13th Week

Quantum State Complexity and Advice

Synopsis.

- Quantum Sate Complexity
- Quantum Advice
- BQP/poly and BQP/Qpoly

July 2, 2018. 23:59

Course Schedule: 16 Weeks

Subject to Change

- Week 1: Basic Computation Models
- Week 2: NP-Completeness, Probabilistic and Counting Complexity Classes
- Week 3: Space Complexity and the Linear Space Hypothesis
- Week 4: Relativizations and Hierarchies
- Week 5: Structural Properties by Finite Automata
- Week 6: Stype-2 Computability, Multi-Valued Functions, and State Complexity
- Week 7: Cryptographic Concepts for Finite Automata
- Week 8: Constraint Satisfaction Problems
- Week 9: Combinatorial Optimization Problems
- Week 10: Average-Case Complexity
- Week 11: Basics of Quantum Information
- Week 12: BQP, NQP, Quantum NP, and Quantum Finite Automata
- Week 13: Quantum State Complexity and Advice
- Week 14: Quantum Cryptographic Systems and Quantum Functions
- Week 15: Quantum Interactive Proofs and Quantum Optimization
- Week 16: Final Evaluation Day (no lecture)

YouTube Videos

- This lecture series is based on numerous papers of T. Yamakami. He gave conference talks (in English) and invited talks (in English), some of which were video-recorded and uploaded to YouTube.
- Use the following keywords to find a playlist of those videos.
- YouTube search keywords:

  Tomoyuki Yamakami conference invited talk playlist

Conference talk video

Main References by T. Yamakami

✎ H. Nishimura and T. Yamakami. Polynomial time quantum computation with advice. Inf. Process. Lett. 90, 195-209 (2004)

✎ T. Yamakami. One-way reversible and quantum finite automata with advice. Information and Computation, Vol. 239, pp. 122-148 (2014)

✎ T. Yamakami. Complexity bounds of constant-space quantum computation. DLT 2015, Lecture Notes in Computer Science, Springer-Verlag, Vol. 9168, pp. 426-438 (2015)

✎ M. Villagra and T. Yamakami. Quantum state complexity of formal languages. DCFS 2015, Lecture Notes in Computer Science, Springer-Verlag, Vol. 9118, pp. 280-291 (2015)

I. Quantum Advice

1. Classical Advice
2. Non-Uniform Complexity Class BQP/poly
3. Generalization to BQP/F
4. Properties of BQP/F
5. Computation with Quantum Advice
6. BQP/Qpoly
7. Generalization to BQP/Q(F)
8. Properties of BQP/Q(F)

Classical Advice (revisited)

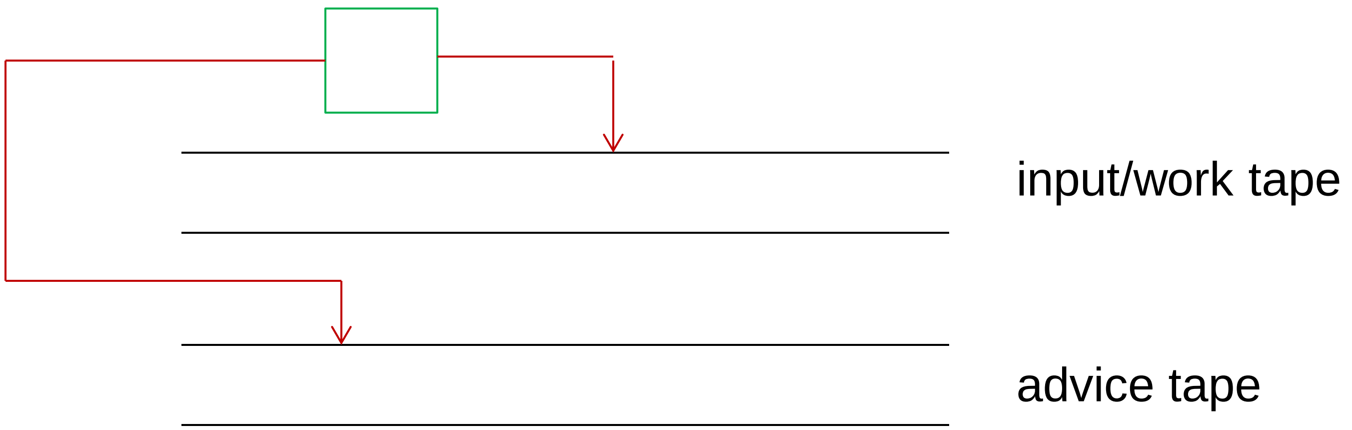
- Recall the notion of advice from Weeks 3 & 5.
- In those weeks, we have considered two types of advice:

  1. deterministic advice, and
  2. randomized advice.

- For clarity, we call such advice classical advice.

Non-Uniform Class P/poly (revisited)

- Recall from Week 3 the non-uniform complexity class P/poly, which is defined by polynomial-time DTMs equipped with advice tapes.



- Recall that non-uniform families of polynomial-size circuits also characterize P/poly (in Week 3).

Non-Uniform Complexity Class BQP/poly I

- Recall the quantum polynomial-time complexity class BQP from Week 12.
- Nishimura and Yamakami (2004) defined complexity class BQP/poly, which is a quantum analogue of P/poly.

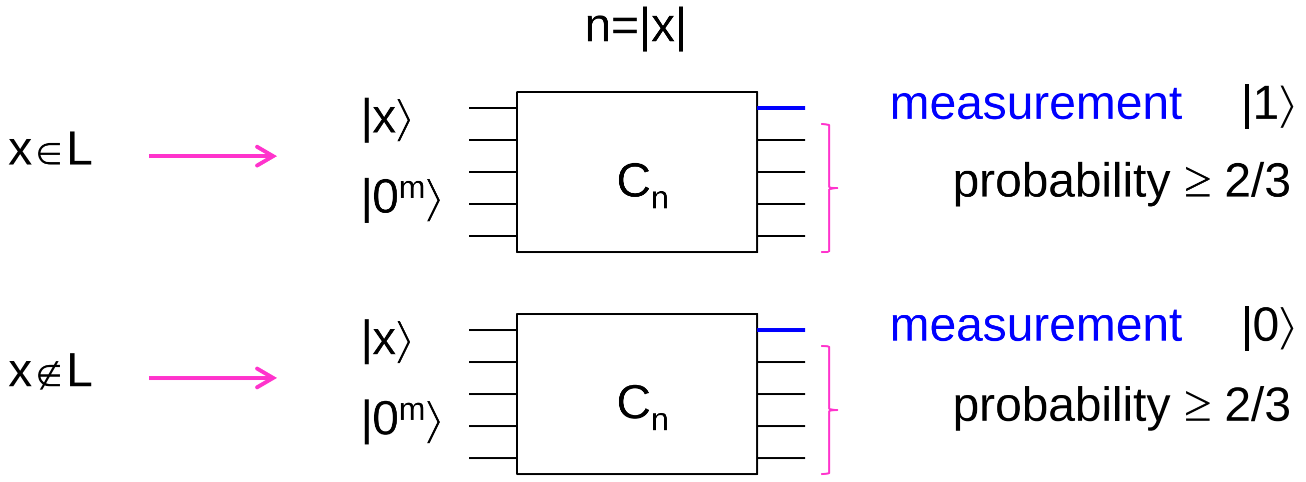
- A language L is in BQP/poly $\Leftrightarrow$ there are a positive polynomial p, an advice function h, and a QTM M equipped with an advice tape such that, for any input x,
  - $|h(|x|)| \leq p(|x|)$ and
  - $x \in L \leftrightarrow$ M accepts $(x,h(|x|))$ with probability $\geq 2/3$.

Non-Uniform Complexity Class BQP/poly II

- Nishimura and Yamakami (2004) proved the following nice characterization of BQP/poly in terms of polynomial-size quantum circuits.

- Theorem: [Nishimura-Yamakami (2004)]

  $L \in$ BQP/poly $\Leftrightarrow$ L has a non-uniform family of polynomial-size quantum circuits C_n with error probability at most 1/3.



Generalization to BQP/F

- By taking a different set F of functions, we can define a non-uniform complexity class BQP/F as a generalization of BQP/poly.
- Let F be a set of functions from N $\rightarrow$ N.
- A language L over alphabet Σ is in BQP/F $\Leftrightarrow$ there are a function f $\in$ F, an advice alphabet Γ, an advice function h: N $\rightarrow \Gamma^*$, and a polynomial-time QTM M equipped with an advice tape such that, for all input $x \in \Sigma^*$,
  - $|h(|x|)| \leq f(|x|)$ and
  - $x \in L \leftrightarrow$ M accepts (x,h(|x|)) with probability $\geq 2/3$.

Properties of BQP/F

- Nishimura and Yamakami (2004) presented the following properties of BQP/F for various class F of functions.

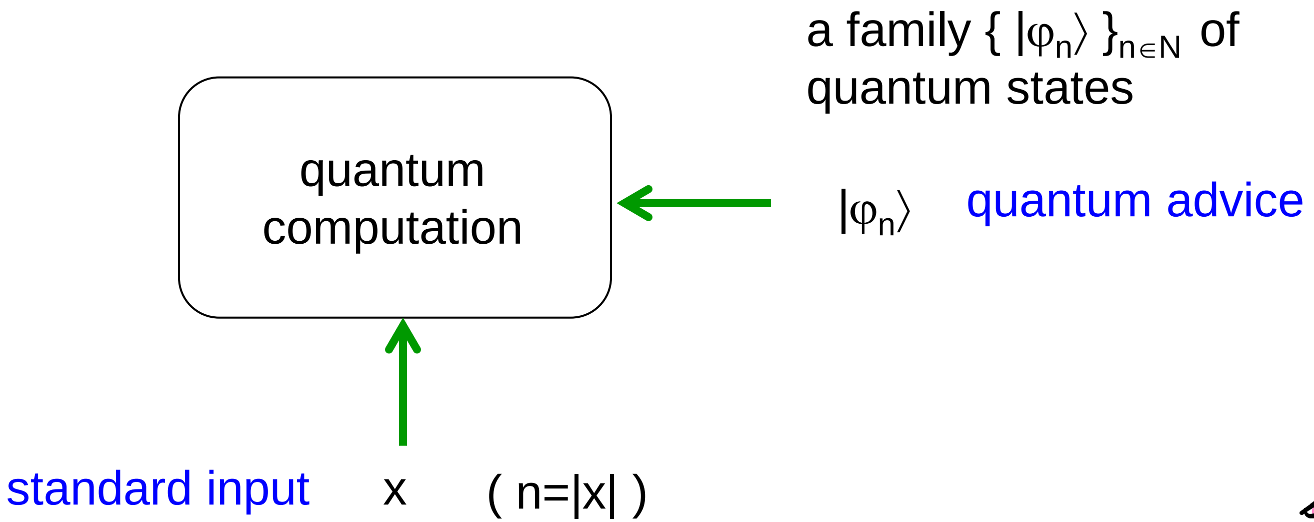
- Theorem:
  1. BQP/poly = BQP^{TALLY}
  2. ESPACE $\not\subseteq$ BQP/poly
  3. $BQP_C \subseteq BQP/\log^3$
  4. BQP/1 $\not\subseteq$ BQP_C

ESPACE consists of all languages recognized by DTMs using $2^{O(n)}$ space.

$\log^3$ means the set of functions of the form $c\log^3(n)+d$ for constants c,d > 0.

Computation with Quantum Advice

- Nishimura and Yamakami (2004) first considered quantum advice for polynomial-time quantum computation.
- We run a machine that takes two inputs, which are a standard input and advice.



BQP/Qpoly I

- With the use of quantum advice, Nishimura and Yamakami (2004) defined complexity class BQP/Qpoly.
- A language L is in BQP/Qpoly $\Leftrightarrow$ there are a positive polynomial p, a family $\{ |\varphi_n\rangle \}_{n \in N}$ of quantum states, and a QTM M with an advice tape such that, for any input x of length n,
  - $|\varphi_n\rangle$ is a quantum state of dimension $2^{p(n)}$,
  - $x \in L \rightarrow$ M accepts $(x,|\varphi_n\rangle)$ with probability $\geq 2/3$,
  - $x \notin L \rightarrow$ M rejects $(x,|\varphi_n\rangle)$ with probability $\geq 2/3$.
- In the next slide, we will see another characterization of BQP/Qpoly.

BQP/Qpoly II

- Here is another characterization of BQP/Qpoly using quantum circuits.
- Recall the characteristic function χ_L of a language L.
- Theorem: [Nishimura-Yamakami (2004)]

L $\in$ BQP/Qpoly $\Leftrightarrow$ there exist a positive polynomial p, a non-uniform family $\{ C_n \}_{n \in N}$ of polynomial-size quantum circuits, and a series $\{ U_n \}_{n \in N}$ of unitary operators acting on p(n) qubits such that, for any length n and any input x of length n,

$$\mathrm{Prob}\left[C_n\left(x, U_n \left| 0^{p(n)} \right\rangle \right) = \chi_L(x) \right] \geq \frac{2}{3}$$

Generalization to BQP/Q(F)

- Similarly to BQP/F, we can generalize BQP/Qpoly to BQP/Q(F) by taking a different set F of functions.
- Let F be a set of functions from $N \rightarrow N$.
- A language L over alphabet Σ is in BQP/Q(F) $\Leftrightarrow$ there are a function $f \in F$, a family $\{ |\varphi_n\rangle \}_{n \in N}$ of quantum states, and a polynomial-time QTM M equipped with an advice tape such that, for all input $x \in \Sigma^n$,
  - $|\varphi_n\rangle$ is a quantum state of dimension $2^{f(n)}$,
  - $x \in L \rightarrow$ M accepts $(x, |\varphi_n\rangle)$ with probability $\geq 2/3$,
  - $x \notin L \rightarrow$ M rejects $(x, |\varphi_n\rangle)$ with probability $\geq 2/3$.
- For example, we can obtain BQP/Qlog and BQP/Q(1).

Properties of BQP/Q(f)

- Concerning quantum advice, Nishimura and Yamakami (2004) proved the following properties.

- Theorem:

1. BQP/Qlog $\subseteq$ BQP/poly
2. BQP/log $\neq$ BQP/Qlog $\neq$ BQP/poly
3. P/log^2 $\nsubseteq$ BQP/Qlog
4. EESPACE $\nsubseteq$ BQP/Qpoly

EESPACE consists of all languages recognized by DTMs using space $2^{2^{O(n)}}$

Open Problems

- Here is a short list of open problems associated with BQP/poly and BQP/Qpoly.
  1. Is BQP/poly = BQP/Qpoly?
  2. Is BQP $\subseteq$ EQP/Qpoly?
  3. Is PSPACE $\not\subseteq$ BQP/poly?

- In the above list, EQP/Qpoly denotes the non-uniform complexity class defined by EQP and polynomial-size quantum advice, similarly to BQP/Qpoly.

II. Reversible Automata with Advice

1. Classical Advice for Finite Automata
2. Advised Language Families
3. Reversible Finite Automata
4. Power of Advice
5. Characterization of 1RFA/n

Track Notation for Advice (revisited)

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

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

Each of them is treated as a new symbol.

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

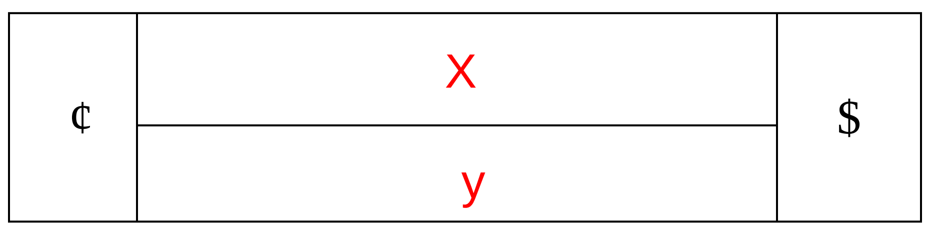
When written on an input tape:

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

Classical Advice for Finite Automata (revisited)

- Let Γ be any advice alphabet.
- Let t(n) be a length function.
- In the case of deterministic advice, an advice string is given for each length t(n).
- In the case of randomized advice, for each length n, all possible strings of length n are given according to an advice probability distribution D_n over $\Gamma^{t(n)}$.

x $\in \Sigma^n$ is an input and D_n generates an advice string y $\in \Gamma^{t(n)}$ with probability $D_n(y)$.



Advice string y is given in the lower track of the tape.

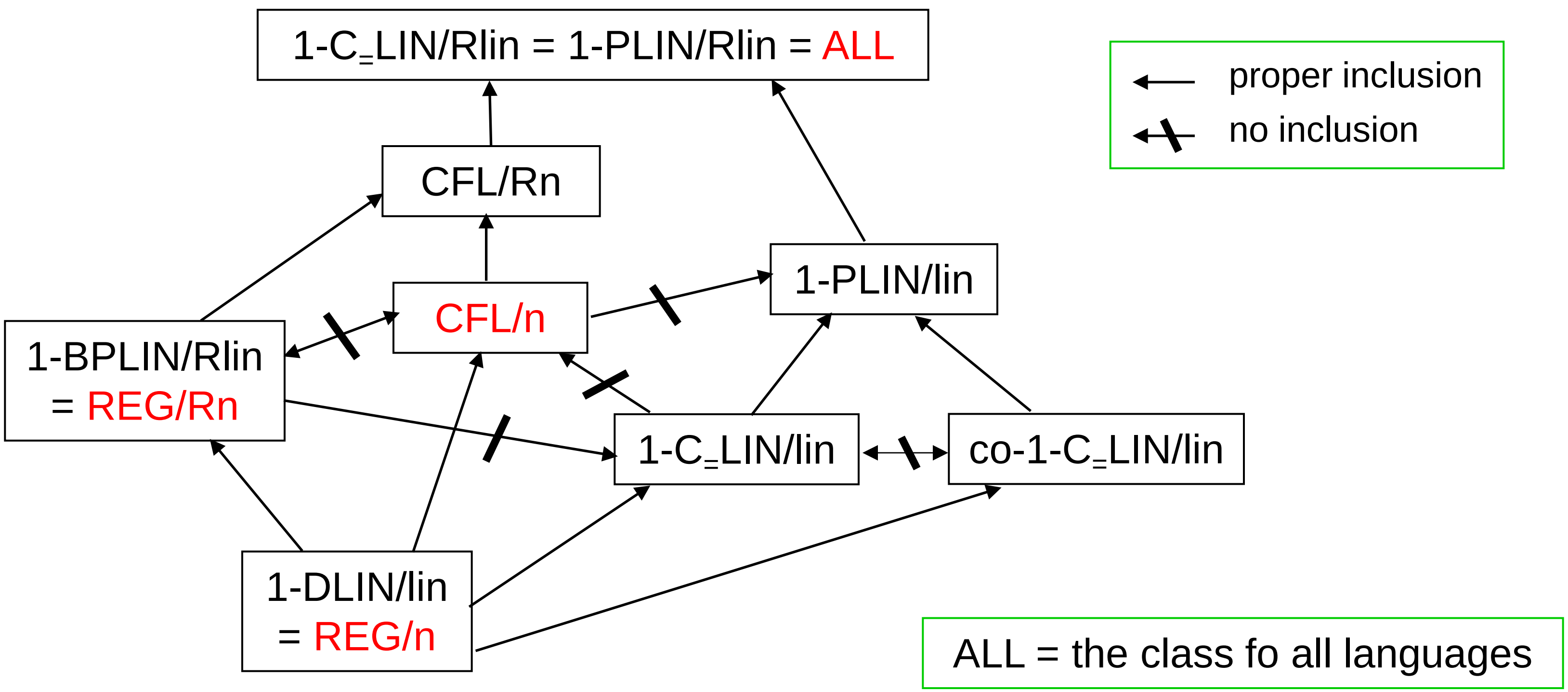
Advised Language Families (revisited)

- Let L be any language over an alphabet Σ.
- $L \in$ REG/n $\Leftrightarrow \exists M$:1dfa $\exists \Gamma$: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 $[x\ h(|x|)]^T$].
- $L \in$ CFL/n $\Leftrightarrow \exists M$:1npda $\exists \Gamma$: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 $[x\ h(|x|)]^T$].
- $L \in$ REG/Rn

  $\Leftrightarrow \exists M$:1dfa $\exists \varepsilon \in [0,½)\ \exists \Gamma\ \exists \{D_n\}_n$: advice prob. distribution
  1. $\forall n \in N$ [D_n generates advice strings $y \in \Gamma^n$].
  2. $\forall x \in \Sigma^n$ [$x \in L \rightarrow$ M accepts $[x\ D_n]^T$ with prob. $\geq 1-\varepsilon$].
  3. $\forall x \in \Sigma^n$ [$x \notin L \rightarrow$ M rejects $[x\ D_n]^T$ with prob. $\geq 1-\varepsilon$].

Inclusions and Separations (revisited)

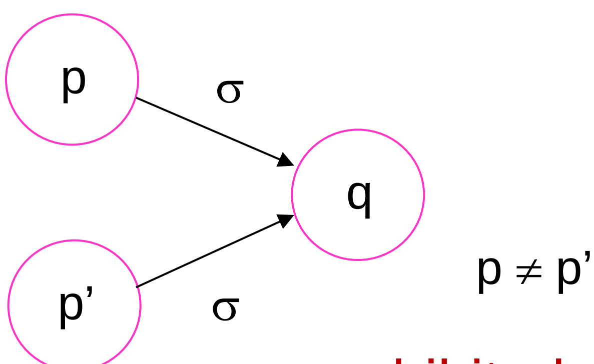
- The following figure shows known class separations among advised language families.



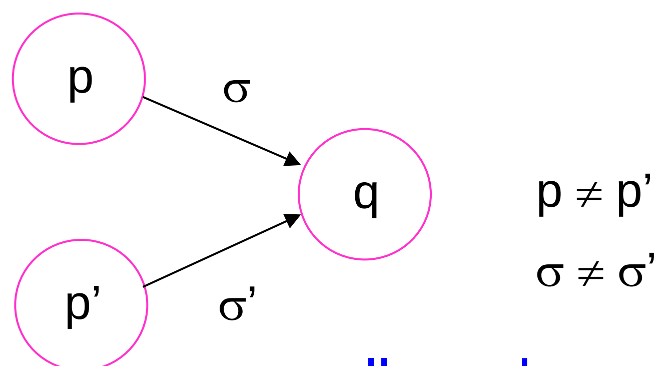
Reversible (Finite) Automata I

- A one-way deterministic reversible (finite) automaton (1rfa) $M = (Q,\Sigma,\{\text{¢},\$\},\delta,q_0,Q_{acc},Q_{rej})$ is a restricted version of a 1dfa, which satisfies the following reversibility condition.

- Reversibility condition: for every inner state $q \in Q$ and every symbol $\sigma \in \Sigma$, there exists at most one inner state $p \in Q$ s.t. $\delta(p,\sigma)=q$.



prohibited



allowed

Reversible (Finite) Automata II

- Reversible finite automata are considered as the error-free version of quantum finite automata.
- Because reversible finite automata are reversible and so are quantum finite automata.

1RFA/n and 1RFA/Rn

- Similarly to REG/n and REG/Rn, we define the following.

Computation with deterministic advice

- $L \in$ 1RFA/n $\Leftrightarrow$ $\exists$ M: 1rfa $\exists$ h: advice function s.t.
  1. $\forall n$ [$|h(n)| = n$] and
  2. $\forall x \in \Sigma^*$ [$M([x\ h(|x|)]^T) = \chi_L(x)$].

Computation with randomized advice

- $L \in$ 1RFA/Rn $\Leftrightarrow$ $\exists$ M: 1rfa $\exists\ \varepsilon \in [0,½)$ $\exists\ \Gamma$ $\exists \{D_n\}_n$:advice prob. dist. s.t.
  1. $\forall n \in N$ [every advice string $y \in \Gamma^n$ is generated with prob. $D_n(y)$].
  2. $\forall x \in \Sigma^n$ [$x \in L \rightarrow$ M accepts $[x\ D_n]^T$ with probability $\geq 1-\varepsilon$].
  3. $\forall x \in \Sigma^n$ [$x \notin L \rightarrow$ M rejects $[x\ D_n]^T$ with probability $\geq 1-\varepsilon$].

Power of Advice

- Consider the context-free language:

  $Pal_{\#} = \{ w\#w^R \mid w\in\{0,1\}^* \}$. (marked palindrome)

  - (Known) $Pal_{\#} \notin REG/n$.
  - (Claim) $Pal_{\#}$ is in 1RFA/Rn. [Yamakami (2014)]

- Consider the context-sensitive language:

  $Dup = \{ ww \mid w\in\{0,1\}^* \}$. (duplicated words)

  - (Known) $Dup \notin CFL/n$.
  - (Claim) Dup is in 1RFA/Rn. [Yamakami (2014)]

Proof of the First Claim

- Consider a language:

$$Pal_{\#} = \{ x\#x^R \mid x \in \{0,1\}^* \} \ (\in DCFL)$$

- Fact: $Pal_{\#} \notin REG/n$ [Yamakami08].
- We claim that $Pal_{\#} \in 1RFA/Rn$.

- Let our 1rfa be s.t.

Compute $x \bullet y$ and $z \bullet y^R$.
Accept $x\#z$ iff $x \bullet y \equiv_2 z \bullet y^R$.

- Let our randomized advice D_n be s.t.

$$D_n(w) = \begin{cases} 1/2^m & \text{if } n = 2m \text{ and } w = y\#y^R \\ 1 & \text{if } n = 2m+1 \text{ and } w = \#^n \\ 0 & \text{otherwise.} \end{cases}$$

if $\lvert x\rvert=\lvert z\rvert$	x	#	z
D_n	y	#	y^R

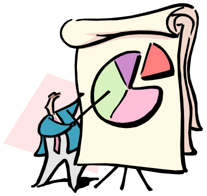
- We run this procedure twice independently to reduce the error probability to ¼.

Separation Results

- 1RFA/Rn is quite powerful, compared with REG/n.
- Lemma: [Yamakami (2014)]
  DCFL$\cap$1RFA/Rn $\not\subseteq$ REG/n.

- Yamakami (2014) further obtained the following class separations among the aforementioned advised language families.
  - 1RFA/Rn $\not\subseteq$ CFL/n
  - 1RFA/n $\neq$ 1RFA/Rn

Characterization of 1RFA/n



- Here is a machine-independent characterization of languages in 1RFA/n given by Yamakami (2014).
- Theorem: Let S be any language over Σ. The following two statements are logically equivalent.
  1. S is in 1RFA/n.
  2. There is an equivalence relation $\equiv_S$ over Δ s.t.
     - the set $\Delta/\equiv_S$ is finite, where $\Delta = \{ (x,n) \mid |x| \leq n \}$, and
     - for any length parameter n, any symbol $\sigma \in \Sigma$, and any two strings $x,y \in \Sigma^*$ with $|x| = |y| \leq n$, the following holds:
       - when $|x\sigma| \leq n$, $(x\sigma,n) \equiv_S (y\sigma,n)$ iff $(x,n) \equiv_S (y,n)$, and
       - if $(x,n) \equiv_S (y,n)$, then $S(xz) = S(yz)$ for all strings z with $|xz| = n$.
- This is an analogue of Myhill-Nerode theorem for REG.

Open Problems

- There is few literature, which covers reversible finite automata with advice.
- Answer the following general questions.

1. Find much simpler characterizations of languages in 1REF/n and 1RFA/Rn.
2. Explore natural properties of 1RFA/n and 1RFA/Rn.

III. Quantum Finite Automata with Advice

1. QFAs with Deterministic Advice
2. Inclusions and Separations
3. Power of Advice
4. Limitations of Advice

Language Families (revisited)

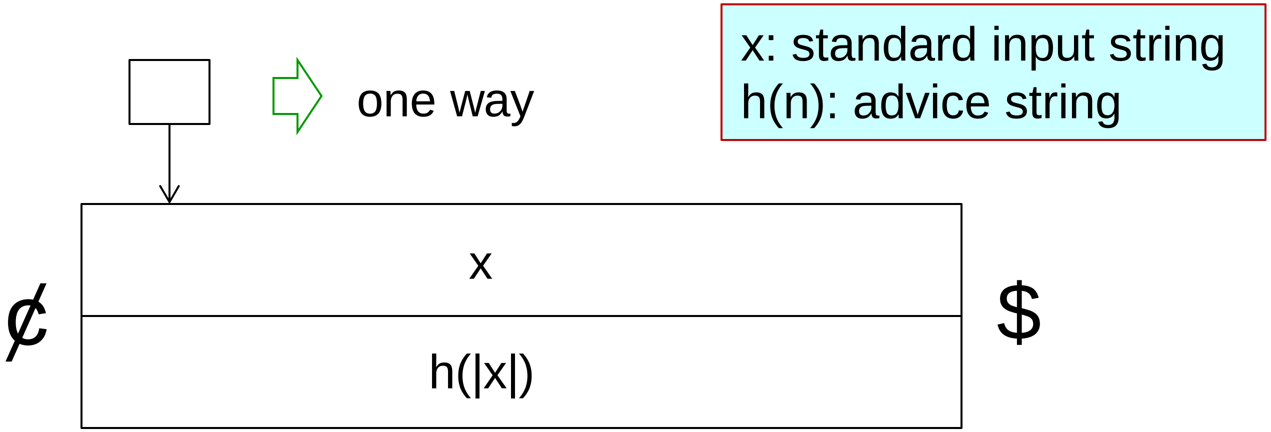
- Recall the following notation.
  - 1qfa = one-way quantum finite automaton
  - 1QFA = collection of all languages recognized by 1qfa's with bounded error (i.e., error bound < ½ - ε)

- (NOTE) In Week 12, the above 1QFA was written as 1BQFA .

- (Claim) 1RFA $\subseteq$ 1QFA $\subseteq$ REG [Kondacs-Watrous (1997)]

QFAs with Deterministic Advice I

- To run a 1-way quantum finite automaton (1qfa) with deterministic advice, we first provide an advice string to the lower track of an input tape.
  - $M = (Q,\Sigma,\{¢,\$\},\delta,q_0,Q_{acc},Q_{rej})$: 1qfa
  - Γ: advice alphabet
  - $h: N \rightarrow \Gamma^*$: advice function with $|h(n)| = n$



QFAs with Deterministic Advice II

- By adding deterministic advice to 1qfa's, we immediately obtain the advised complexity class 1QFA/n.
- Let L be any language over an alphabet Σ.
- $L \in$ 1QFA/n

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

  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 $\geq 1-\varepsilon$].

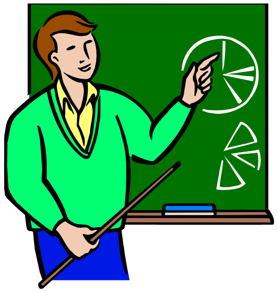
- Recall that reversible automata are considered as an error-free version of quantum automata. Thus, 1RFA/n $\subseteq$ 1QFA/n holds.

Relationships between 1RFA/n and 1QFA/n

- Yamakami (2014) proved the following statements.
- The non-advice relations 1RFA $\subseteq$ 1QFA $\subseteq$ REG can transfer to the advice case.
- Lemma: 1RFA/n $\subseteq$ 1QFA/n $\subseteq$ REG/n.

- There is a limitation of 1RFA/n.
- Proposition: 1QFA $\not\subseteq$ 1RFA/n.
- The above proposition immediately yields the following class separation.
- Corollary: 1QFA/n $\neq$ 1RFA/n.

Limitation of 1QFA/n



There is a limitation of 1QFA/n.

- Theorem: REG $\not\subseteq$ 1QFA/n. [Yamakami (2014)]
- Corollary: 1QFA/n $\neq$ REG/n. [Yamakami (2014)]

- This result extends Kodacs-Watrous (1997)'s result of 1QFA $\neq$ REG. However, we employ a totally different proof technique, because their argument does not work.

Why?

- Kondacs-Watrous (1997) used L_0 ={ x0 | x$\in${0,1}* }, which separates 1QFA from REG. But, L_0 is already in 1QFA/n and it is no use to separate REG from 1QFA/n.

Necessary Condition for 1QFA/n

- Here is a machine-independent condition that is necessary for a language to be in 1QFA/n given by Yamakami (2014).

- Theorem: If S is in 1QFA/n, then the following condition holds:

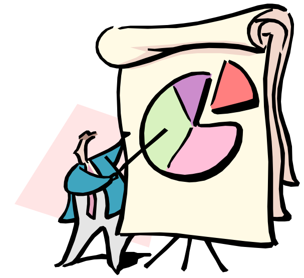
  There are two constants c,d > 0, an equivalence relation $\equiv_S$ over Δ, a partial order $\leq_S$ over Δ, and a closeness relation $\approx$ over Δ that satisfy the following. Let $(x,n),(y,n) \in \Delta$, $z \in \Sigma^*$, and $\sigma \in \Sigma$ with $|x| = |y|$, where $\Delta = \{ (x,n) \mid |x| \leq n \}$. Define $(x,n) =_S (y,m) \Leftrightarrow (x,n) \leq_S (y,m)$ and $(x,n) \leq_S (y,m)$.

  1. The set $\Delta/\equiv_S$ is finite.
  2. If $(x,n) \approx (y,n)$, then $(x,n) \equiv_S (y,n)$.
  3. If $|x\sigma| \leq n$, then $(x\sigma,n) \leq_S (x,n)$.
  4. If $|xz| \leq n$, $(x,n) =_S (xz,n)$, $(y,n) =_S (yz,n)$, and $(xz,n) \approx (yz,n)$, then $(x,n) \equiv_S (y,n)$.
  5. If $(x,n) \equiv_S (y,n)$ iff $S(xz) = S(yz)$ for all z with $|xz| = n$.
  6. Any strictly descending chain (w.r.t. $\leq_S$) in Δ has length $\leq$ c.
  7. Any $\approx$-discrepancy subset of Δ has cardinality $\leq$ d.

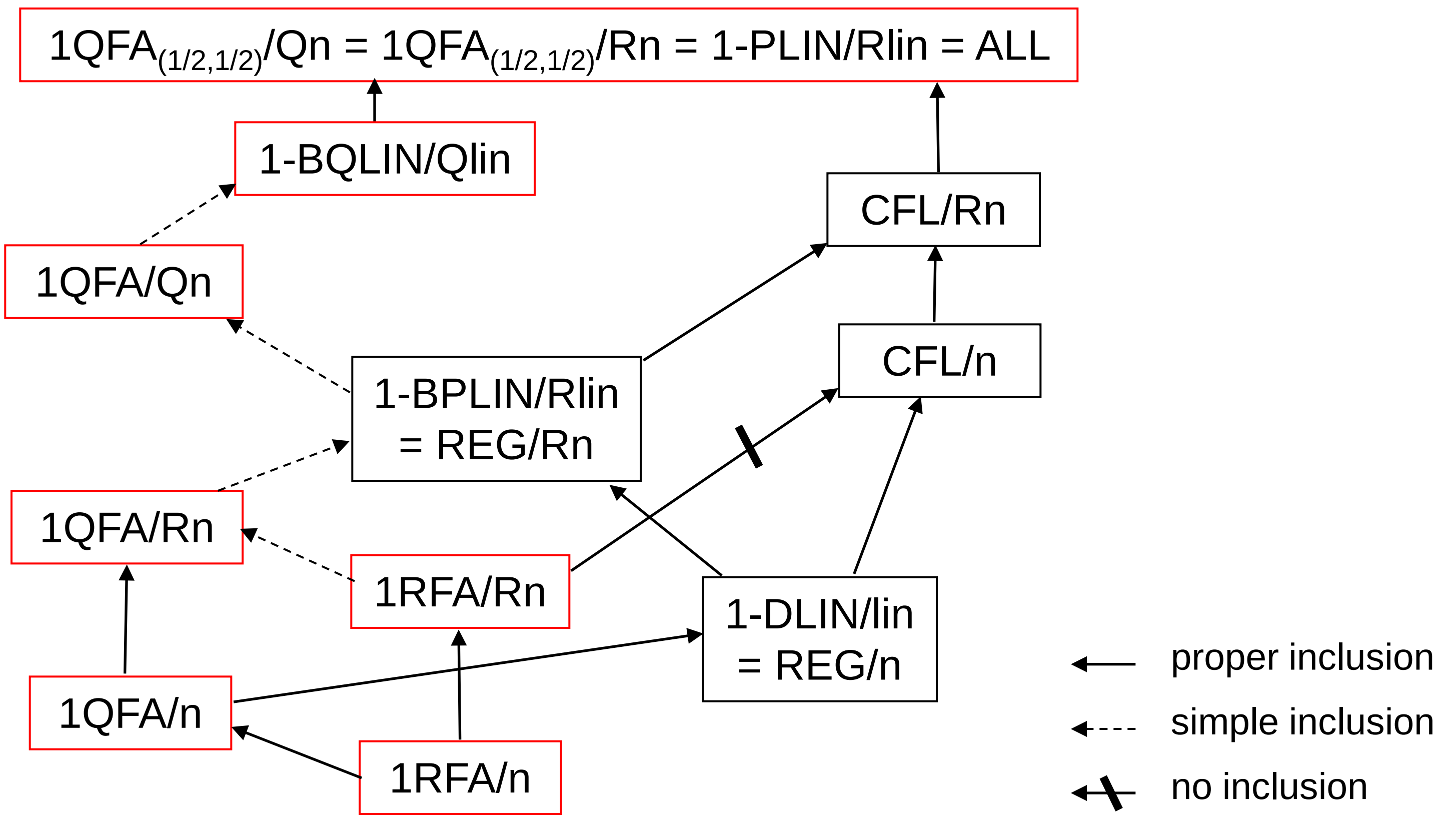
Separation Results

- Yamakami (2014) presented the following separation results.
  - 1QFA $\not\subseteq$ 1RFA/n.
  - 1RFA/n $\neq$ 1QFA/n.
  - REG $\not\subseteq$ 1QFA/n.
  - 1QFA/n $\neq$ REG/n.

A Quick Overview



- Here is a quick overview of inclusions and separations.



Power of 1QFA/Rn

- We exhibit another example of the power of randomized advice.

- Proposition: [Yamakami (2014)]
  $1QFA_{(1/2,1/2)}$/Rn = ALL.

- In other words, the advised language family $1QFA_{(1/2,1/2)}$/Rn consists of all languages.

- In the next slide, we will give a quick explanation.

Why $1QFA_{(1/2,1/2)}/Rn = ALL$?

- Proof Sketch

- Let L be any language over Σ. For simplicity, assume $L \cap \Sigma^n \neq \Sigma^n$. Let our randomized advice D_n be

$$D_n(y) = 1/|\Sigma^n - L| \text{ if } y \in \Sigma^n - L; \quad D_n(y) = 0 \text{ if } y \in L \cap \Sigma^n.$$

Input string	x
D_n generates	y

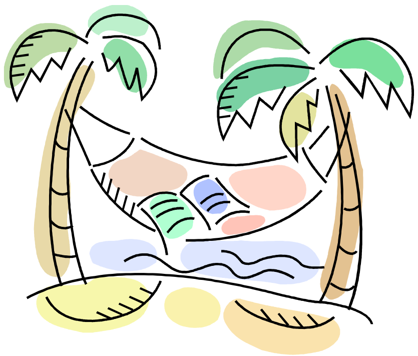
- Let our 1qfa M be s.t.

$$\begin{cases} \text{if } x = y, \text{ then reject } x; \\ \text{if } x \neq y, \text{ then accept/reject with equal probability } ½. \end{cases}$$

- It is easy to check that $x \in L \leftrightarrow \text{Prob}[\, M([x\ D_n]^T) = 1\,] = 1/2$.
- Hence, $L \in 1QFA_{(1/2,1/2)}/Rn$.

QED

1QFA/Rn vs. REG/n



- Proposition: [Yamakami (2014)]
  1QFA/Rn $\subseteq$ REG/Rn.

- NOTE: This inclusion is not immediate from 1QFA $\subseteq$ REG [KW97], because "advice" does not automatically commute the inclusion relationship between two language families.

❑ Proof Idea: This is done by a direct simulation of a 1qfa on a 1qfa together with a careful treatment of a given advice probability ensemble.

QED

Power of 1QFA/Rn

- Randomized advice may give more power than deterministic advice does.
- Recall that DCFL$\cap$1RFA/Rn $\not\subseteq$ REG/n.
- Moreover, we can show the following.

- Proposition: [Yamakami (2014)]
  1QFA/n $\neq$ 1QFA/Rn.

❑ Proof Sketch

- Assume that 1QFA/n = 1QFA/Rn.
- From the above claim, it follows that 1RFA/Rn $\not\subseteq$ REG/n.
- Since 1RFA/Rn $\subseteq$ 1QFA/Rn, we obtain 1QFA/Rn $\not\subseteq$ REG/n, and thus 1QFA/n $\not\subseteq$ REG/n.
- This contradicts the fact that 1QFA/n $\subseteq$ REG/n.

QED

Open Problems

- In quantum automata theory, there are still a lot of interesting open problems to solve.

- Give a complete characterization of 1QFA/n.
- Prove or disprove each of the following statements.
  1. 1QFA/Rn $\neq$ REG/Rn
  2. 1RFA/Rn $\neq$ 1QFA/Rn

IV. Quantum Advice for QFAs

1. How to Define Quantum Advice
2. Read-Only Advice Tracks
3. Rewritable Advice Tracks
4. Advised Language Families
5. Power of 1QFA/Qn
6. Limitation of 1QFA/Qn

How to Define Quantum Advice

- We extend random advice to quantum advice by replacing probability distributions with quantum states.

- Advice alphabet Γ
- H_{Γ^n} = Hilbert space spanned by $\{ |s\rangle \mid s \in \Gamma^n \}$
- A quantum advice state $|\phi_n\rangle$ = a unit vector in H_{Γ^n}
- That is,

$$|\phi_n\rangle = \sum_{s \in \Gamma^n} \alpha_s |s\rangle$$

where $\alpha \in C$ and

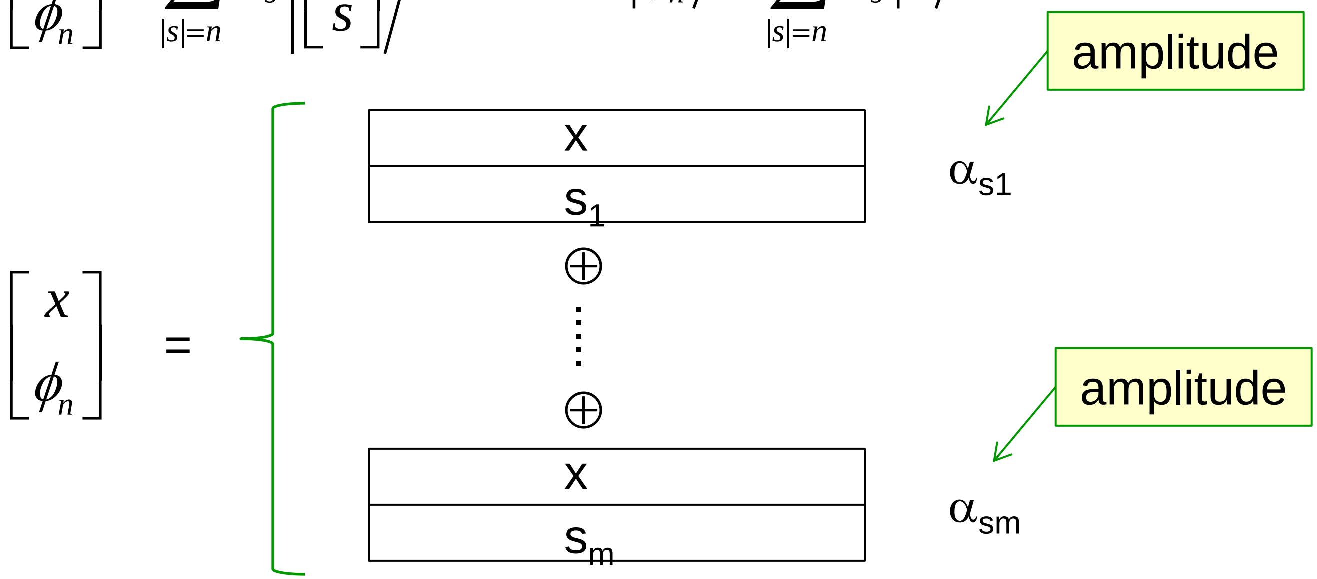
$$\sum_{s \in \Gamma^n} |\alpha|^2 = 1$$

Illustration: Quantum Advice

- A quantum advice state $|\phi_n\rangle = \sum_{s \in \Gamma^n} \alpha_s |s\rangle$ is given to the lower track of an input tape in parallel to a standard input string $x \in \Sigma^n$.

superposition of the content of an input tape

$$\begin{bmatrix} x \\ \phi_n \end{bmatrix} = \sum_{|s|=n} \alpha_s \left| \begin{bmatrix} x \\ s \end{bmatrix} \right\rangle, \quad \text{where} \quad |\phi_n\rangle = \sum_{|s|=n} \alpha_s |s\rangle$$



A Possible Candidate of 1QFA/Qn

- In analogy to 1QFA/n, we may possibly define 1QFA/Qn in the following way.

- 1QFA/Qn may consist of all languages L for which
  - $\exists$ M: 1qfa with read-only input tape $\exists\ \Gamma$: advice alphabet $\exists\ \varepsilon \in [0,1/2)$ $\exists\ \{\, |\phi_n\rangle \,\}_n$: quantum advice states s.t. $\forall n \in N\ \forall\ x \in \Sigma^n$ $\mathrm{Prob}[M([x\ \phi_n]^T) = A(x)] \geq 1-\varepsilon$.

Weakness of Read-Only Advice Tracks

- Unfortunately, the previous definition does not provide any extra power to the underlying 1qfa's.
- Lemma: [Yamakami (2014)]

Let A be any language over Σ. The following two statements are equivalent.

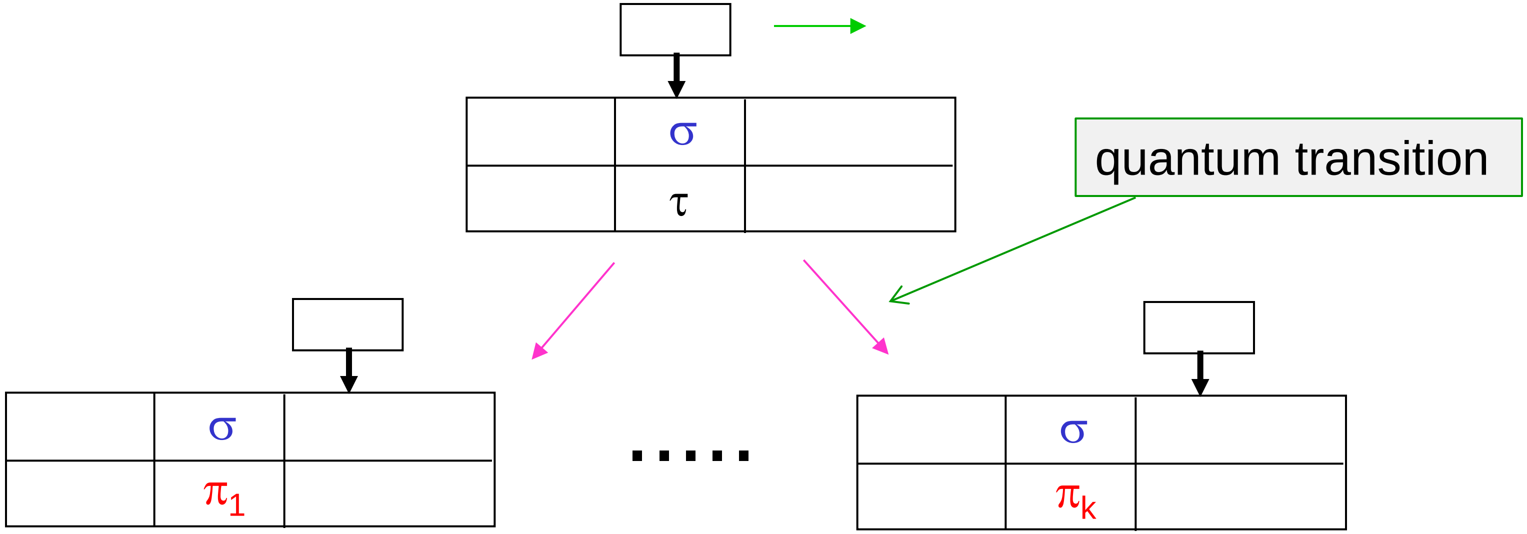
1. $A \in$ 1QFA/Rn.
2. $\exists$ M: 1qfa with read-only input tape $\exists\ \Gamma$: advice alphabet $\exists\ \varepsilon \in [0,1/2)$ $\exists\ \{ |\phi_n\rangle \}_n$: quantum advice states s.t.

$$\forall n \in N\ \forall\ x \in \Sigma^n\ \ \mathrm{Prob}[M([x\ \phi_n]^T) = A(x)] \geq 1-\varepsilon.$$

- In other words, quantum advice is reduced to random advice as far as we use read-only advice tracks.

Rewritable Advice Tracks

- To make use of quantum advice, we need a certain modification of 1qfa's.
- We allow a 1qfa to alter the content of an advice track.
- However, a tape head cannot move back or stay still.
- Moreover, input strings must be unchanged.



- "Rewritable track" is used as a "garbage tape," into which unwanted information can be dumped

Advised Class 1QFA/Qn

- A rewritable 1qfa means a 1qfa eqipped with a rewritable advice track.
- We formally define 1QFA/Qn as the collection of all languages recognized by rewritable 1qfa's with bounded error probability.
- NOTE: In a 1dfa case, rewritable tracks do not increase the computational power of 1dfa's, because it is known that

1-DLIN/lin = REG/n [Tadaki-Yamakami-Lin (2004)].

1-DLIN/lin: 2-way 1DTMs with rewritable tapes

REG/n: 1-way dfa's with read-only tapes

Power of 1QFA/Qn

- Surprisingly, the rewritability of the lower tracks of input tapes increases the computational power of 1qfa's.

- Proposition: [Yamakami (2014)]
  REG/Rn $\subseteq$ 1QFA/Qn $\subseteq$ 1-BQLIN/Qlin.

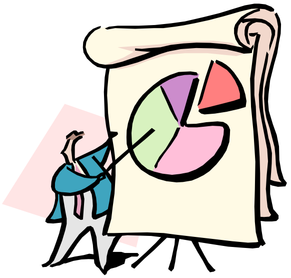
- For comparison, recall that 1QFA $\subsetneq$ REG [Kndacs-Watrous (1997)].

Closure Properties of 1QFA/Qn

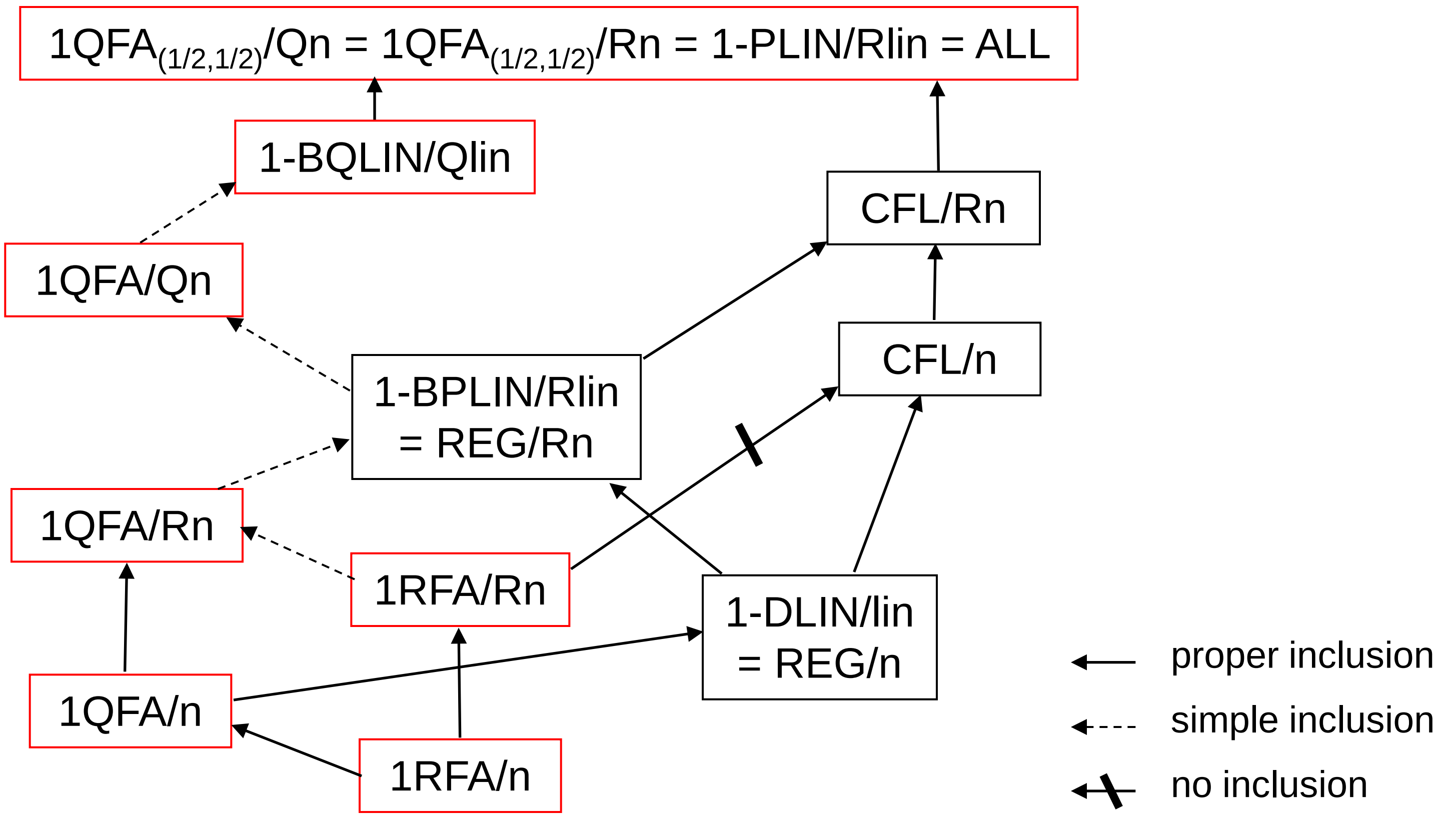
- We consider closure properties of 1QFA and 1QFA/Qn.
- (Claim) 1QFA is not closed under union or intersection. [Ambainis-Ķikusts-Valdats (2001)]
- By contrast, 1QFA/Qn enjoys the following closure properties.
- Proposition: [Yamakami (2014)]

  1QFA/Qn is closed under Boolean operations (i.e., complementation, union, and intersection).
- NOTE: Such closure properties (except for complementation) are not known for 1QFA.

A Quick Review (again)



- Here is a quick review of inclusions and separations that we have already discussed.



Open Problems

- In quantum automata theory, there are still many interesting open problems to solve.

- Prove or disprove each of the following statements.
  1. 1QFA/Qn $\neq$ REG/Rn
  2. 1QFA/Qn $\nsubseteq$ 1-PLIN/lin
  3. CFL/n $\nsubseteq$ 1QFA/Qn

V. Quantum State Complexity

1. Conservative State Complexity
2. Intrinsic State Complexity
3. Quantum State Complexity
4. Definitions of 1QSC/2QSC
5. Basic Properties
6. Union/Intersection
7. State Complexity vs. Advice
8. State Complexity vs. Approximate Rank

Conservative State Complexity

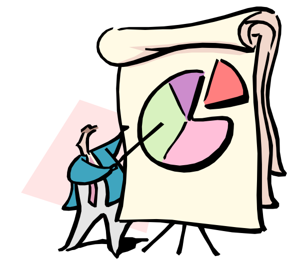
- Conservative (or traditional) state complexity concerns
  - the minimum number of inner states of M working on all inputs $x \in \Sigma^*$
- Such conservative state complexity of quantum finite automata has been studied for many years.
- Ambanis and Freivalds (1998)
  - studied $L_p = \{1^n : n|p\}$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

Intrinsic State Complexity

- 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 $x \in \Sigma^{\leq n}$)

- Such intrinsic state complexity of quantum finite automata has been studied by:
- Ambainis, Nayak, Ta-Shma, and 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



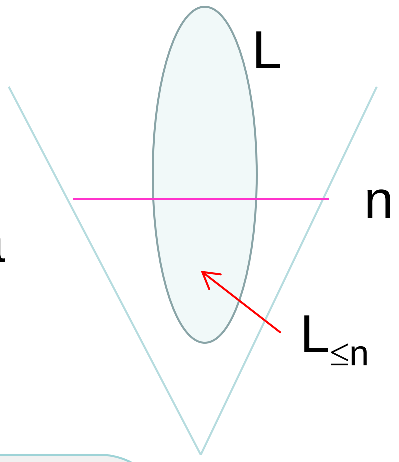
- We define quantum state complexity QSC
  - $M = (Q,\Sigma,\delta,q_0,Q_{acc},Q_{rej})$: either 1qfa or 2qfa
  - L : a language over Σ, $n \in N$, $L_n = L \cap \Sigma^n$
  - $\varepsilon : N \to [0,1/2)$ error bound, K : amplitude set $\subseteq C$

- State complexity of M: sc(M) = |Q| (the # of inner states)

- 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.

Quantum State Complexity II



- 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, $n \in N$,
  - $L_{\le n} = L \cap \Sigma^{\le n}$

- M recognizes L up to n with error ε using K $\Leftrightarrow$

  1. M has K-amplitudes
  2. $\forall x \in L_{\le n}$ [M accepts x with prob. $\ge 1-\varepsilon(n)$]
  3. $\forall x \in \Sigma^{\le n} - L_{\le n}$ [M rejects x with prob. $\ge 1-\varepsilon(n)$]

- No requirement is imposed on the outside of $\Sigma^{\le n}$.

Definitions of 1QSC/2QSC

- Villagra and Yamakami (2015) introduced two state complexity measure functions: $1QSC_{K,\varepsilon}[L]()$ 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 $\}$

- Lemma: [Villagra-Yamakami (2015)]

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

State Complexity of 2BQFA

- To emphasize the "bounded error" property, we write 1BQFA and 2BQFA for 1QFA and 2QFA, respectively.
- The following properties hold for alphabet Σ with $|\Sigma|\geq 2$.
- Lemma: [Villagra-Yamakami (2015)]

  $\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 Sketch

- 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, $2QSC_{C,\varepsilon}[L](\leq n) = O(1)$.

QED

Basic Properties

- The following properties hold for alphabet Σ with $|\Sigma| \geq 2$.
- Lemma: [Villagra-Yamakami (2015)]
  1. $1 \leq 2QSC_{K,\varepsilon}[L](n) \leq |\Sigma|^n + 1$
  2. $2QSC_{K,\varepsilon}[L^c](n) = 2QSC_{K,\varepsilon}[L](n)$, where $L^c = \Sigma^* - L$.
  3. $2QSC_{C,\varepsilon}[L](n) \leq 2QSC_{R,\varepsilon}[L](n) \leq 2 \times 2QSC_{C,\varepsilon}[L](n)$
- There is an exponential gap between $1QSC_{C,\varepsilon}[L](\leq n)$ and $1QSC_{C,\varepsilon}[L](n)$.
- Lemma: [Villagra-Yamakami (2015)]

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

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

Union/Intersection (1QFAs)

- Recall that 1BQFA is not closed under union or intersection.

- Proposition: [Villagra-Yamakami (2015)]

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

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

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

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

❑ Proof Sketch

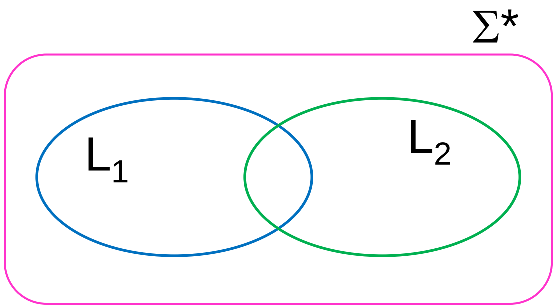
- By a direct simulation of minimal 1qfa's M_1 and M_2 for L_1 and L_2, respectively.

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 $L_1, L_2 \in 2BQFA_C$,

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

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



- Proposition: [Villagra-Yamakami (2015)]
  $\forall L_1, L_2 \in 2BQFA_A$ over Σ ($|\Sigma| \geq 2$)

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

1BQFA/n and 2BQFA/n (revisited)

- Recall the advised classes 1BQFA/n and 2BQFA/n.
- 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. $\forall x \in \Sigma^n$ [$x \in L \rightarrow$ M accepts $[x\ h(|x|)]^T$ with prob. $\geq 1-\varepsilon$].
  3. $\forall x \in \Sigma^n$ [$x \notin L \rightarrow$ M rejects $[x\ h(|x|)]^T$ 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. $\forall x \in \Sigma^n$ [$x \in L \rightarrow$ M accepts $[x\ h(|x|)]^T$ with prob. $\geq 1-\varepsilon$].
  3. $\forall x \in \Sigma^n$ [$x \notin L \rightarrow$ M rejects $[x\ h(|x|)]^T$ with prob. $\geq 1-\varepsilon$].

State Complexity vs. Advice

- Proposition: [Villagra-Yamakami (2015)]
  $\forall L \in$ 2BQFA/n over Σ ($|\Sigma| \geq 2$) $\exists \varepsilon \in [0,1/2)$
  s.t. $2QSC_{C,\varepsilon}[L](n) = O(n)$

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

- This result can be compared to:
- (Claim) $\forall L \in$ 2BQFA over Σ ($|\Sigma| \geq 2$) $\exists \varepsilon \in [0,1/2)$
  s.t. $2QSC_{C,\varepsilon}[L](n) = O(1)$

Approximate Matrix Rank

- $L \subseteq \Sigma^*$: a language over alphabet Σ
- M_L: characteristic matrix for L $\Leftrightarrow$

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

- $M_L(n)$: a restriction of M_L on strings (x,y) with $|xy| \leq n$
- Fix a quantum algorithm A.
- $P_n = (p_{xy})_{x,y}$ with $|xy| \leq n$: a matrix

  s.t. p_{xy} = acceptance probability of A on input xy

- (Claim)

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

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

State Complexity vs. Approximate Rank

- The following statements hold.
- Theorem: [Villagra-Yamakami (2015)]

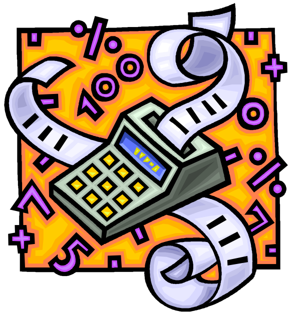
  $\forall$t: function on N $\forall$L $\forall\varepsilon,\varepsilon'$ ($0<\varepsilon'<\varepsilon<1/2$),

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

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

- Corollary: [Villagra-Yamakami (2015)]

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



Open Problems

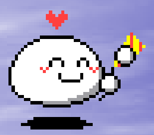
- In elementary automata theory, there are still a lot of interesting open problems to solve.

- Prove or disprove each of the following statements.

1. For any two languages $L_1,L_2 \in 2BQFA_C$,

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

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



Thank you for listening

Q & A

I’m happy to take your question!

END