

Space-efficient quantum automata

Andris Ambainis
Nikolay Nahimov

Department of Computer Science
University of Latvia

TQC 2008

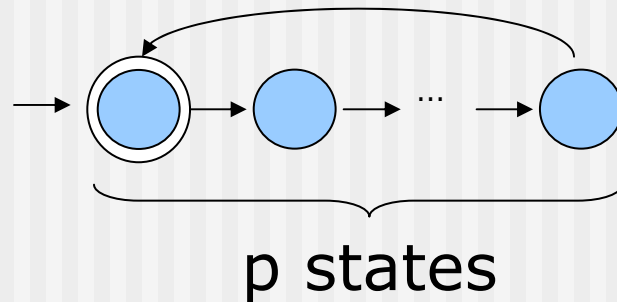
Quantum Finite Automata

- Mathematical model for quantum computers with limited memory
- Recognize the same set of languages as DFA (deterministic finite automata)
- Can be exponentially more space-efficient

Computational problem

$$L_p = \{ a^j \mid j \equiv 0 \pmod{p}, p \in P \}$$

- DFA requires $O(p)$ states



- QFA requires $O(\log(p))$ states

Known results

- A. Ambainis, R. Freivalds “1-way quantum finite automata: strengths, weaknesses and generalizations”
- A. Ambainis, N. Nahimovs “Improved constructions of quantum automata”

Improvements

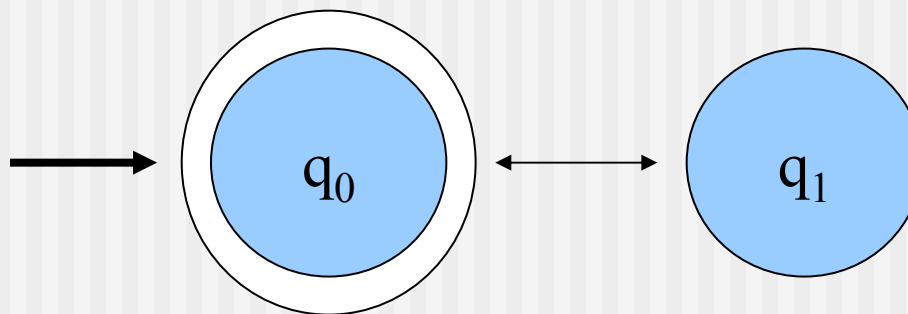
- Simpler construction with better constant in front of $\log(p)$ and with a much simpler analysis.
- A simple rule for derandomization of automata construction.

Construction steps

- Define simple 2-state QFA U_k depending on single parameter k
- Take $c \cdot \log(p)$ automata U_k with different k

Construction: building blocks

- $Q = \{q_0, q_1\}$, $Q_{\text{acc}} = \{q_0\}$, $Q_{\text{rej}} = \{q_1\}$
- Starting state q_0
- Left and right endmarker leaves state unchanged



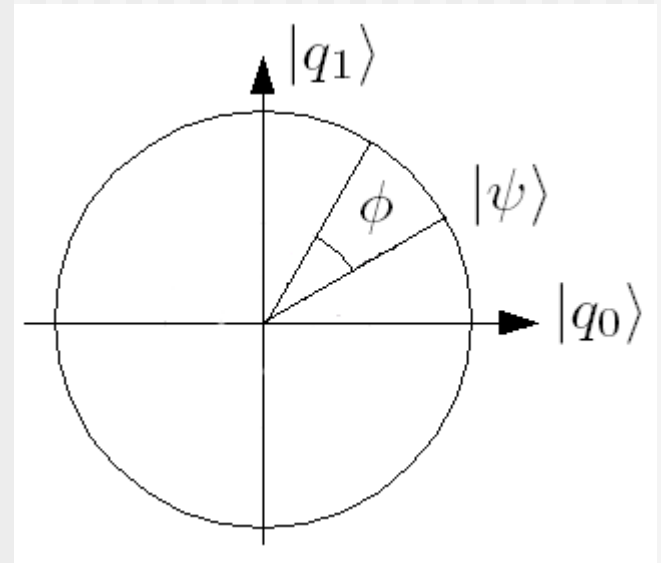
Construction: building blocks

- Reading 'a' performs U_k state "rotation"

$$|q_0\rangle \rightarrow \cos \phi_k |q_0\rangle + \sin \phi_k |q_1\rangle$$

$$|q_1\rangle \rightarrow -\sin \phi_k |q_0\rangle + \cos \phi_k |q_1\rangle$$

$$\text{where } \phi_k = \frac{2\pi k}{p}$$



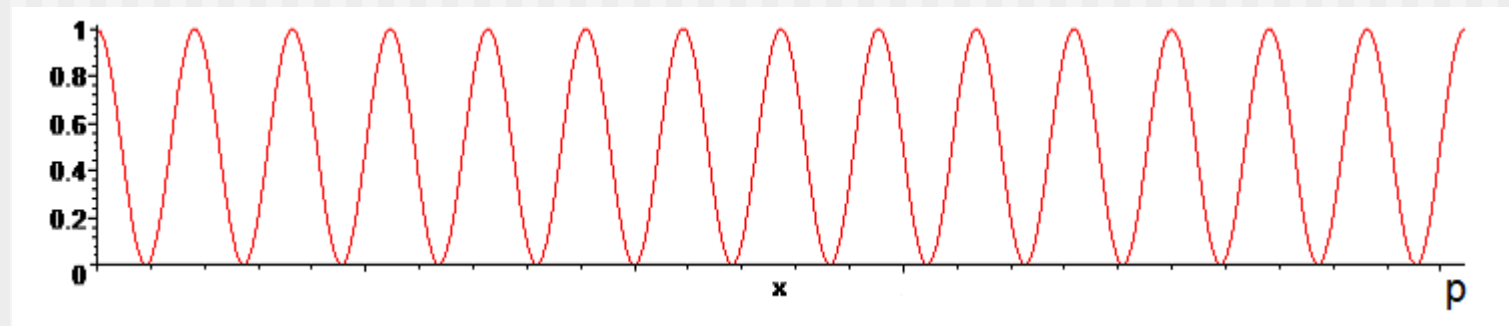
- Parameter k represents a rotation frequency

Construction: building blocks

- After reading a^j the state of U_k is

$$\cos \frac{2\pi k j}{p} |q_0\rangle + \sin \frac{2\pi k j}{p} |q_1\rangle$$

- Accepts a^j with probability $\cos^2\left(\frac{2\pi k j}{p}\right)$



Construction: building blocks

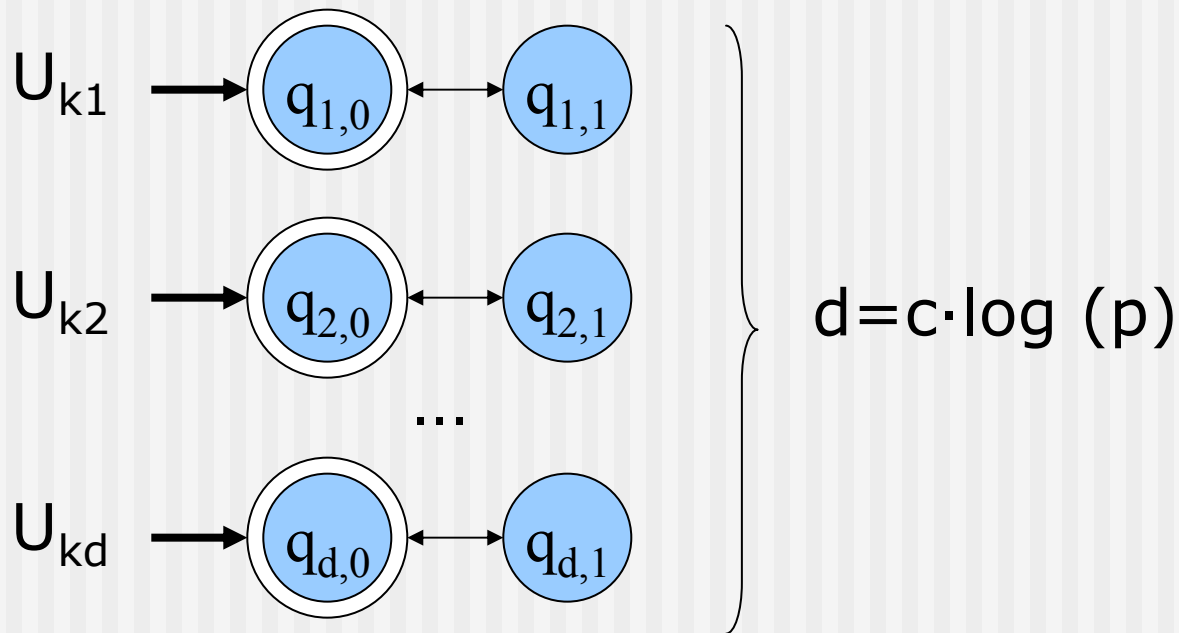
- After reading a^j the state of U_k is

$$\cos \frac{2\pi k j}{p} |q_0\rangle + \sin \frac{2\pi k j}{p} |q_1\rangle$$

- Accepts a^j with probability $\cos^2\left(\frac{2\pi k j}{p}\right)$
- If $a^j \in L_p$ accepts a^j with probability 1

Construction

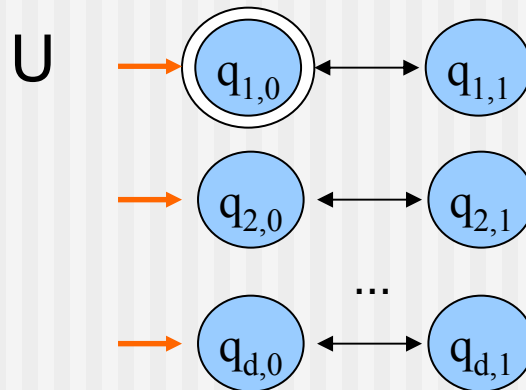
- Take $d = c \cdot \log(p)$ automata U_k with different k



Construction

- Start at equal state $|q_{i,0}\rangle$ superposition

$$|\varphi_{start}\rangle = \frac{1}{\sqrt{d}} \left(|q_{1,0}\rangle + |q_{2,0}\rangle + \dots + |q_{d,0}\rangle \right)$$



Construction

- Start at equal state $|q_{i,0}\rangle$ superposition

$$|\varphi_{start}\rangle = \frac{1}{\sqrt{d}} \left(|q_{1,0}\rangle + |q_{2,0}\rangle + \dots + |q_{d,0}\rangle \right)$$

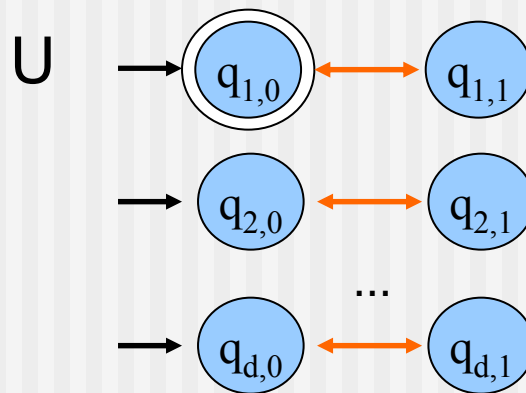
- **Alternative view:** start at $|q_{1,0}\rangle$ and on the left endmarker perform a transformation

$$|q_{1,0}\rangle \rightarrow \frac{1}{\sqrt{d}} \left(|q_{1,0}\rangle + |q_{2,0}\rangle + \dots + |q_{d,0}\rangle \right)$$

Construction

- Transformation for 'a' is as before

$$\begin{aligned} |q_{i,0}\rangle &\rightarrow \cos \phi_{k_i} |q_{i,0}\rangle + \sin \phi_{k_i} |q_{i,1}\rangle \\ |q_{i,1}\rangle &\rightarrow -\sin \phi_{k_i} |q_{i,0}\rangle + \cos \phi_{k_i} |q_{i,1}\rangle \end{aligned} \text{ where } \phi_{k_i} = \frac{2\pi k_i}{p}$$



Construction

- Transformation for 'a' is as before

$$\begin{aligned} |q_{i,0}\rangle &\rightarrow \cos \phi_{k_i} |q_{i,0}\rangle + \sin \phi_{k_i} |q_{i,1}\rangle \\ |q_{i,1}\rangle &\rightarrow -\sin \phi_{k_i} |q_{i,0}\rangle + \cos \phi_{k_i} |q_{i,1}\rangle \quad \text{where} \quad \phi_{k_i} = \frac{2\pi k_i}{p} \end{aligned}$$

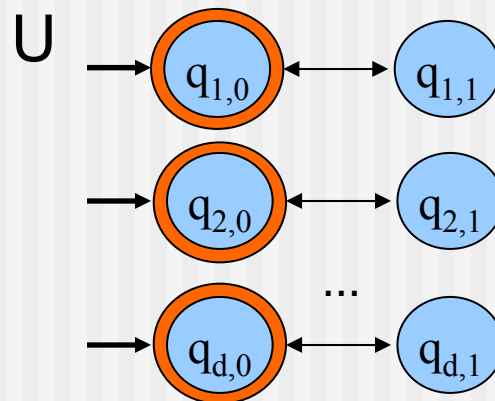
- After reading a^j the state of U is

$$\frac{1}{\sqrt{d}} \sum_i \left(\cos \frac{2\pi k_i j}{p} |q_{i,0}\rangle + \sin \frac{2\pi k_i j}{p} |q_{i,1}\rangle \right)$$

Construction

- Measure difference from initial state

$$|\varphi_{start}\rangle = \frac{1}{\sqrt{d}} \left(|q_{1,0}\rangle + |q_{2,0}\rangle + \dots + |q_{d,0}\rangle \right)$$



Construction

- Measure difference from initial state

$$|\varphi_{start}\rangle = \frac{1}{\sqrt{d}} \left(|q_{1,0}\rangle + |q_{2,0}\rangle + \dots + |q_{d,0}\rangle \right)$$

- **Alternative view:** on the right endmarker perform transformation

$$|q_{i,0}\rangle \rightarrow \frac{1}{\sqrt{d}} |q_{1,0}\rangle + \sum_j \alpha_j |q_{j,0}\rangle$$

and measure if state is $|q_{1,0}\rangle$

Construction

- Accepts a^j with probability

$$\frac{1}{d^2} \left(\cos \frac{2\pi k_1 j}{p} + \cos \frac{2\pi k_2 j}{p} + \dots + \cos \frac{2\pi k_d j}{p} \right)^2$$

- If $a^j \in L_p$ accepts a^j with probability 1
- If $a^j \notin L_p$ we want probability to be small

Theorem

For any $\varepsilon > 0$ and $p \in \mathbb{P}$, there exist k_1, k_2, \dots, k_d

$$d = \left\lceil \frac{2 \cdot \log(2p)}{\varepsilon} \right\rceil, \text{ that for all } j \in \{1, \dots, p-1\}$$

$$\frac{1}{d^2} \left(\cos \frac{2\pi k_1 j}{p} + \cos \frac{2\pi k_2 j}{p} + \dots + \cos \frac{2\pi k_d j}{p} \right)^2 < \varepsilon$$

Notes on the theorem proof

- Proof is by a probabilistic argument. It applies sequence of parameters k_1, k_2, \dots, k_d that are chosen at random.
- Proof does not give an explicit parameter sequence.
- A deterministic sequence construction rule is required.

Derandomization hypothesis

If g is a primitive root modulo $p \in P^*$, then sequence $S_g = \{ k_i \equiv g^i \pmod{p} \}_{i=1}^d$ for all d and all $j \in \{1, \dots, p-1\}$ satisfies

$$\frac{1}{d^2} \left(\cos \frac{2\pi k_1 j}{p} + \cos \frac{2\pi k_2 j}{p} + \dots + \cos \frac{2\pi k_d j}{p} \right)^2 < \varepsilon$$

* All $g^i \pmod{p}$, $i \in \{0, \dots, p-1\}$, are different

Notation

- We will refer $S_g = \{g^i \pmod{p}\}$ as cyclic sequence and g as the sequence generator.
- We will also use S_{rand} to denote a random sequence.

Hypothesis check

- We have checked all $p \in \{2, \dots, 9973\}$
- For each p all generators g
- For each p and g all sequence lengths $d < p$ choosing a corresponding ε value
- We haven't found any counterexample.

Random vs. cyclic sequences

- In 99.98% - 99.99% of our experiments, random sequences achieved the bound of theorem.
- For randomly selected $p \in P$, $\varepsilon > 0$ and generator g , a cyclic sequence S_g gives a better result than a random sequence S_{rand} in 98.29% of cases.

Random vs. cyclic sequences

- Probability of error for different p , ε and g

p	e	g	e_{rand}	e_g
1523	0.1	948	0.03635	0.01517
2689	0.1	656	0.03767	0.0195
3671	0.1	2134	0.03803	0.02122
4093	0.1	772	0.03822	0.01803
5861	0.1	2190	0.03898	0.01825
6247	0.1	406	0.03922	0.02006
7481	0.1	6978	0.03932	0.01691
8581	0.1	5567	0.03942	0.02057
9883	0.1	1260	0.04011	0.01905

Different generators

- Every $p \in P$ might have multiple generators.
- Different generators give QFA with different probabilities of error. One with a minimal error will be referred as a minimal generator.
- Typically, the minimal generator give a QFA with a substantially smaller probability of error.

Different generators

- Minimal generators for different p

p	e	g	e_g	g_min	e_g_min
1523	0.1	948	0.01517	624	0.00919
2689	0.1	656	0.0195	1088	0.0106
3671	0.1	2134	0.02122	1243	0.01121
4093	0.1	772	0.01803	1063	0.01154
5861	0.1	2190	0.01825	5732	0.01133
6247	0.1	406	0.02006	97	0.01182
7481	0.1	6978	0.01691	2865	0.01205
8581	0.1	5567	0.02057	4362	0.01335
9883	0.1	1260	0.01905	5675	0.01319

Open questions

- Strict mathematical proof of derandomization hypothesis.
- Is it possible to find a minimal generator without an exhaustive search of all generators ?
- Can other functions be represented in a similar way ?

Thank you!
