigma) \rightarrow q \ \wedge \ \delta_r(q'', \sigma) \rightarrow q$



RFAs

- Zustandsüberführung in Matrizenschreibweise
  - Zustände werden durch Einheitsvektoren beschrieben
  - Quadratische Matrizen
  - Alle Einträge aus $\{0, 1\}$
  - Permutationsmatrizen

Beispiel

$\delta(q_0, \sigma) = q_1$ und $\delta(q_1, \sigma) = q_0$

$$q_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad q_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$V_\sigma(q_0) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = q_1$$

$$V_\sigma(q_1) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = q_0$$

1-QFAs

– $M = \{Q, \Sigma, q_0, \delta_q, Q_{acc}, Q_{rej}\}$

– $Q_{non} = Q \setminus (Q_{acc} \cup Q_{rej})$

– Endmarkierungen: $\dashv \quad ; \quad \vdash$

– Zustände q_i beschreiben Einheitsvektoren aus $\mathbb{C}^n$

– Alle $q_i \in Q$ spannen komplexen Vektorraum auf

– Überlagerungen möglich: $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |q_i\rangle$
mit $|||\psi\rangle|| = 1$

– $|\psi\rangle$ ist Punkt im komplexen Vektorraum

Zustandsüberführung

– Überführungsfunktion $\delta_q : Q \times \Gamma \times Q \to \mathbb{C}$

– Auch als Überführungsmatrix V_σ
– $V_\sigma|\psi\rangle = \sum_{j=1}^{n} \sum_{q_i \in Q} \psi_j \delta(q_j, \sigma, q_i)|q_i\rangle$
– Unitarität: $V_\sigma^\dagger V_\sigma = I$

Beispiel

$$\delta_q(q_0, \sigma, q_0) = \alpha_1 \quad ; \quad \delta_q(q_0, \sigma, q_1) = \alpha_2$$
$$\delta_q(q_1, \sigma, q_0) = \alpha_3 \quad ; \quad \delta_q(q_1, \sigma, q_1) = \alpha_4$$

$$V_\sigma = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{bmatrix}$$

$\longrightarrow$ RFAs sind spezielle QFAs

Messungen

Für $|\psi\rangle = \sum_{i=0}^{n-1} \alpha_i |q_i\rangle$

- Zustand aus Q_{acc} wird mit Wahrscheinlichkeit $\sum_{q_i \in Q_{acc}} |\alpha_i|^2$ gemessen
  - Der Automat stoppt und akzeptiert
- Analog für Q_{rej}
- Zustand aus Q_{non} wird mit Wahrscheinlichkeit $\sum_{q_i \in Q_{non}} |\alpha_i|^2$ gemessen
  - Der Automat fällt in die Überlagerung $|\psi_{neu}\rangle = \sum_{q_i \in Q_{non}} \alpha_i |\psi_i\rangle$
  - $|\psi_{neu}\rangle$ muss noch normiert werden:

$$\sum_{q_i \in Q_{non}} \frac{1}{|||\psi_{neu}\rangle||} |\psi_i\rangle$$

Ablauf eines Rechenschrittes

– Ausgangspunkt: $|\psi_1\rangle = \sum_{i=0}^{n-1} \alpha_i |q_i\rangle$

– Lesen der Bandinschrift σ an Kopfposition

– Anwenden der zugehörigen Überführungsfunktionen $\delta_q(q_i, \sigma)$

– Resultierende Überlagerung:

$$|\psi_2\rangle = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \alpha_i \delta(q_i, \sigma, q_j) |q_j\rangle = \sum_{i=1}^{n-1} \beta_i |q_i\rangle$$

– Messen der Überlagerung $|\psi_2\rangle$

– Normieren

– Kopfbewegung

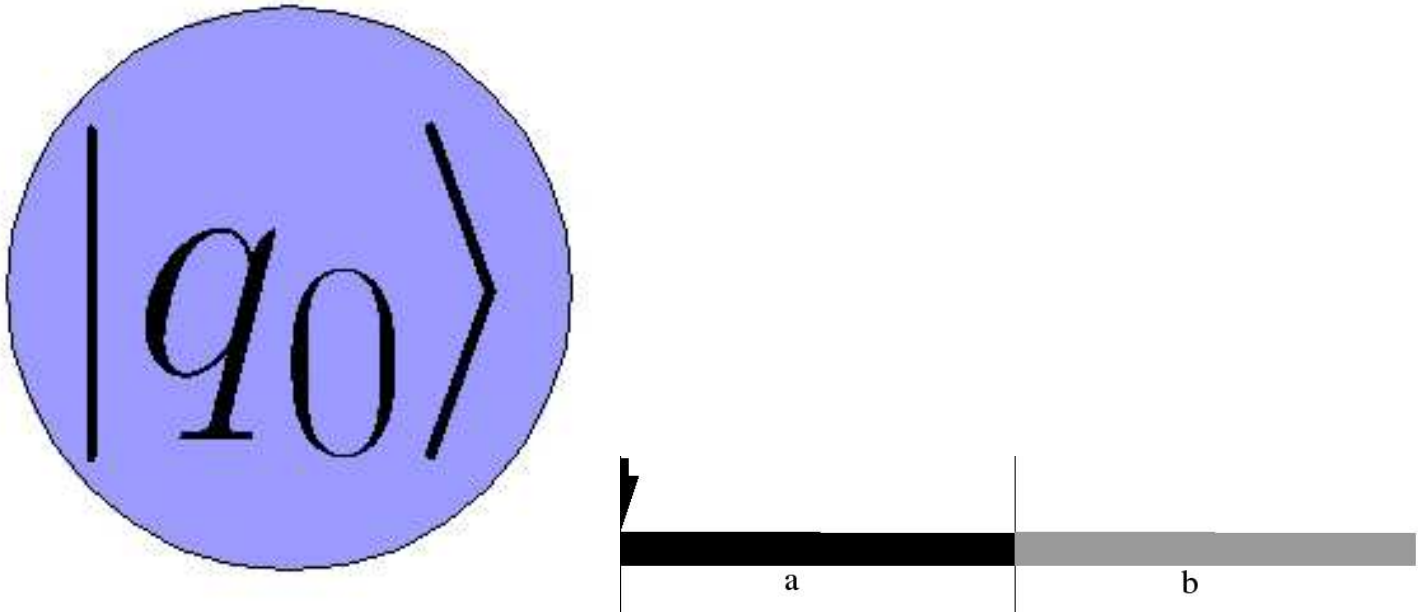
Beispiel für einen 1-QFA, der $L_{ab} = \{a^*b^*\}$erkennt

- Problem:
  - Überführungsmatrizen müssen unitär sein
  - DFA kann deswegen nicht einfach übertragen werden
- Lösung hier:
  - Zulassen eines Fehlers $1 - p$ mit

$$p^3 = 1 - p \Rightarrow p \approx 0.68\ldots$$

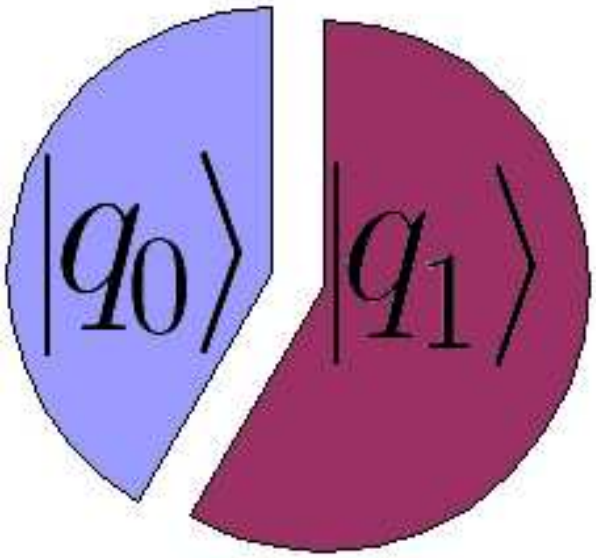
Eingabe: $w \in L_{ab} = \{a^* b^*\}$

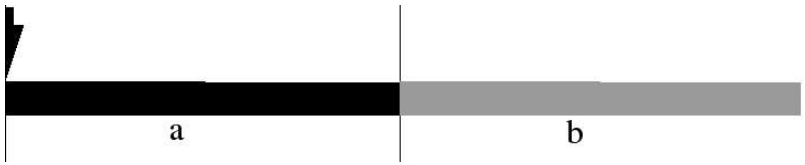
Startzustand: $|q_0\rangle$



Gelesenes Zeichen: $\dashv$

resultierende Überlagerung: $\sqrt{1-p}|q_0\rangle + \sqrt{p}|q_1\rangle$

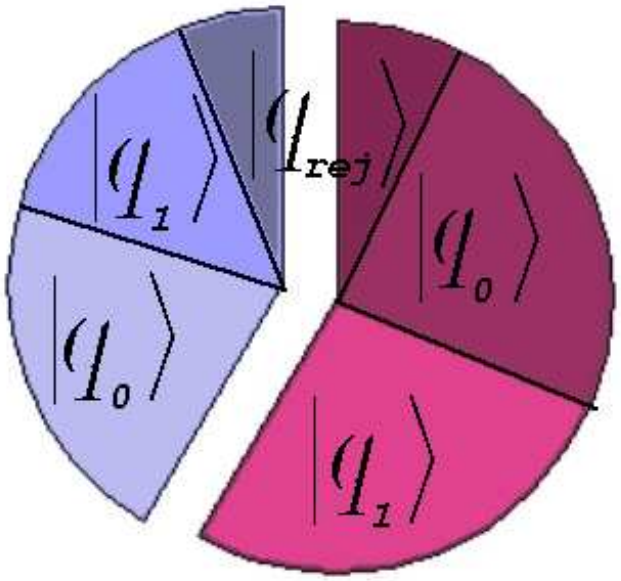


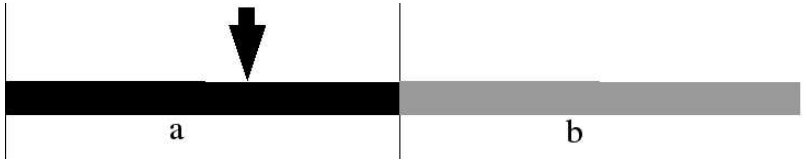


Gelesenes Zeichen: a

resultierende Überlagerung:

$$\sqrt{1-p}((1-p)|q_0\rangle + \sqrt{p(1-p)}|q_1\rangle + \sqrt{p}|q_{rej}\rangle)$$
$$+\sqrt{p}(\sqrt{p(1-p)}|q_0\rangle + p|q_1\rangle - \sqrt{1-p}|q_{rej}\rangle)$$
$$= \sqrt{1-p}|q_0\rangle + \sqrt{p}|q_1\rangle$$

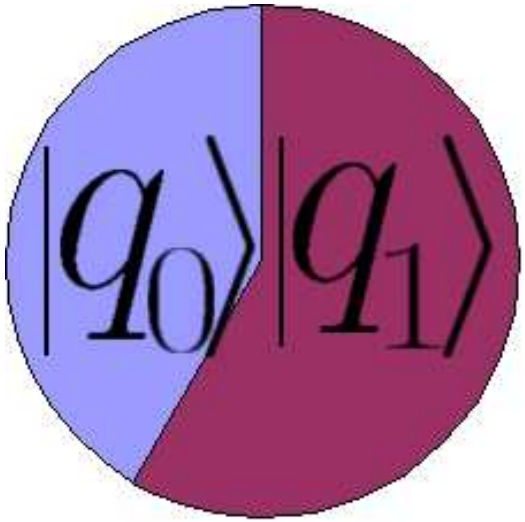


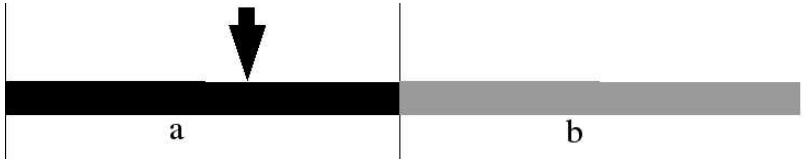


Die Amplituden vor $|q_{rej}\rangle$ heben sich gegenseitig auf !

Überlagerung nach dem Normieren:

$$\sqrt{1-p}|q_0\rangle + \sqrt{p}|q_1\rangle$$



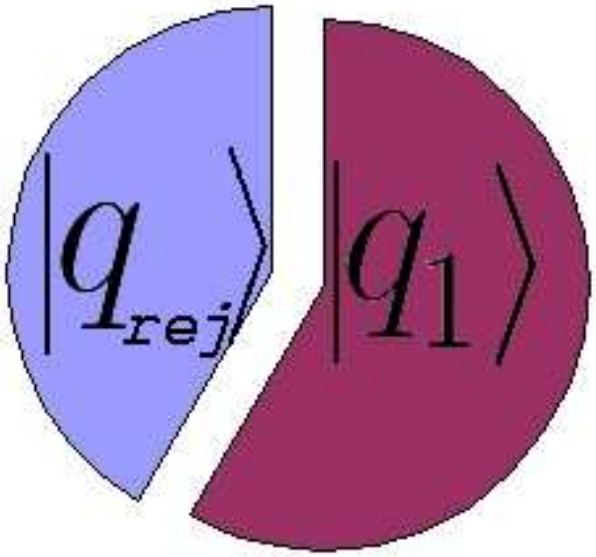


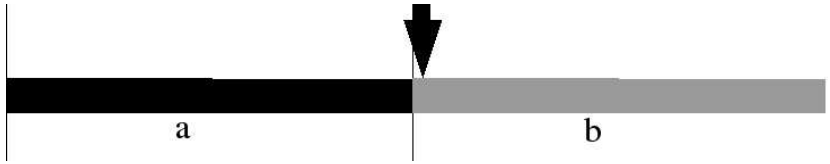
Der QFA bleibt in dieser Überlagerung, solange a gelesen wird

Gelesenes Zeichen: b

Resultierende Überlagerung:

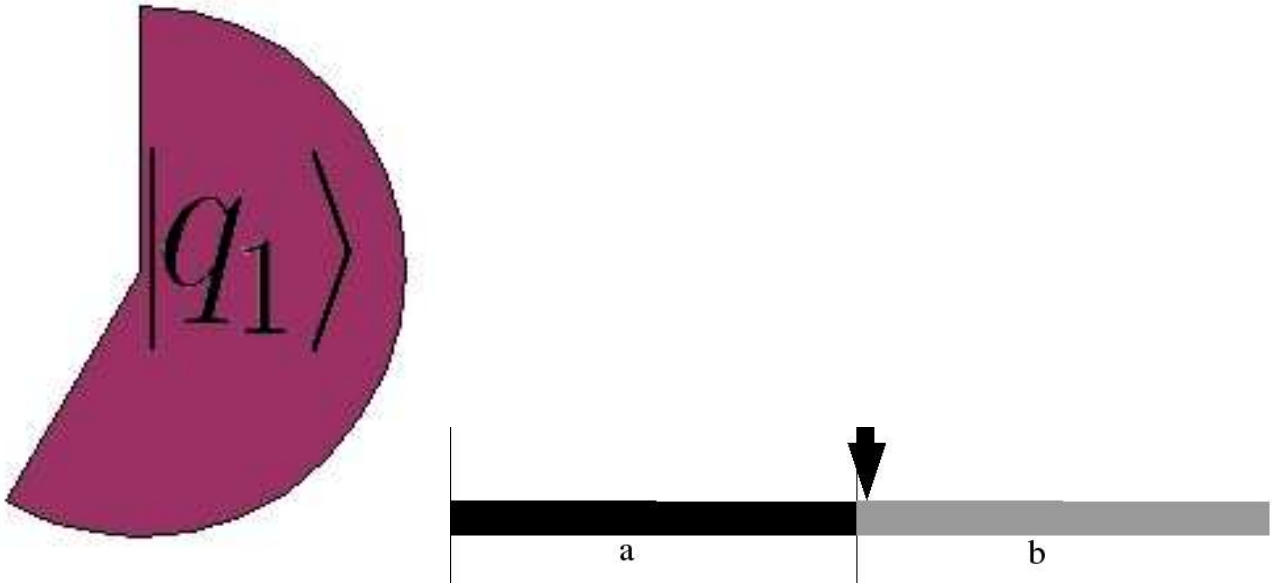
$\sqrt{1-p}|q_{rej}\rangle + \sqrt{p}|q_1\rangle$





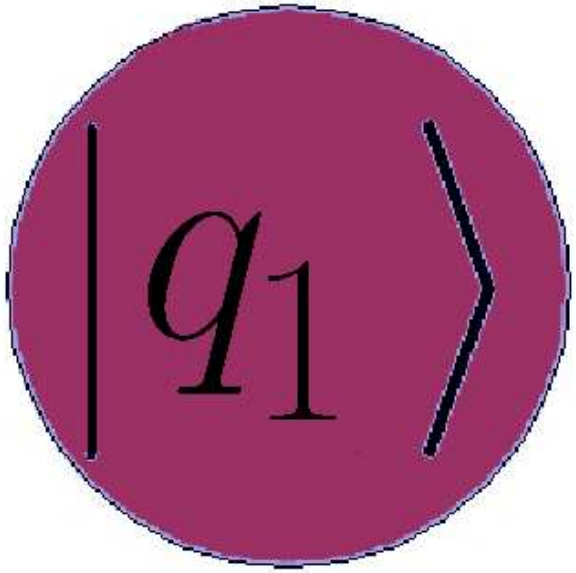
Zustände $q_i \in Q_{non}$:

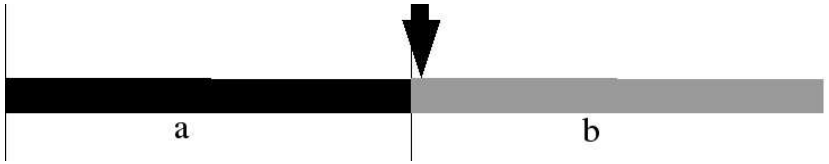
$\sqrt{p}$



Nach dem Normieren:

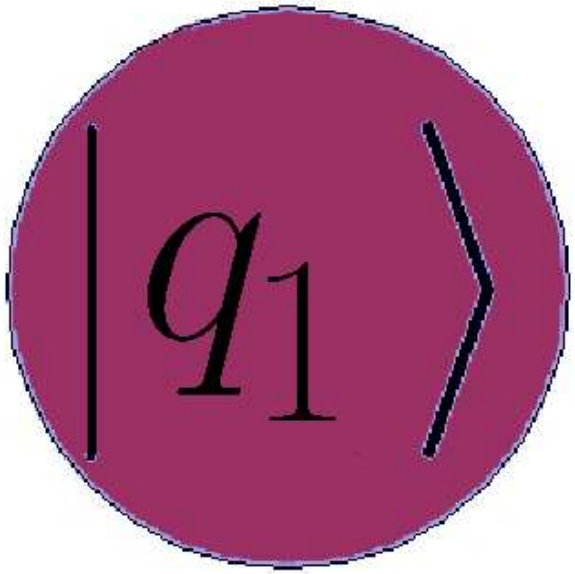
$|q_1\rangle$

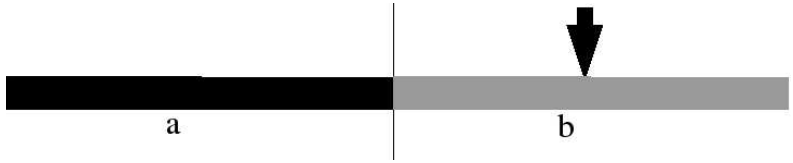




Gelesenes Zeichen: b

Der Zustand bleibt unverändert

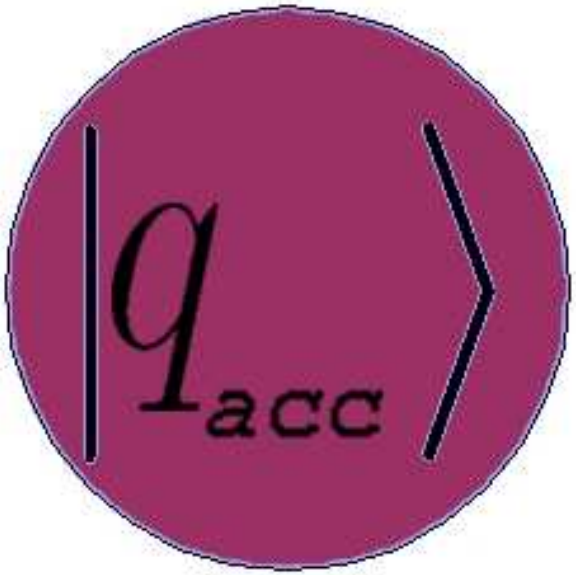


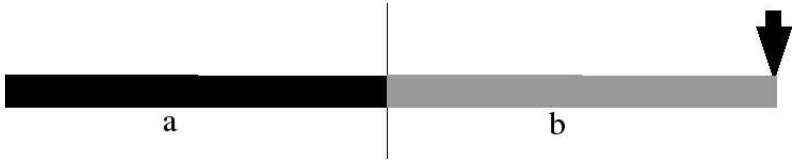


Gelesenes Zeichen: $\vdash$

Resultierende Überlagerung:

$|q_{acc}\rangle$





Insgesamt

- $w \in L_{ab} = \{a^*b^*\}$
  - QFA verwirft mit Wahrscheinlichkeit $1 - p < \frac{1}{2}$
  - QFA akzeptiert mit Wahrscheinlichkeit $1 - (1 - p) = p$
- $w \notin L_{ab} = \{a^*b^*\}$
  - QFA verwirft mit Wahrscheinlichkeit p

2-QFAs

– Kopf darf sich nach links, rechts oder gar nicht bewegen

– Überführungsfunktion $\delta_q : Q \times \Gamma \times Q \times \{-1, 0, 1\} \rightarrow \mathbb{C}$

– Überführungsmatrix V_σ ist unitär

– Die Kopfbewegung wird durch den erreichten Zustand bestimmt :

$$D(q_i) = d \quad ; \quad d \in \{-1, 0, 1\}$$

Bekannte Ergebnisse

- Ein 1-QFA kann von einem 2-RFA simuliert werden

  Kondacs, Watrous (1997)

- 1-QFAs können $L_{*a} = \{a, b\}^* a$ nicht erkennen

  Kondacs, Watrous (1997)

- 1-QFAs mit größerer Fehlerwahrscheinlichkeit können mehr Sprachen erkennen

  Ambainis, Freivalds (1998);

  Ambainis, Bonner, Freivalds, Golovkins, Karpinski (1999)

2-QFAs sind mächtiger als 2-DFAs

- 2-QFAs können alle regulären Sprachen erkennen
  - – Ein 1-DFA kann von einem 2-RFA simuliert werden - *Kondacs, Watrous (1997)*
  - – Ein 2-RFA ist ein spezieller 2-QFA
- Ein 2-QFA kann die nicht-reguläre Sprache $L_{eq} = \{a^k b^k | k \in \mathbb{N}\}$ erkennen

  Kondacs, Watrous (1997)
- Es gibt einen 2-QFA, der die nicht-kontextfreie Sprache $L_{3eq} = \{a^m b^m c^m | m \in \mathbb{N}\}$ erkennt

  Kondacs, Watrous (1997)

2-QFA, der $L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$ erkennt

M_N erkennt $L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$ mit einseitigem Fehler ϵ

– N ist frei wählbar und bestimmt den Fehler ϵ

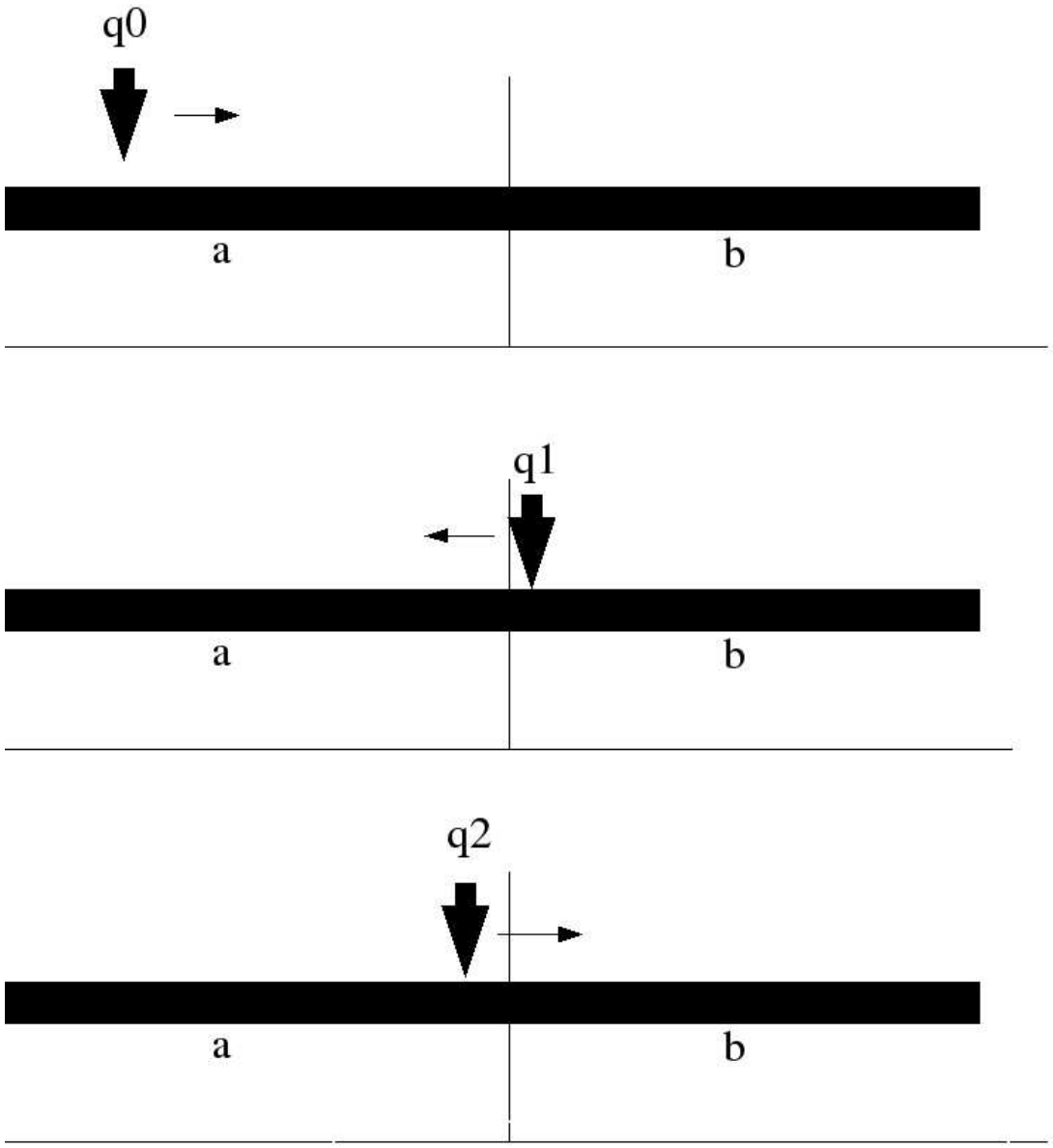
– für $w \in L_{eq}$ akzeptiert M_N mit Wahrscheinlichkeit 1

– ansonsten verwirft M_N mit Wahrscheinlichkeit mindestens $1 - \frac{1}{N}$

Beweis

Phase 1: Jede Eingabe w mit $w \notin \{a^u b^v | u, v \in \mathbb{N}\}$ wird von M_N verworfen

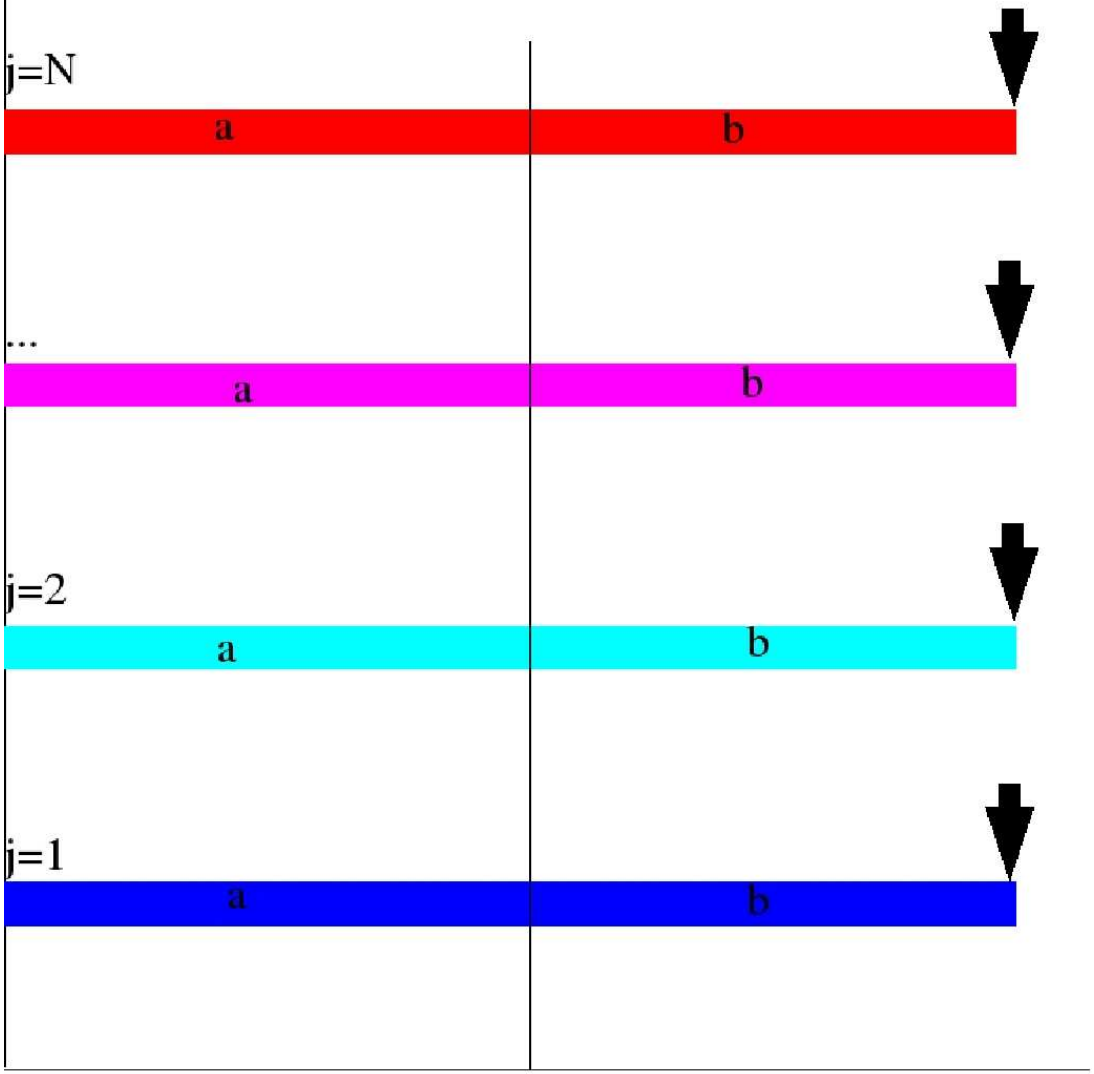
Phase 2: Eingaben w mit $w \in \{a^u b^v | u \neq v\}$ werden mit Wahrscheinlichkeit $1 - \frac{1}{N}$ verworfen

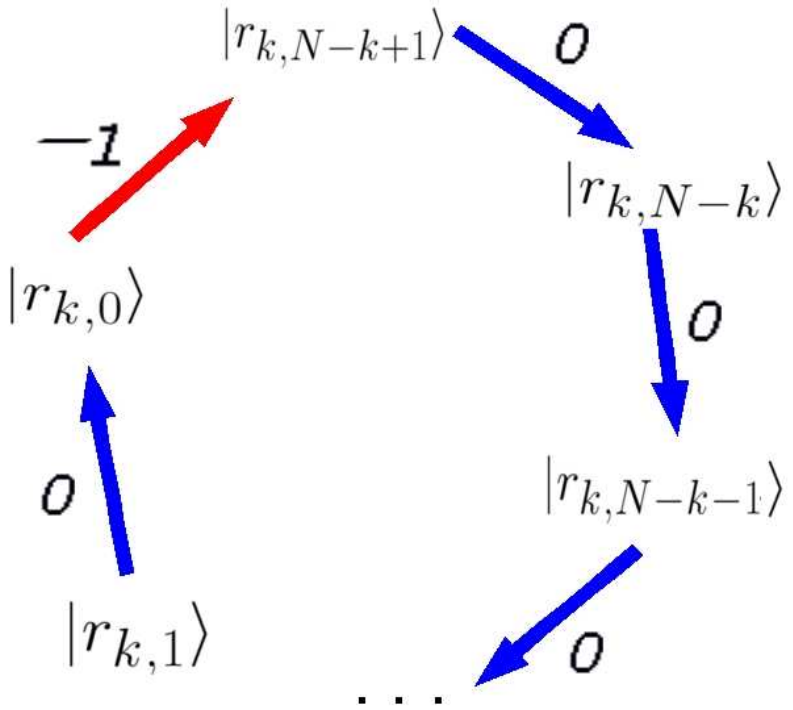


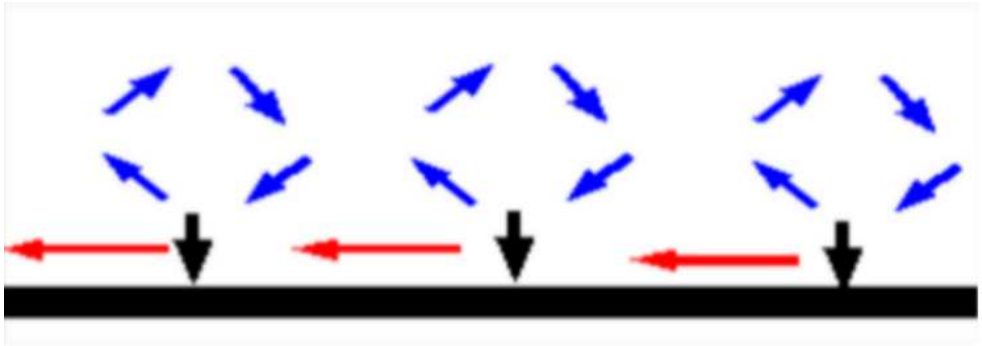
Teste,

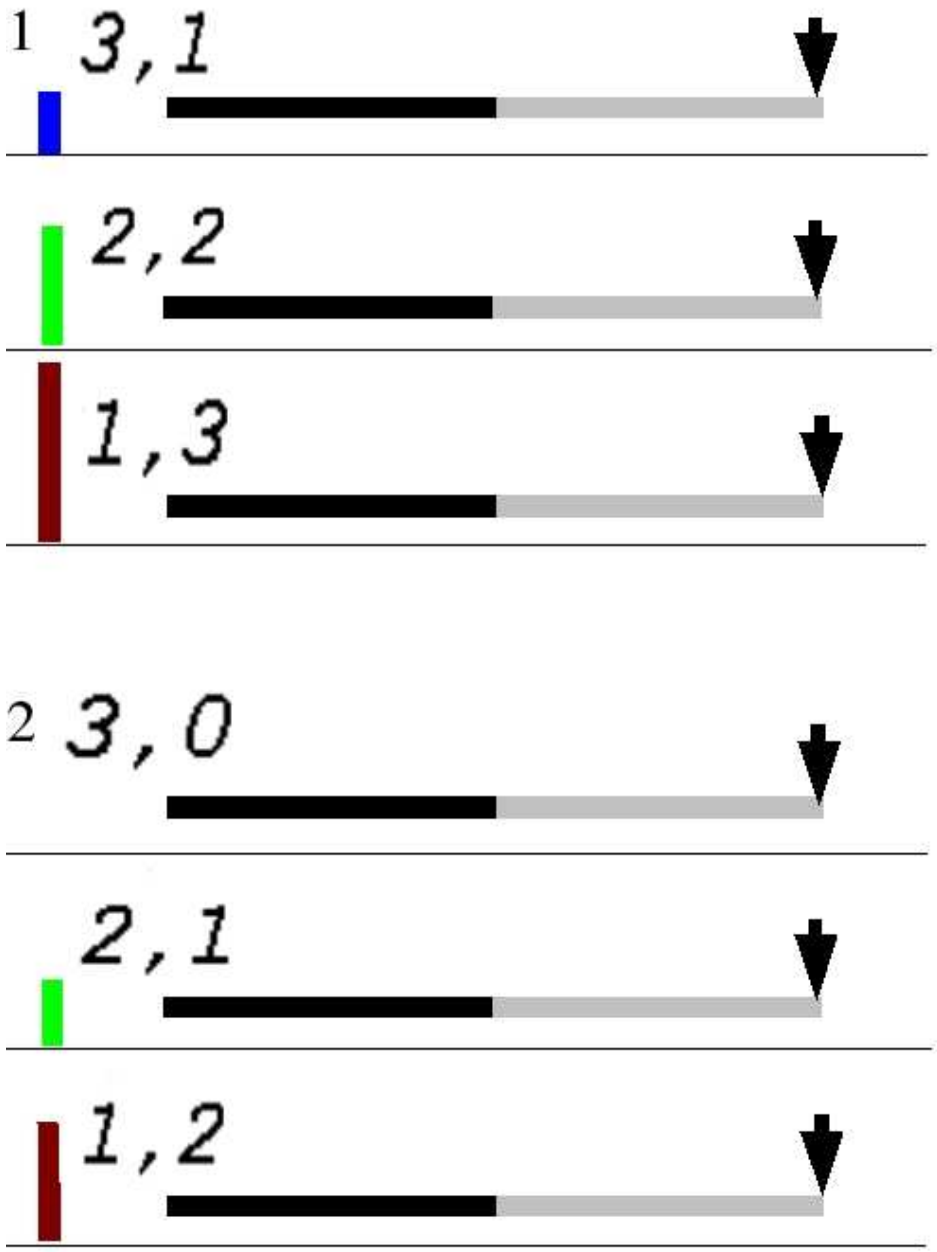
ob $w \in a^+b^+$

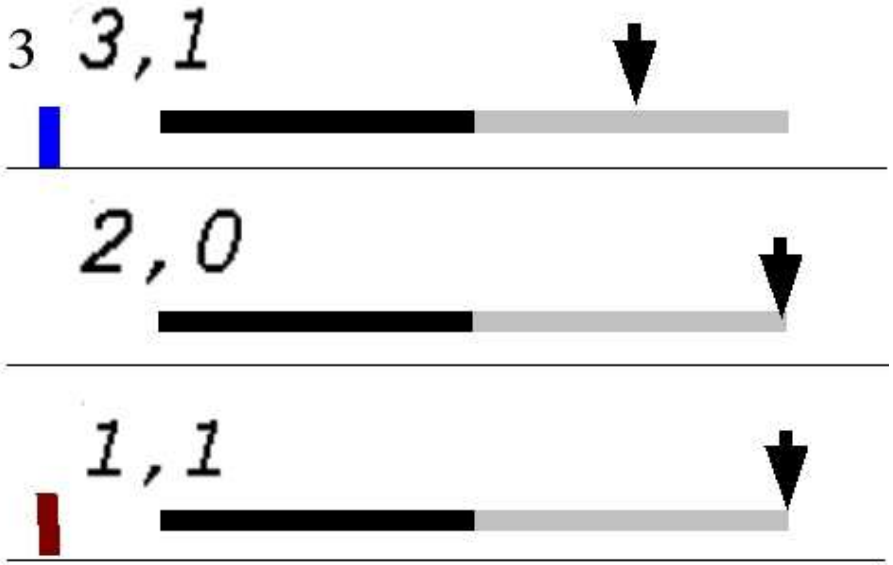
$$|\psi\rangle = \frac{1}{\sqrt{N}}(|r_{1,0}\rangle \cdots |r_{N,0}\rangle)$$

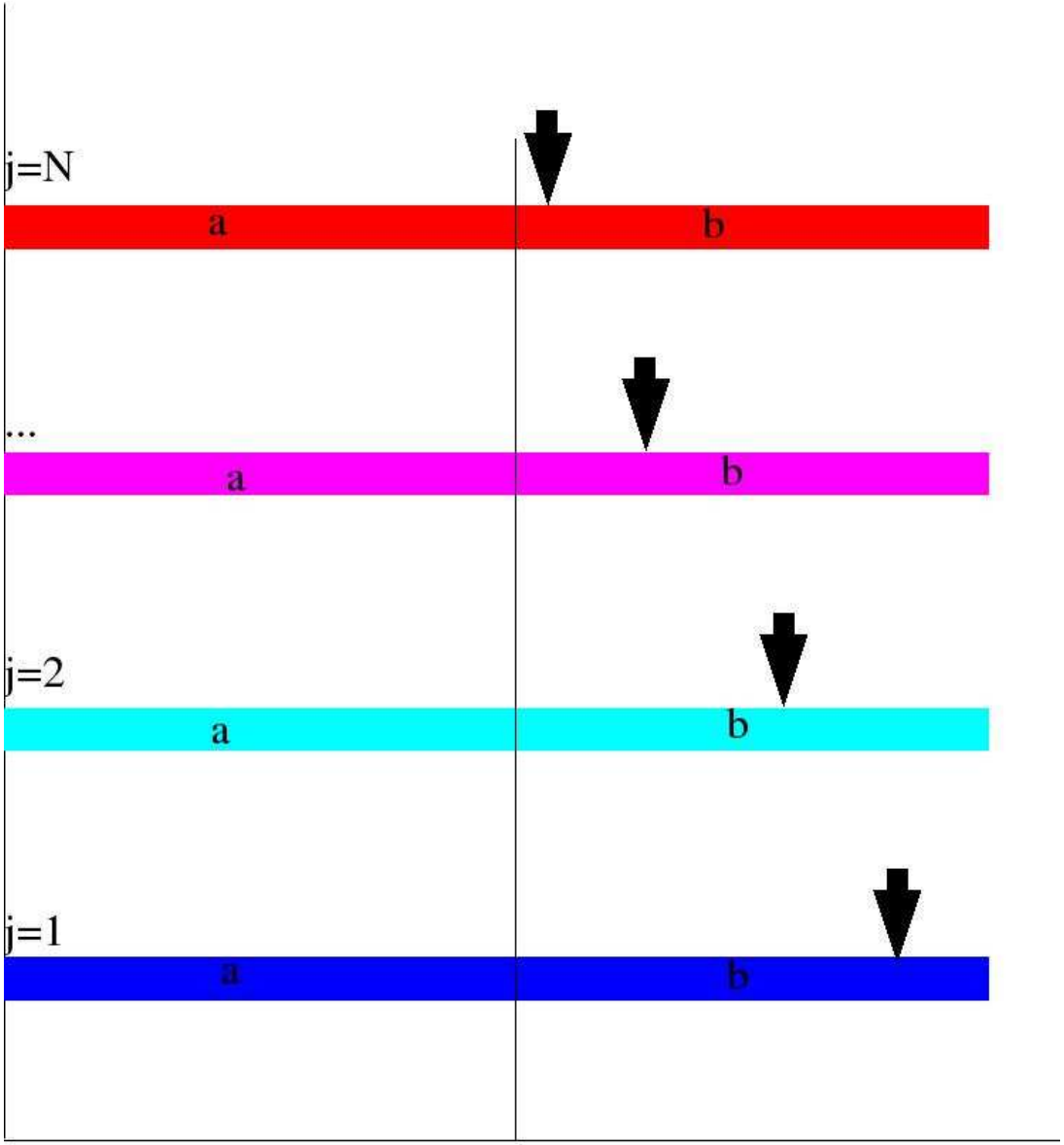



$|r_{k,N-k+1}\rangle$
0
$|r_{k,N-k}\rangle$
0
$|r_{k,N-k-1}\rangle$
0
...
$|r_{k,1}\rangle$
0
$|r_{k,0}\rangle$
−1




1
3,1
2,2
1,3
2
3,0
2,1
1,2


3
3,1
2,0
1,1


j=N
a
b
...
a
b
j=2
a
b
j=1
a
b

Beweis - Phase 2

Wieviele Schritte benötigt jeder Pfad für $w = a^u b^v$?

- Für jeden der N *Pfade:*
  - Für jeden Buchstaben b werden $N - j + 2$ Schritte benötigt
  - Für jeden Buchstaben a werden $j + 1$ Schritte benötigt
  - Insgesamt also: $(j + 1)u + (N - j + 2)v + 1$ Schritte

Beweis - Phase 2

Wieviele Schritte benötigt jeder Pfad für $w = a^u b^v$?

- Für jeden der N *Pfade:*
  - – Für jeden Buchstaben b werden $N - j + 2$ Schritte benötigt
  - – Für jeden Buchstaben a werden $j + 1$ Schritte benötigt
  - – Insgesamt also: $(j + 1)u + (N - j + 2)v + 1$ Schritte
- Unter der Annahme $j \neq j'$ gilt

  $u = v \Leftrightarrow$

  $(j + 1)u + (N - j + 2)v + 1 =$

  $(j' + 1)u + (N - j' + 2)v + 1$

Beweis - Phase 2

- Für $w \in \{a^u b^v | u = v\}$:
  – Jeder Pfad erreicht die Markierung $\dashv$ zur selben Zeit
- Andernfalls
  – erreicht jeder der Pfade die linke Endmarkierung zu einem anderen Zeitpunkt
- Quanten Fourier Transformation

Einschub: Fourier-Transformation

- Klassischer Fall
  - Eingabe: $x_0, \ldots, x_{N-1} \in \mathbb{C}$
  - Ausgabe: $y_0, \ldots, y_{N-1} \in \mathbb{C}$ mit

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k / N}$$

- Quanten Fourier-Transformation
  - Orthonormale Basis $|0\rangle, \ldots, |N-1\rangle$
  - Ausgabe:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$$

Beweis - Phase 2

- Nach der Fourier-Transformation
  - Fall 1: $w \in L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:

$$\frac{1}{N} \sum_{l=1}^{N} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} jl\right)} |s_l, 0\rangle$$

Beweis - Phase 2

- Nach der Fourier-Transformation
  - Fall 1: $w \in L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:

$$\frac{1}{N} \sum_{l=1}^{N} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} jl\right)} |s_l, 0\rangle$$

$$= \underbrace{\frac{1}{N} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} Nj\right)}}_{=1} |s_N, 0\rangle + \underbrace{\frac{1}{N} \sum_{l=1}^{N-1} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} jl\right)}}_{=0} |s_l, 0\rangle$$

Beweis - Phase 2

- Nach der Fourier-Transformation
  - Fall 1: $w \in L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:

$$\frac{1}{N} \sum_{l=1}^{N} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} jl\right)} |s_l, 0\rangle$$

$$= \underbrace{\frac{1}{N} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} Nj\right)}}_{=1} |s_N, 0\rangle + \underbrace{\frac{1}{N} \sum_{l=1}^{N-1} \sum_{j=1}^{N} e^{\left(\frac{2\pi i}{N} jl\right)}}_{=0} |s_l, 0\rangle$$

$$= |s_N, 0\rangle$$

Beweis - Phase 2

- Falls $w \notin L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:
  - Die Pfade erreichen die Markierung $\dashv$ einzeln

$$\frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle + \sum_{i \neq k} \frac{1}{\sqrt{N}} |r_{i,v_i}\rangle$$

mit $v_i \in \{0 \ldots N-1\}$

Beweis - Phase 2

- Falls $w \notin L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:
  - Die Pfade erreichen die Markierung $\dashv$ einzeln

$$\frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle + \sum_{i \neq k} \frac{1}{\sqrt{N}} |r_{i,v_i}\rangle$$

mit $v_i \in \{0 \ldots N-1\}$

  - Für den k-ten Pfad:

$$\frac{1}{\sqrt{N}} e^{\left(\frac{2\pi i}{N} kN\right)} |s_N, 0\rangle + \frac{1}{\sqrt{N}} \sum_{l=1}^{N-1} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle$$

Beweis - Phase 2

- Falls $w \notin L_{eq} = \{a^n b^n | n \in \mathbb{N}\}$:
  - Die Pfade erreichen die Markierung $\dashv$ einzeln

$$\frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle + \sum_{i \neq k} \frac{1}{\sqrt{N}} |r_{i,v_i}\rangle$$

mit $v_i \in \{0 \ldots N-1\}$

  - Für den k-ten Pfad:

$$\frac{1}{\sqrt{N}} e^{\left(\frac{2\pi i}{N} kN\right)} |s_N, 0\rangle + \frac{1}{\sqrt{N}} \sum_{l=1}^{N-1} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle$$

$$= \frac{1}{\sqrt{N}} |s_N, 0\rangle + \frac{1}{\sqrt{N}} \sum_{l=1}^{N-1} e^{\left(\frac{2\pi i}{N} kl\right)} |s_l, 0\rangle$$

  - Insgesamt wird nur mit Wahrscheinlichkeit $1/N$ akzeptiert

Offene Fragen

- QFAs mit verallgemeinerten Messungen
- Konstruktion von unterschiedlichen QFA Varianten für verschiedene Sprachen ?
- ’Pumping Lemma’ für Quantenautomaten ?

Danke für die Aufmerksamkeit !