DCFS 2015

Quantum State Complexity of Formal Languages

June 26, 2015. 14:30-15:00. Waterloo, Canada

Dr. Tomoyuki Yamakami

University of Fukui, Fukui, JAPAN

Before starting my talk,

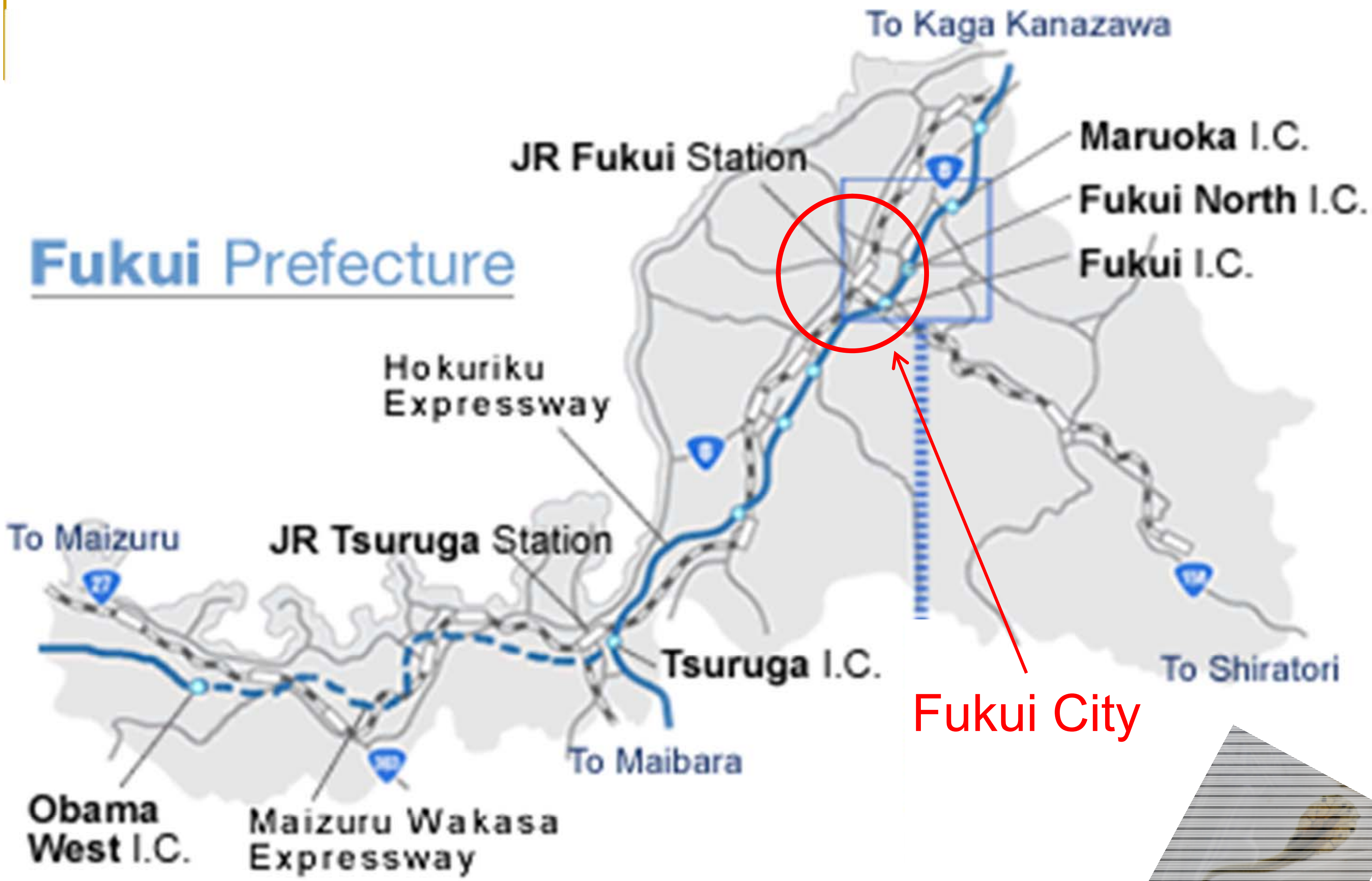
let me show you …..

Where is the University of Fukui?

47 prefectures

Tokyo - Fukui:
3 hours 30 minutes (by train)

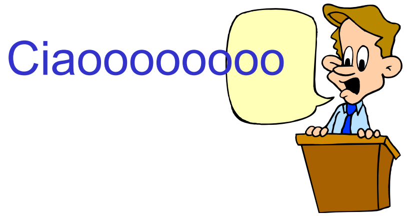
Osaka - Fukui:
1 hour 50 minutes (by train)


Fukui Prefecture
To Kaga Kanazawa
JR Fukui Station
Maruoka I.C.
Fukui North I.C.
Fukui I.C.
Hokuriku Expressway
To Maizuru
JR Tsuruga Station
Tsuruga I.C.
Fukui City
To Shiratori
To Maibara
Obama West I.C.
Maizuru Wakasa Expressway

tadpole

Let’s get back to our main theme!

Synopsis of Today's Talk



- This seminal talk is all about:
  - A state complexity measure of languages on 1-way/2-way quantum finite automata.
- I will explore
  - Basic properties of the quantum state complexity measure.
- I will demonstrate
  - A new lower bound technique for the quantum state complexity.

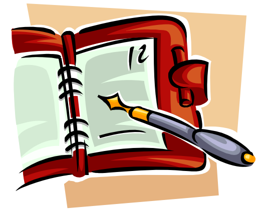
✓ homepage ↪ http://TomoyukiYamakami.ORG

✓ twitter ↪ tomoyamakami

I. Motivational Discussion

1. Why Quantum?
2. Physical Representation of Quantum Bits
3. Quantum Entanglement
4. How to Obtain Quantum Information

Why Do We Need Quantum?

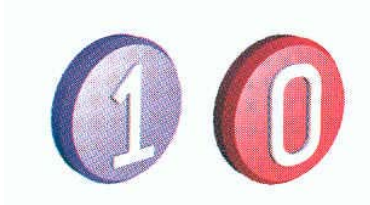


- Limitations of the existing computers
  - The existing computer will face physical difficulty in making computer chips smaller.
  - The existing computer may not solve a large number of important problems efficiently.
- Looking into physics
  - Fundamentally, a computer is a physical object.
  - The existing computer is based on classical physics whereas Nature obeys quantum mechanics.
  - Realization of the fact that information is physical.

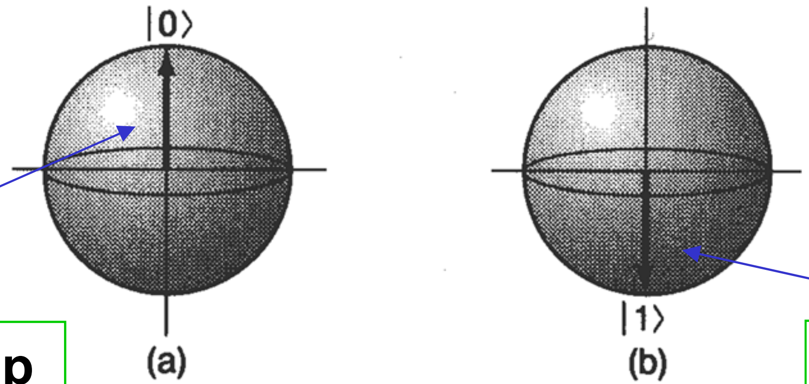
What is a Qubit?

Unit of Quantum Information

- The elementary unit of classical information is bit.



- Quantum bit (qubit) is used in quantum information theory.
- Dirac's notation is used to describe those "qubits."
  - Conventionally, we write $|0\rangle$ for bit 0 and $|1\rangle$ for bit 1.



$|0\rangle$ - spin head up

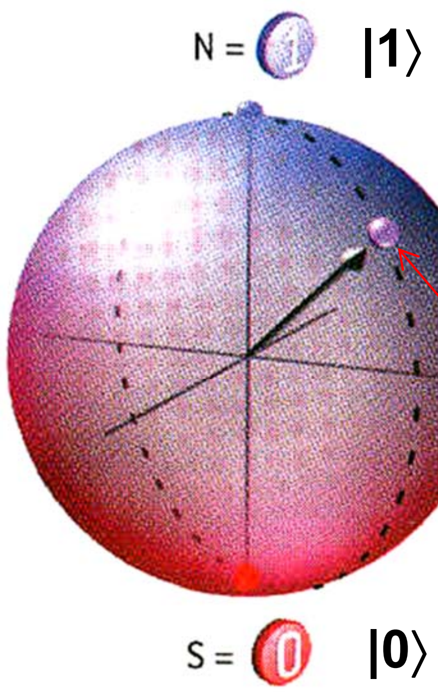
$|1\rangle$ - spin head down

Physical Representation of Quantum Bits

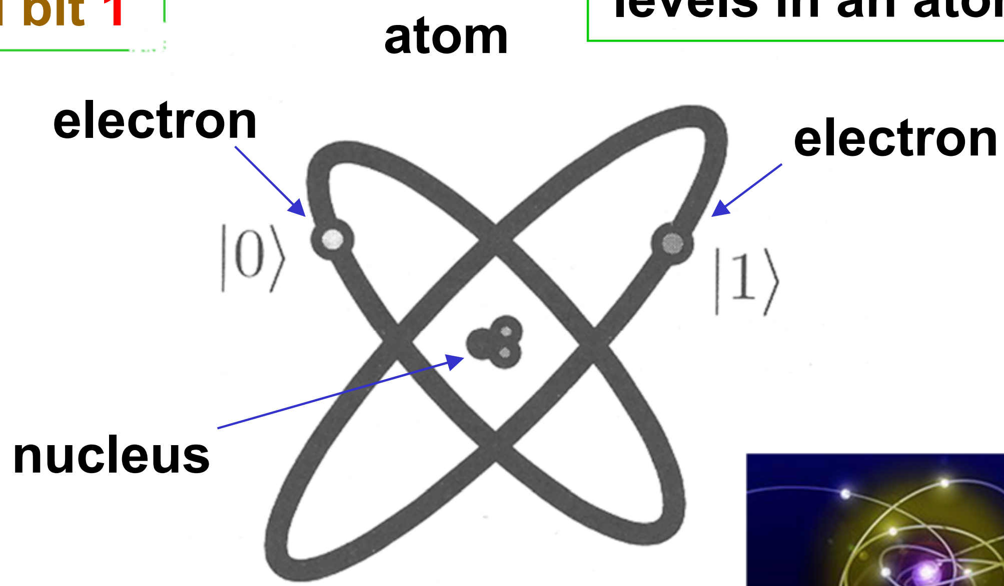
A quantum bit (qubit) is a quantum analogue of a classical bit.

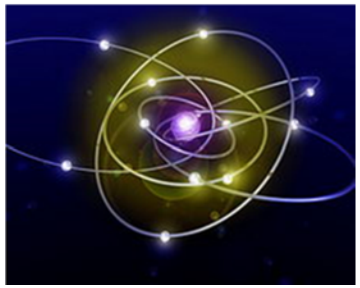
|0⟩ represents classical bit 0
|1⟩ represents classical bit 1

Two electronic levels in an atom



|φ⟩ = α|0⟩ + β|1⟩



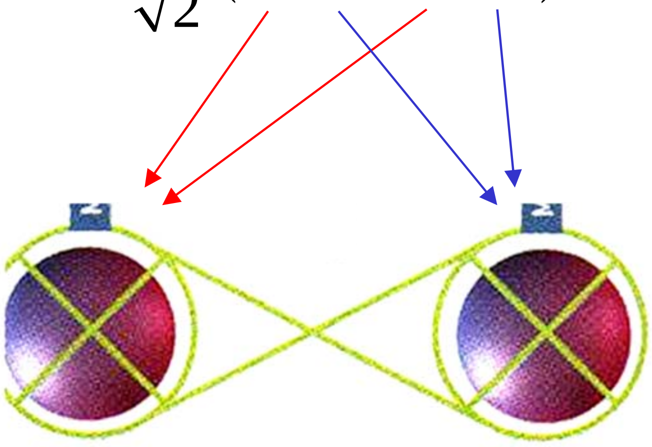


A qubit is a linear combination of |0⟩ and |1⟩.

What is Quantum Entanglement?

An EPR pair $|\psi\rangle$

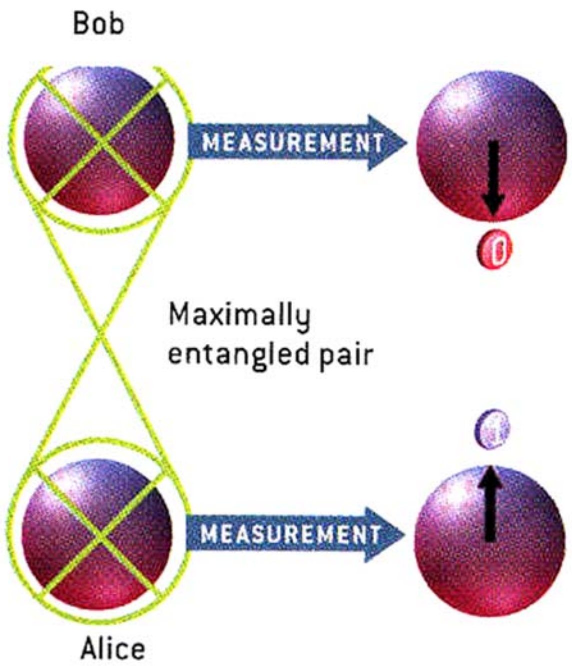
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$



Bob's qubit

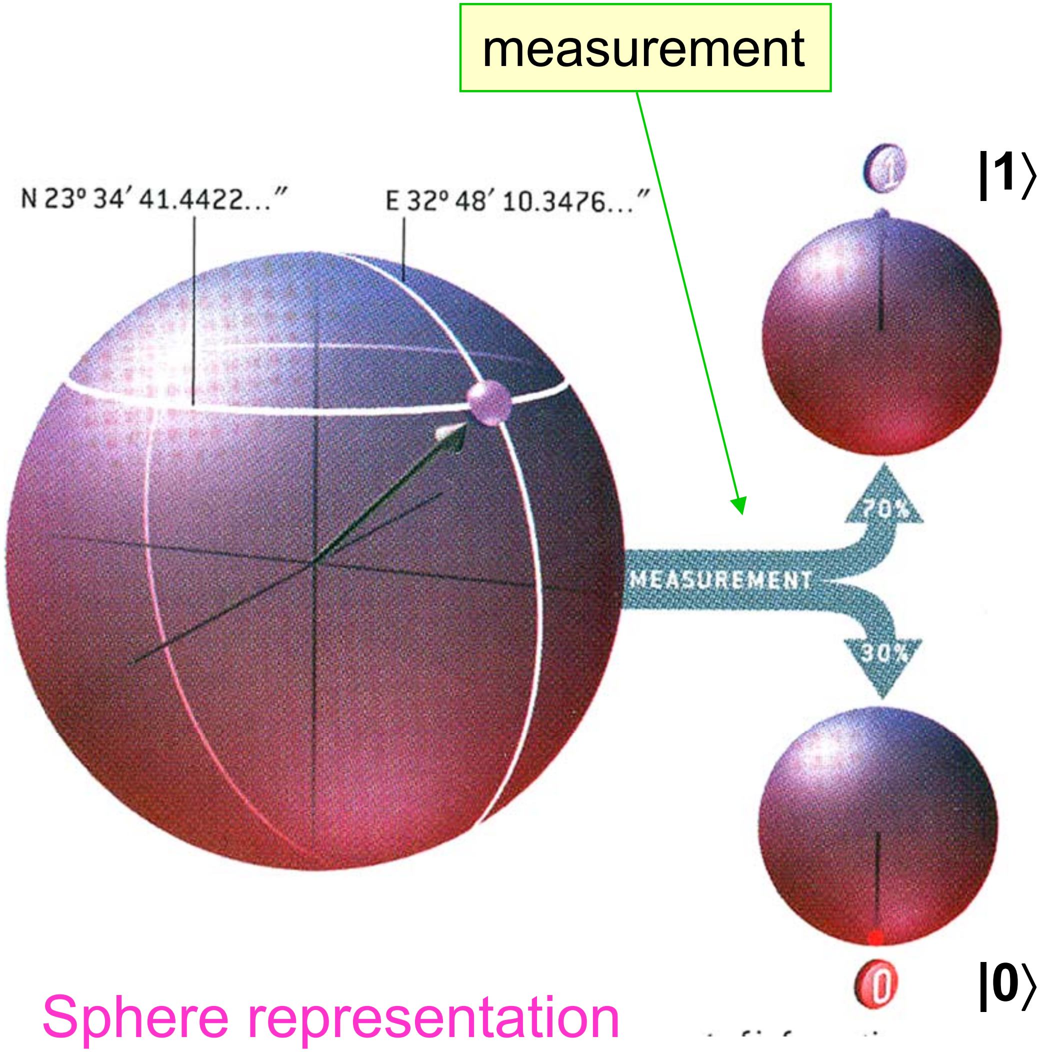
Alice's qubit

If Bob measures $|\psi\rangle$ and obtain $|0\rangle$, then Alice must obtain $|0\rangle$ after measurement.



If Bob measures $|\psi\rangle$ and obtain $|1\rangle$, then Alice must obtain $|1\rangle$ after measurement.

How to Obtain Quantum Information



Sphere representation

- The measurement is the way to find out what is going on inside the quantum system.
- When a qubit is measured, quantum mechanics requires the result to be always a classical bit.

II. Basics of Quantum Finite Automata

1. Quantum Finite Automata
2. Examples
3. More Examples

Probabilistic Finite Automata

Let's review a "standard" model of 1-way/2-way probabilistic finite automaton (or simply, 1pfa or 2pfa).

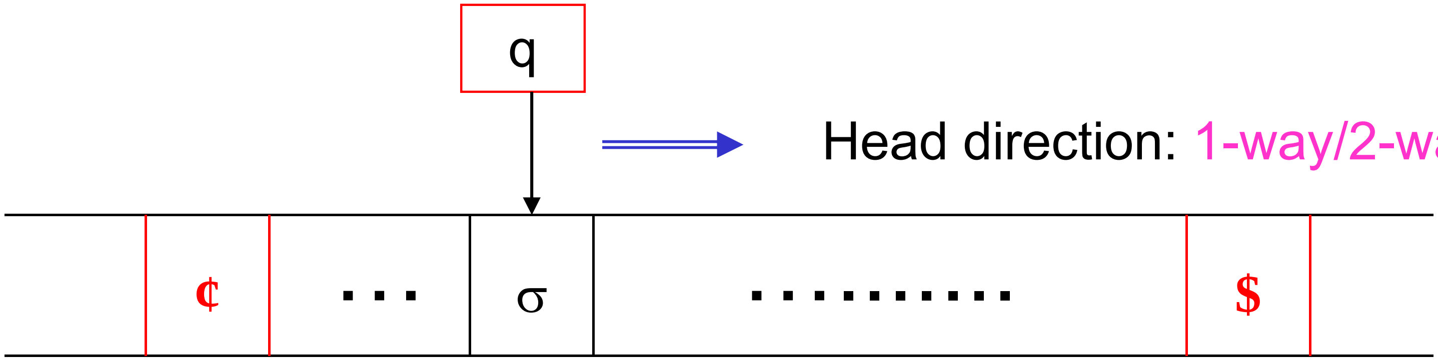
$M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$

Σ = input alphabet

$Q_{halt} = Q_{acc} \cup Q_{rej} \subseteq Q$

δ : a probabilistic transition function

Inner state $q \in Q$



Head direction: 1-way/2-way

End-marker   Infinite read-only input tape   End-marker

Formal Definition of PFAs

A 2pfa M = $(Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$ has a read-only input tape and a special probabilistic transition function δ:

$$\delta : Q \times \breve{\Sigma} \times Q \times D \rightarrow [0,1]$$

$\breve{\Sigma} = \Sigma \cup \{$ ₵, \$ $\}$

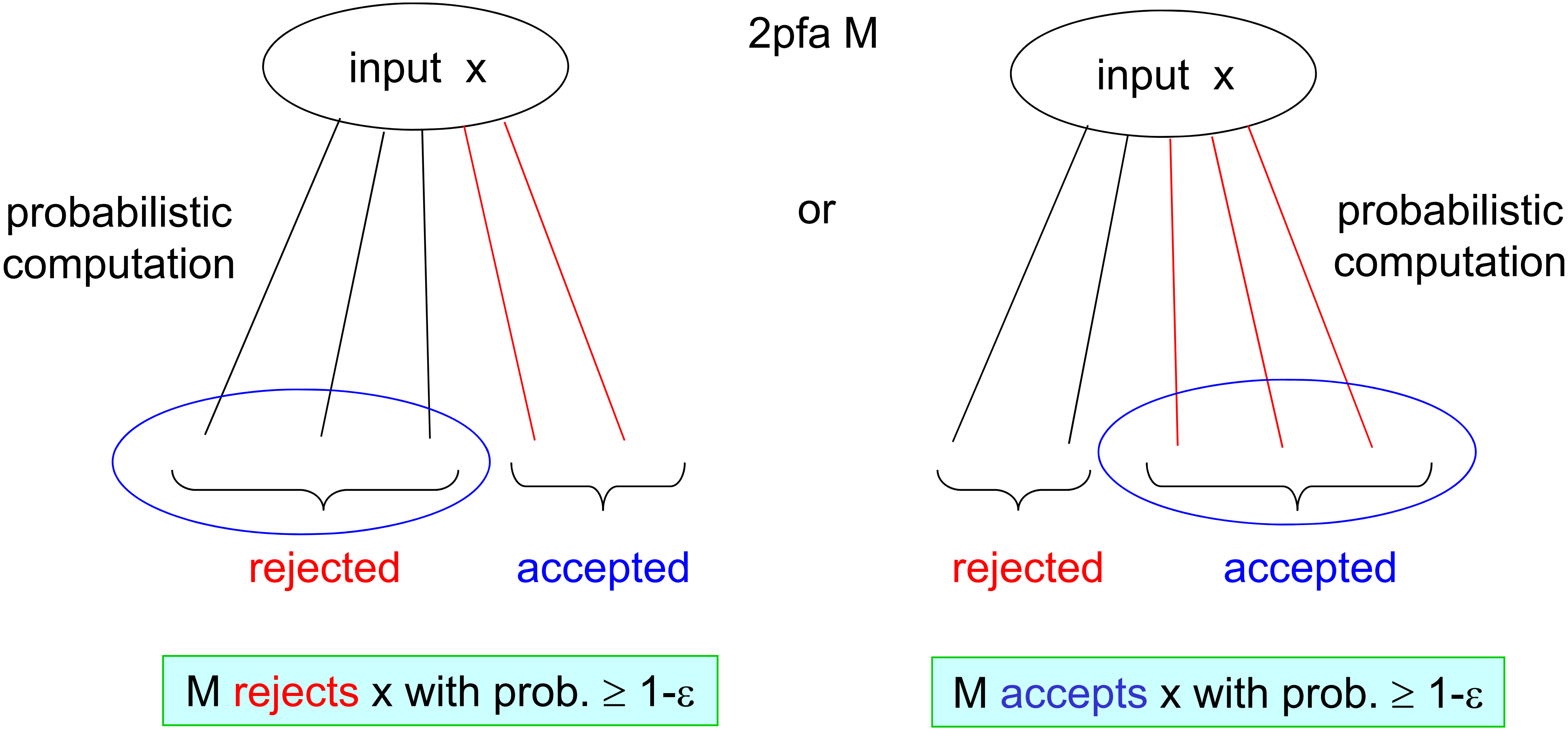
D = { -1, 0, +1 }

- Stochastic Requirement: $\forall(q,\sigma)\left[\sum_{(p,d)} \delta(q,\sigma,p,d) = 1\right]$
- Endmarker condition:
  - No tape head should move out of the region marked between ₵ and \$.

All probabilities sum up to 1.

Bounded-Error Probabilistic Computation

- A 2pfa produces **accepting/rejection computation paths**.
- $\varepsilon \in [0,1/2)$ – an error bound



1-Way/2-Way Quantum Finite Automata

- A qfa (quantum finite automaton) is similar to a pfa with a read-only input tape and a quantum transition function.

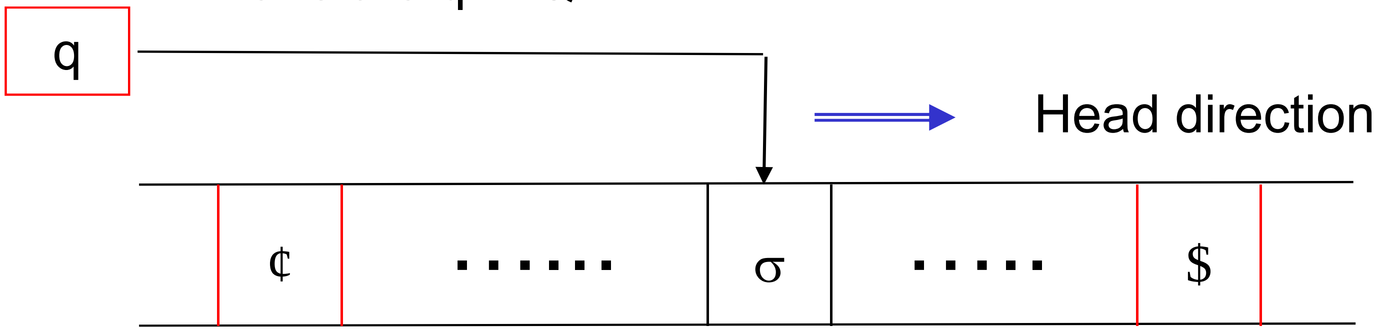
$M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$

Σ = input alphabet

$Q_{halt} = Q_{acc} \cup Q_{rej} \subseteq Q$

δ : a quantum transition function

Inner state $q \in Q$



Head direction: 1-way/2-way

Infinite read-only input tape

- For simplicity, the input tape is assumed to be circular.

Formal Definition of QFAs

A 2qfa $M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$ has a read-only input tape and a special probabilistic transition function δ:

$$\delta : Q \times \breve{\Sigma} \times Q \times D \rightarrow C$$

$\breve{\Sigma} = \Sigma \cup \{ ¢, \$ \}$

D = { -1, 0, +1 }

- Time-evolution matrix:

$$U_\delta^{(x)} |q,h\rangle = \sum_{(p,d)} \delta(q, x_h, p, d) | p, h + d \,(\mathrm{mod}\, n+1) \rangle$$

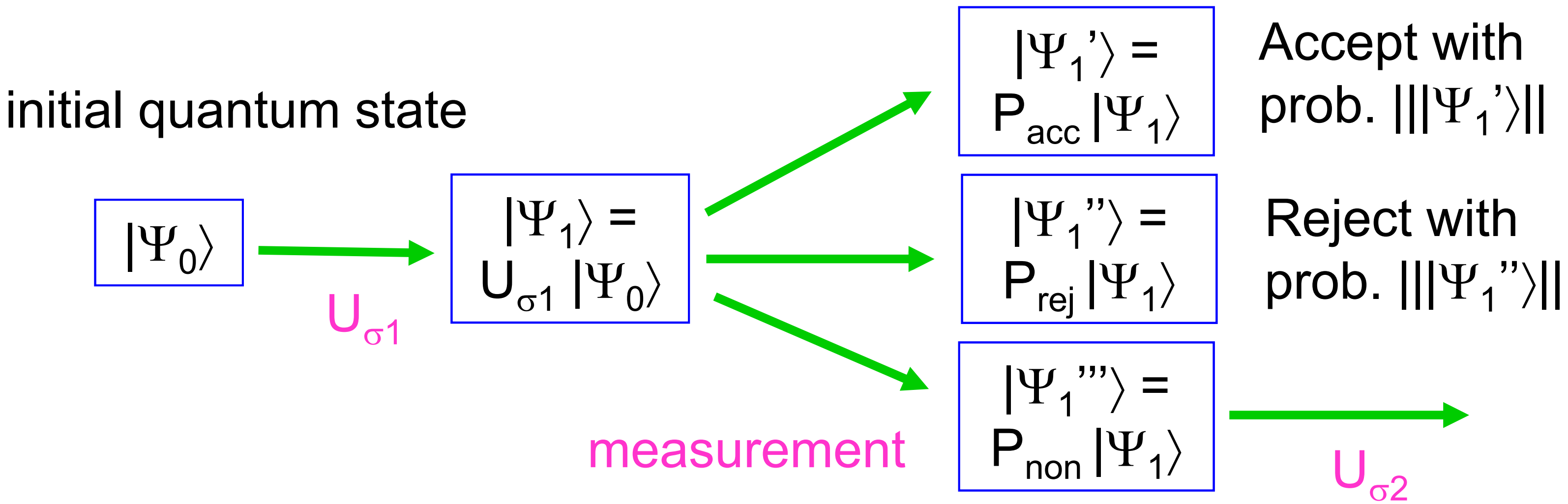
- Unitary Requirement: $U_\delta^{(x)}$ is a unitary matrix.

U is unitary ⇔ $U(U^*)^T = (U^*)^T U = I$

1-Way Quantum Finite Automata

A 1qfa can be defined much simpler.

- A 1qfa $M = (Q, \Sigma, \{U_\sigma\}_\sigma, q_0, Q_{acc}, Q_{rej})$
  - U_σ is a time-evolution operator
  - $P_{acc}, P_{rej}, P_{non}$ are (projection) measurement operators.
  - $T_\sigma = P_{non}U_\sigma$ is a transition operator.
  - $T_x = T_{\sigma n}\ T_{\sigma(n-1)} \ldots\ldots\ T_{\sigma 2}\ T_{\sigma 1}$ if $x = \sigma_1\sigma_2\ldots\sigma_n$



2BQFA

- L : language over alphabet Σ,   K : amplitude set $\subseteq$ C
- L $\in$ 2BQFA$_K$ $\Leftrightarrow$

  $\exists$M : 2qfa $\exists\varepsilon\in$[0,1/2) s.t.

  1. M has K-amplitudes
  2. $\forall x\in L$ [M accepts x with prob. $\geq 1-\varepsilon(n)$]
  3. $\forall x\in\Sigma^* - L$ [M rejects x with prob. $\geq 1-\varepsilon(n)$]

- 1BQFA $\subseteq$ REG $\subseteq$ 2BQFA

III. Quantum State Complexity

1. Past Literature I, II
2. Quantum State Complexity I, II
3. Examples
4. Basic Properties

Past Literature I

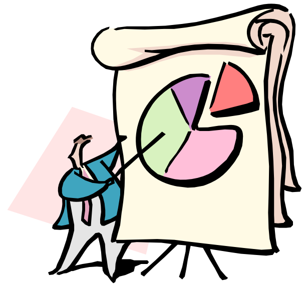
- Conservative (or traditional) state complexity concerns
  - the minimum number of inner states of M working on all inputs $x \in \Sigma^*$
- Ambanis, Freivalds (1998)
  - $L_p = \{1^n : n|p\}$ for a fixed prime p
    - O(log p) inner states on 1qfa
    - At least p inner states on 1pfa
- Mereghetti, Palano, Pighizzini (2001)
- Freivalds, Ozols, Mančinska (2009)
- Yakaryilmaz, Say (2010)
- Zheng, Gruska, Qiu (2014)

Past Literature II

- Intrinsic (or non-traditional) state complexity concerns
  - for each length $n \in N$, the minimum number of inner states of M working on inputs $x \in \Sigma^n$ (or $x \in \Sigma^{\leq n}$)

- Ambainis, Nayak, Ta-Shma, Vazirani (2002)
  - Each $L_n = \{ w0 \mid w \in \{ 0,1 \}^*, |w0| \leq n \}$ $(n \in N)$ requires
    - O(n) inner states on 1dfa
    - $2^{\Omega(n)}$ inner states on bounded-error 1qfa

Quantum State Complexity I



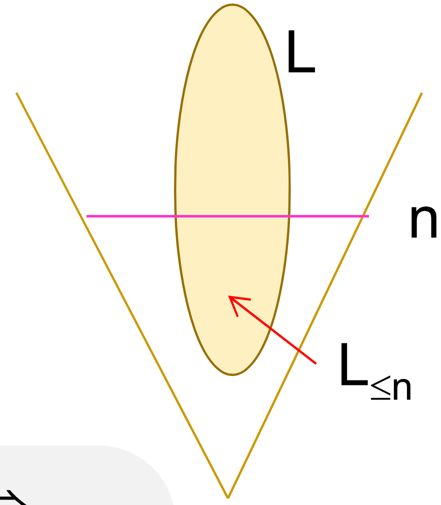
- We define quantum state complexity QSC

- $M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$: either 1qfa or 2qfa
- L : a language over Σ, $n \in N$, $L_n = L \cap \Sigma^n$
- $\varepsilon : N \to [0,1/2)$ error bound, K : amplitude set $\subseteq C$

- M recognizes L at n with error ε using K $\Leftrightarrow$
  1. M has K-amplitudes
  2. $\forall x \in L_n$ [M accepts x with prob. $\geq 1-\varepsilon(n)$]
  3. $\forall x \in \Sigma^n - L_n$ [M rejects x with prob. $\geq 1-\varepsilon(n)$]

- No requirement is imposed on the outside of Σ^n.
- State complexity of M: sc(M) = |Q| (the # of inner states)

Quantum State Complexity II



- $M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$: either 1qfa or 2qfa
- L : a language over Σ, $n \in N$,
- $L_{\leq n} = L \cap \Sigma^{\leq n}$
- M recognizes L up to n with error ε using K $\Leftrightarrow$
  1. M has K-amplitudes
  2. $\forall x \in L_{\leq n}$ [M accepts x with prob. $\geq 1-\varepsilon(n)$]
  3. $\forall x \in \Sigma^{\leq n} - L_{\leq n}$ [M rejects x with prob. $\geq 1-\varepsilon(n)$]
- No requirement is imposed on the outside of $\Sigma^{\leq n}$.
- State complexity of M: sc(M) = |Q| (the # of inner states)

Definition of 1QSC/2QSC

- We define $1QSC_{K,\varepsilon}[L]()$ and $2QSC_{K,\varepsilon}[L]()$.
  - L : a language over Σ, $n \in N$
  - $\varepsilon : N \rightarrow [0,1/2)$ error bound, K : amplitude set $\subseteq C$

- $1QSC_{K,\varepsilon}[L](n) = \min_M \{ sc(M) :$ 1qfa M recognizes L at $n \}$
- $2QSC_{K,\varepsilon}[L](n) = \min_M \{ sc(M) :$ 2qfa M recognizes L at $n \}$

- $1QSC_{K,\varepsilon}[L](\leq n) = \min_M \{ sc(M) :$ 1qfa M recognizes L up to $n \}$
- $2QSC_{K,\varepsilon}[L](\leq n) = \min_M \{ sc(M) :$ 2qfa M recognizes L up to $n \}$

Relationships

- $1QSC_{K,\varepsilon}[L](n) \leq 1QSC_{K,\varepsilon}[L](\leq n)$, $2QSC_{K,\varepsilon}[L](n) \leq 2QSC_{K,\varepsilon}[L](\leq n)$

Examples

- The following properties hold for alphabet Σ with $|\Sigma|\geq 2$.

- $\forall L \in$ 2BQFA over Σ ($|\Sigma|\geq 2$)
  $\exists \varepsilon \in [0,1/2)$ s.t. $2QSC_{C,\varepsilon}[L](\leq n) = O(1)$

- PROOF:
  Since $L \in$ 2BQFA implies $\exists M$:2qfa $\exists \varepsilon$ [M recognizes L with prob. $\geq 1-\varepsilon$, the traditional state complexity of M equals O(1). Therefore, $2QSC_{C,\varepsilon}[L](\leq n) = O(1)$.

Basic Properties

- The following properties hold for alphabet Σ with $|\Sigma| \geq 2$.

- $1 \leq 2QSC_{K,\varepsilon}[L](n) \leq |\Sigma|^n + 1$
- $2QSC_{K,\varepsilon}[L^c](n) = 2QSC_{K,\varepsilon}[L](n)$, where $L^c = \Sigma^* - L$.
- $2QSC_{C,\varepsilon}[L](n) \leq 2QSC_{R,\varepsilon}[L](n) \leq 2 \bullet 2QSC_{C,\varepsilon}[L](n)$

- An exponential gap between $1QSC_{C,\varepsilon}[L](\leq n)$ and $1QSC_{C,\varepsilon}[L](n)$

- $\exists L \in REG\ \forall \varepsilon \in (0,1/2)$

$$1QSC_{C,\varepsilon}[L](\leq n) = 2^{\Omega(1QSC_{C,\varepsilon}[L](n))}$$

IV. Main Results

1. Union/Intersection
2. Advised Computation
3. Approximate Matrix Rank
4. Future Challenges

Union/Intersection (1QFAs)

- 1BQFA is not closed under union or intersection.

Proposition (upper bound)

$\forall\ L_1,L_2\ \ \forall\varepsilon\ (0 \leq \varepsilon(n) < (3-\sqrt{5})/2)\ \forall\circledcirc\in\{\cap, \cup\}.$

Let $1QSC_{C,\varepsilon}[L_1](n) = k_1(n)$ and $1QSC_{C,\varepsilon}[L_2](n) = k_2(n)$.

$$1QSC_{C,\varepsilon}[L_1 \circledcirc L_2](n) \leq 8(n+3)k_1(n)k_2(n),$$

where

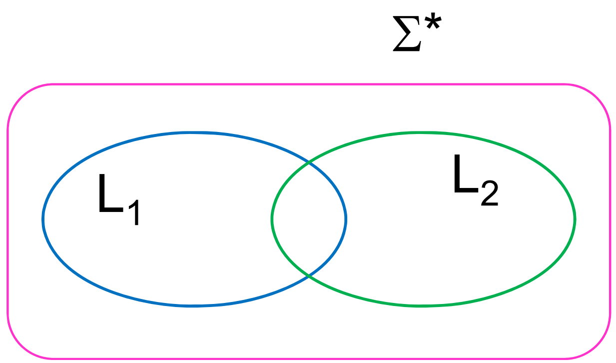
$$\varepsilon'(n) = \frac{\varepsilon(n)(2-\varepsilon(n))}{1+\varepsilon(n)-\varepsilon(n)^2}$$

- PROOF: By a direct simulation of minimal 1qfa's M_1 and M_2 for L_1 and L_2, respectively.

Union/Intersection (2QFAs)

- It is not yet known whether 2BQFA is closed under union or intersection.
- In other words, we do not know that, for $L_1, L_2 \in 2BQFA_C$,

$$2QSC_{C,\varepsilon}[L_1 \circ L_2](n) = O(1)$$



- Proposition (upper bound)

$\forall L_1, L_2 \in 2BQFA_A$ over Σ ($|\Sigma| \geq 2$)

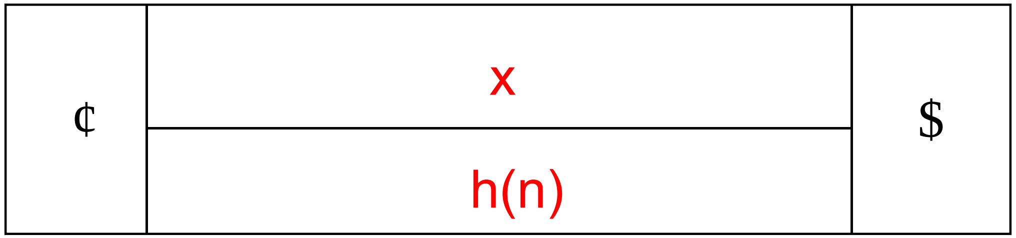
$$2QSC_{A,0}[L_1 \circ L_2](n) = 2^{O(\log^2 n)}$$

where $\circ \in \{\cap, \cup\}$.

Advised Computation

- Input string $x \in \Sigma^n$ over an input alphabet Σ
- Advice alphabet Γ
- Advice string h(n), depending only on length n of x

- Two-track representation



Damm and Holzer (1995) defined "advice" in a quite different manner.

Advice string h(n) is given in the lower track of the tape.

- Regarding advice, there are two important questions to ask.
  1. How powerful is advice?
  2. Is there any limitation of advice?

(*) Tadaki, Yamakami, and Lin. SOFSEM 2004, LNCS Vol.2932, 2004.

Track Notation for Advice

- More precisely, we use the following two-track representation of [Tadaki-Yamakami-Lin04].

$$\begin{bmatrix} x \\ w \end{bmatrix} = \begin{bmatrix} x_1 \\ w_1 \end{bmatrix} \begin{bmatrix} x_2 \\ w_2 \end{bmatrix} \cdots \begin{bmatrix} x_i \\ w_i \end{bmatrix} \cdots \begin{bmatrix} x_n \\ w_n \end{bmatrix} \quad \text{if} \quad \begin{cases} x = x_1 x_2 \cdots x_i \cdots x_n \\ w = w_1 w_2 \cdots w_i \cdots w_n \end{cases}$$

Each of them is treated as a new symbol.

$$\begin{bmatrix} x_i \\ w_i \end{bmatrix}$$ new symbol

When written on an input tape:

Upper track	¢	.....	x_i	.....	$
Lower track		.....	w_i	.....	

(*) Tadaki, Yamakami, and Lin. SOFSEM 2004, LNCS Vol.2932, 2004.

Advised Language Families

Quantum computation with deterministic advice

- Let L be any language over an alphabet Σ.

- L$\in$1BQFA/n

  $\Leftrightarrow \exists$M:1qfa $\exists\ \varepsilon\in[0,½)$ $\exists\Gamma$:advice alphabet $\exists h:N\rightarrow\Gamma^*$

  1. $\forall n\in N$ [$|h(n)| = n$].
  2. $\forall x\in\Sigma^n$ [$x\in L \leftrightarrow$ M accepts $[x\ h(|x|)]^T$ with prob $\geq 1-\varepsilon$].

- L$\in$2BQFA/n

  $\Leftrightarrow \exists$M:2qfa $\exists\ \varepsilon\in[0,½)$ $\exists\Gamma$:advice alphabet $\exists h:N\rightarrow\Gamma^*$

  1. $\forall n\in N$ [$|h(n)| = n$].
  2. $\forall x\in\Sigma^n$ [$x\in L \leftrightarrow$ M accepts $[x\ h(|x|)]^T$ with prob $\geq 1-\varepsilon$].

State Complexity vs. Advice

- Proposition

$$\forall L \in 2BQFA/n \text{ over } \Sigma \ (|\Sigma| \geq 2) \ \exists \varepsilon \in [0,1/2)$$
$$\text{s.t. } 2QSC_{C,\varepsilon}[L](n) = O(n)$$

- This is compared to:

$$\forall L \in 2BQFA \text{ over } \Sigma \ (|\Sigma| \geq 2) \ \exists \varepsilon \in [0,1/2)$$
$$\text{s.t. } 2QSC_{C,\varepsilon}[L](n) = O(1)$$

A length-n advice string is somewhat equivalent to O(n) extra inner states.

Approximate Matrix Rank

- $L \subseteq \Sigma^*$: a language over alphabet Σ
- M_L: characteristic matrix for L $\Leftrightarrow$
  $\forall x,y \in \Sigma^*$

$$M_L(x,y) = \begin{cases} 1 & \text{if } xy \in L \\ 0 & \text{if } xy \notin L \end{cases}$$

This means that $\|P_n - M_L(n)\|_\infty \le \varepsilon$

- $M_L(n)$: a restriction of M_L on strings (x,y) with $|xy| \le n$
- $P_n = (p_{xy})_{x,y}$ with $|xy| \le n$: a matrix
  s.t. p_{xy} = acceptance probability of A on input xy

FACT:
P_n ε-approximates $M_L(n)$ $\Leftrightarrow$ A recognizes $L_{\le n}$ with error prob $\le \varepsilon$

State Complexity vs. Approximate Rank

- Theorem

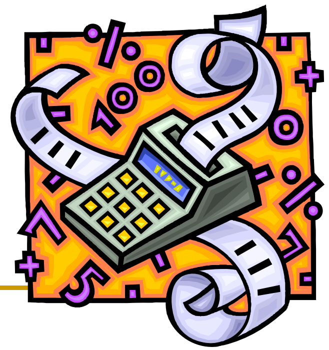
∀t: function on N ∀L ∀ε,ε' (0<ε'<ε<1/2),

$$2QSC^{t}_{R,\varepsilon'}[L](\leq n) \geq \frac{\sqrt{rank^{\varepsilon}(M_L(n))}}{\sqrt{t'(n)(t'(n)+1)(n+1)}}$$

where $t'(n)=\lceil t(n)/(\varepsilon-\varepsilon')\rceil$,

- Corollary

$L \not\subset$ 2BQFA(t-time), where $t(n) = 2^{n/6}/n^2$



Future Challenges

1. Explore more general properties of 1QSC/2QSC.
   - E.g., closure properties
2. Prove or disprove:
   - For any $L_1, L_2 \in$ 2BQFA, $L_1 \odot L_2 \in$ 2BQFA, where $\odot \in \{ \cap, \cup \}$.
3. Discover new techniques to prove lower bounds of 2QSC.
   - E.g., diagonalization techniques

Thank you for listening

Q & A

I’m happy to take your question!

END

Thank you for listening!