NCMA 2017

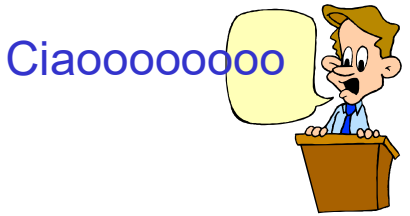
A Recursive Definition of Quantum Polynomial Time Computability

August 17, 2017. 17:15-17:45. Prague, Czech Republic

Dr. Tomoyuki Yamakami

University of Fukui, Fukui, JAPAN

Synopsis of Today's Talk



- This seminal talk is all about:
  - Quantum computability
- I will propose
  - A new recursive way to define polynomial-time quantum functions
- I will show
  - A new characterization of BQP and FBQP

✓ homepage ↪ http://TomoyukiYamakami.ORG
✓ twitter ↪ tomoyamakami

I. Recursive Functions

1. Recursive Functions
2. Kleene's Recursive Definition

Recursive Functions

- A family of recursive functions has been developed.
- This notion is characterized in several different ways.
  - Turing machine model
  - λ-calculus model
  - e.t.c.
- Different models give different ways to look into the same concepts.
- Each model may have its own advantage (and also disadvantage) of using it.

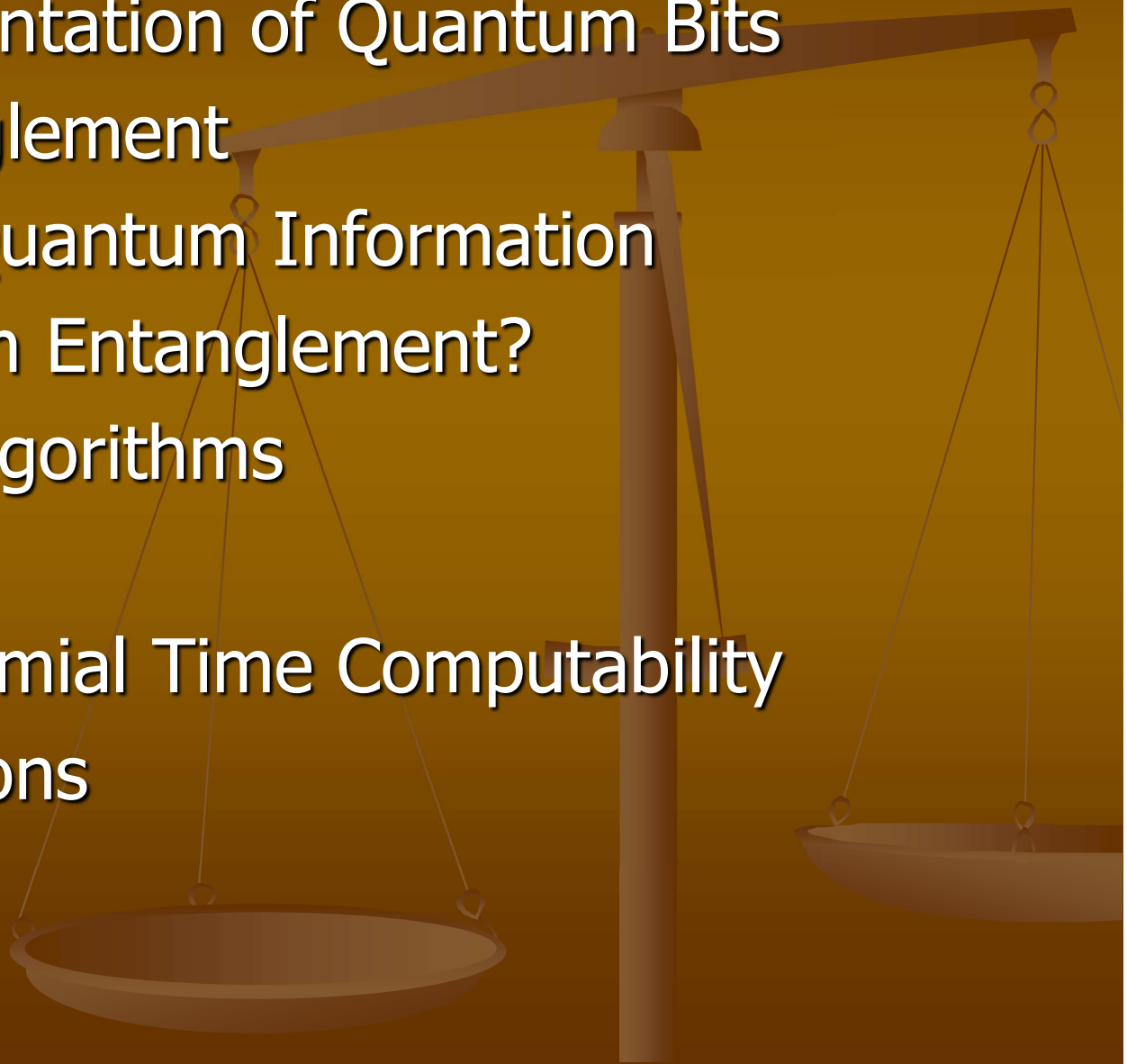
Kleene's Recursive Definition

- The family of recursive functions is defined from a small set of "basic" functions and several "basic" rules of how to construct a new function from the existing ones.

- Initial functions
- Construction Rules

II. Basics of Quantum Information

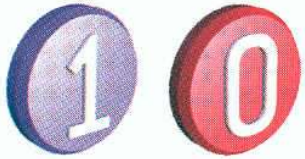
1. Physical Representation of Quantum Bits
2. Quantum Entanglement
3. How to Obtain Quantum Information
4. What is Quantum Entanglement?
5. Fast Quantum Algorithms
6. QTMs
7. Quantum Polynomial Time Computability
8. Quantum Functions



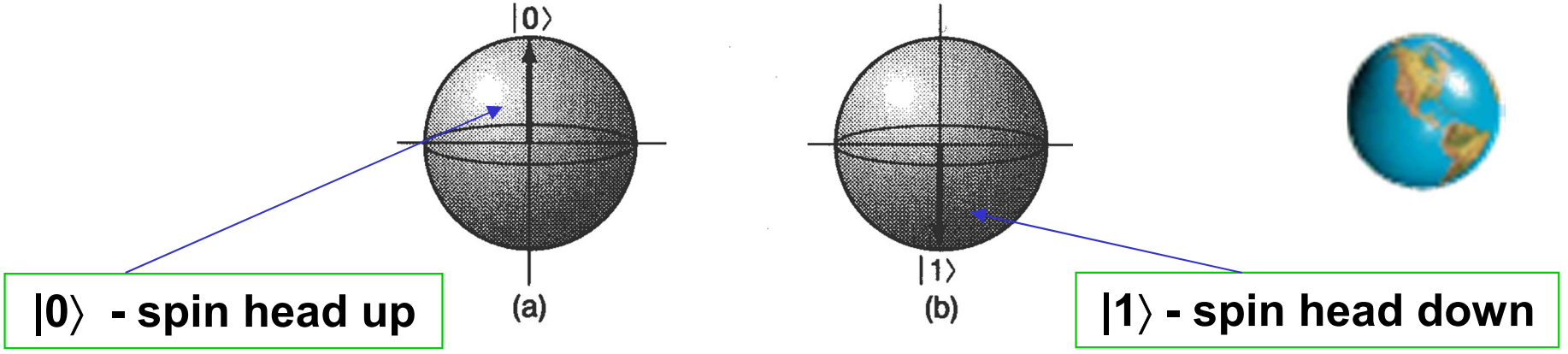
What is a Qubit?

Unit of Quantum Information

- The elementary unit of classical information is bit.



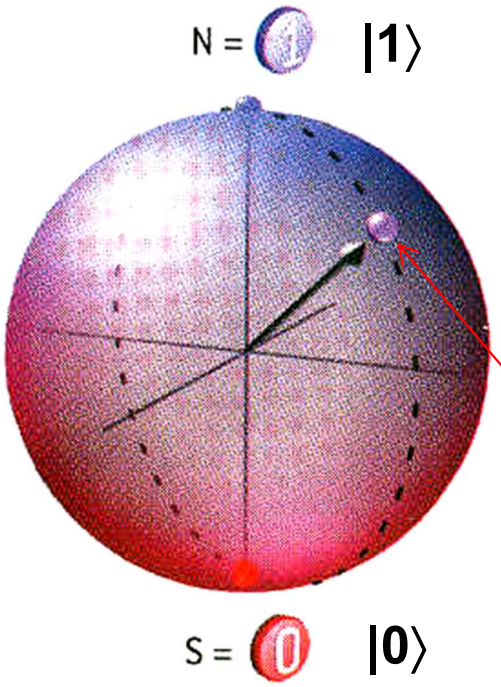
- Quantum information theory uses quantum bit (qubit).
- Dirac's notation is used to describe those "qubits."
  - ❖Conventionally, we write $|0\rangle$ for bit 0 and $|1\rangle$ for bit 1.



Physical Representation of Quantum Bits

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

$|0\rangle$ represents classical bit 0
$|1\rangle$ represents classical bit 1

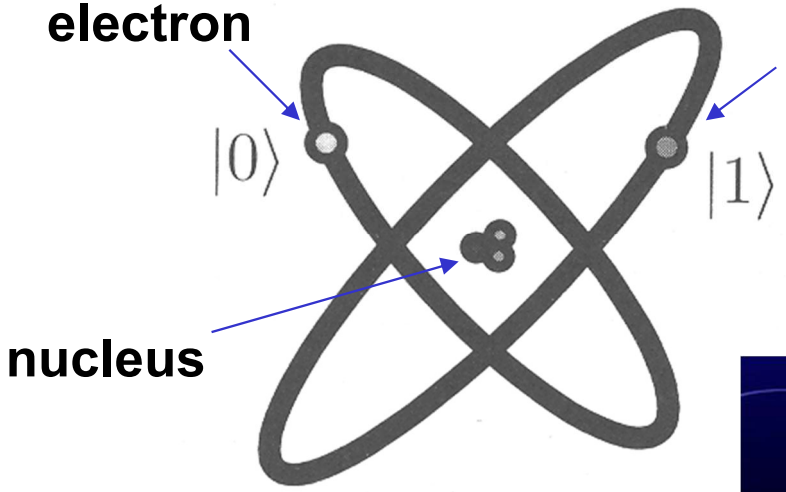


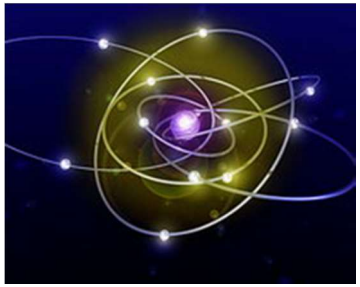
$|1\rangle$

$|0\rangle$

$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

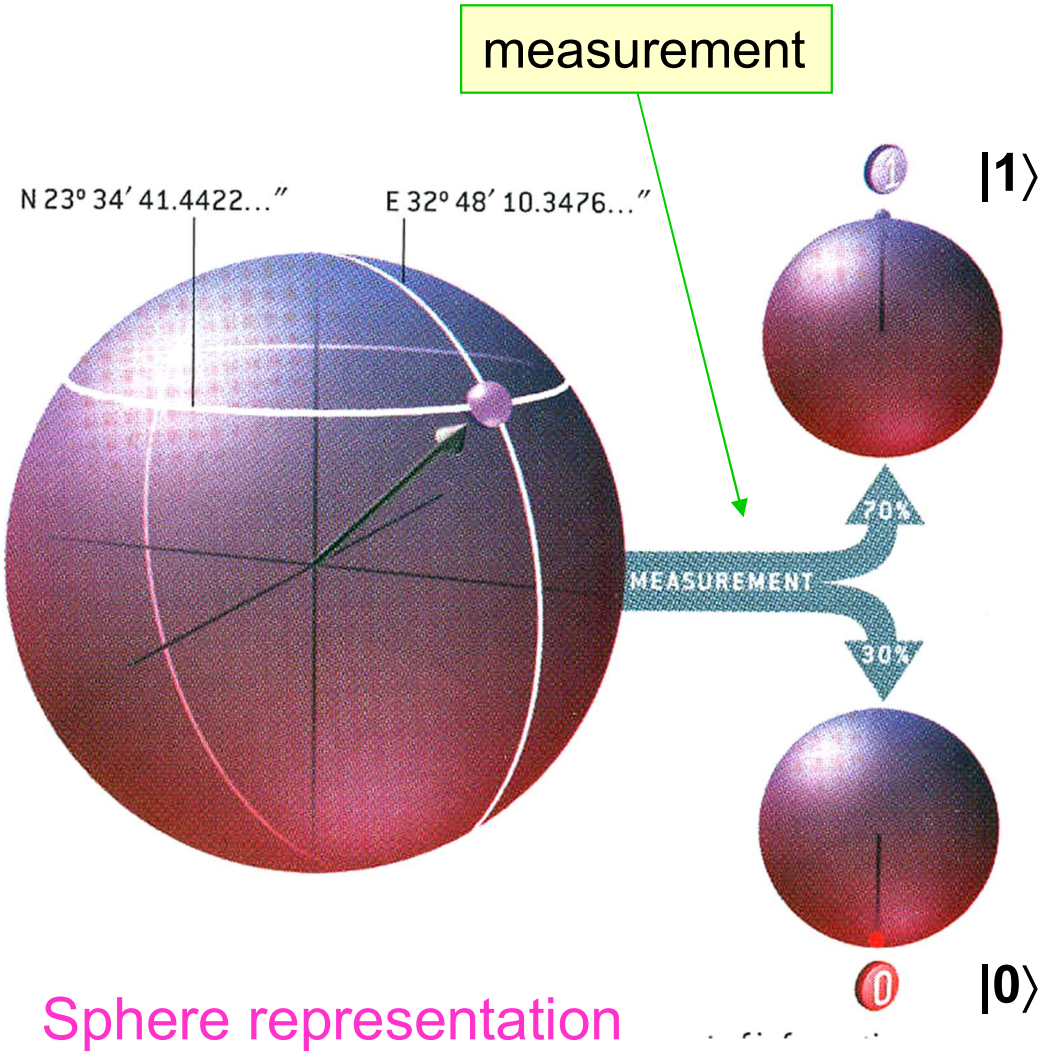
Two electronic levels in an atom





A qubit is a linear combination of $|0\rangle$ and $|1\rangle$.

How to Obtain Quantum Information



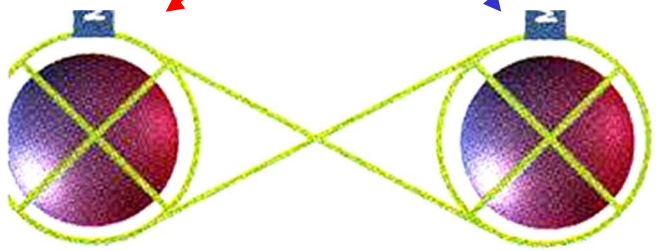
Sphere representation

- The measurement is the way to find out what is going on inside the quantum system.
- When a qubit is measured (or observed), quantum mechanics dictates the result must turn into a classical bit.

What is Quantum Entanglement?

An EPR pair $|\psi\rangle$

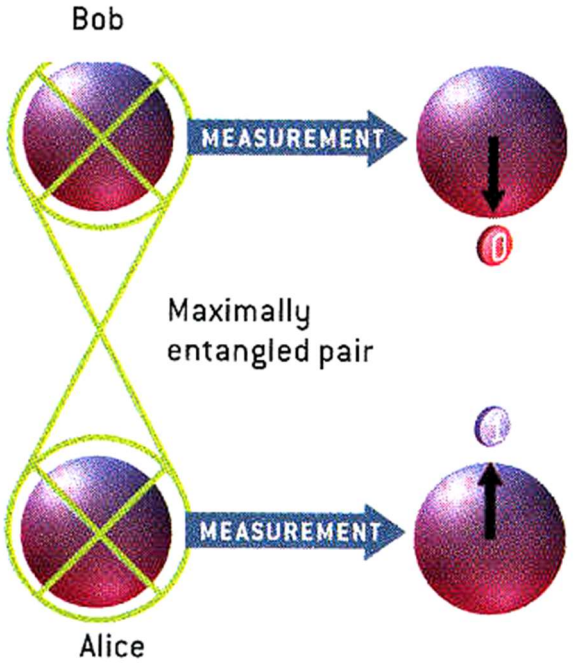
$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$$



Bob's qubit

Alice's qubit

If Bob measures $|\psi\rangle$ and obtain $|0\rangle$, then Alice must obtain $|1\rangle$ after measurement.



If Bob measures $|\psi\rangle$ and obtain $|1\rangle$, then Alice must obtain $|0\rangle$ after measurement.

Fast Quantum Algorithms

- There are several well-known fast quantum algorithms, which perform (presumably) better than classical algorithms.

- Integer factorization
  - Shor (1997, SIAM J. Comput.)
- Database search
  - Grover (1996, STOC)

Quantum Turing Machines

- Deutsch (1985) considered a quantum analogue of Turing machine.
- Berstein-Vazirani (1997) developed a theory of quantum Turing machine.
- Yamakami (1999) and Ozawa-Nishimura (2000) considered multiple-tape QTMs.

What is a Quantum Turing Machine?

- A quantum Turing machine (QTM) is similar to a TM with k input/work tapes but with a quantum transition function.

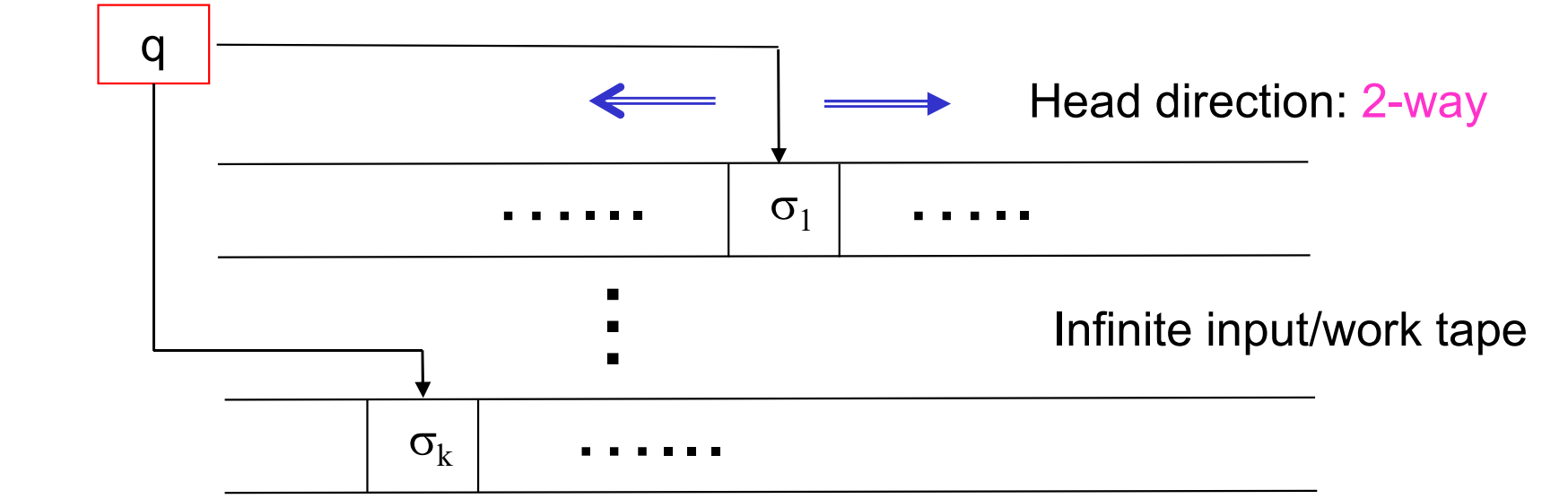
$M = (Q, \Sigma, \Gamma_1, \ldots, \Gamma_k, \delta, q_0, Q_{acc}, Q_{rej})$

Σ = input alphabet

Γi = i-th tape alphabet

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

δ : a quantum transition function

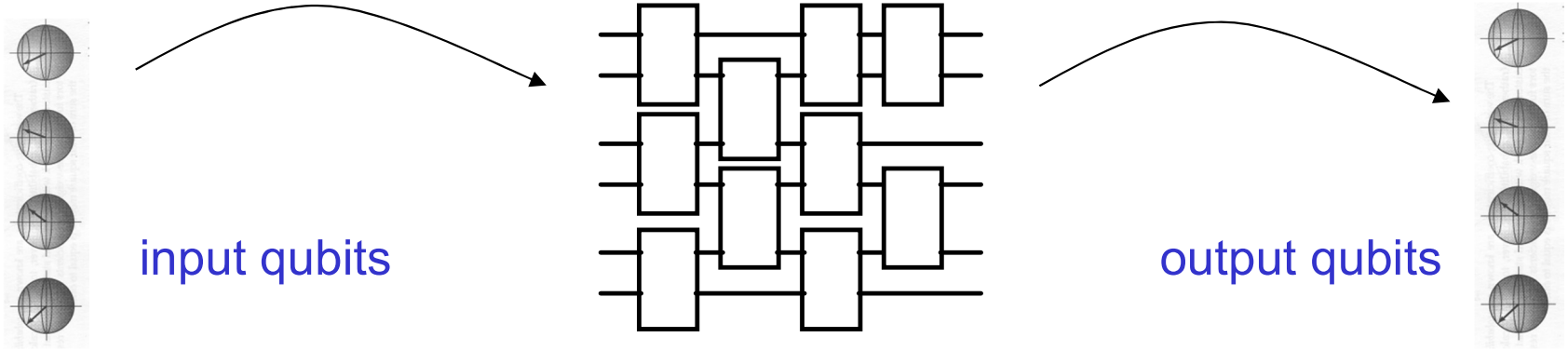


Quantum Circuits

- Deutsch (1999) considered a quantum analogue of Boolean circuits, called quantum network.
- Yao (1993) introduced a quantum analogue of Boolean circuits, called quantum circuits.

What is a Quantum Circuit?

- To manipulate quantum information, we use unitary operations, which are realized by quantum circuits made of a finite set of “simple” quantum gates.
- In particular, we use quantum circuits whose circuitry can be “efficiently” designed in a reasonable amount of time (say, polynomial time).
- Such a quantum circuit transforms qubits as follows:



A quantum circuit

Quantum Polynomial-Time Computability

- BQP is the collection of languages accepted quantumly in polynomial time with bounded error probability.
- Theorem:

  The following are equivalent.

  1) $L \in BQP$
  2) There is a polynomial-time, well-formed QTM M that recognizes L with bounded-error probability.
  3) There is a P-uniform family $\{C_n\}_{n \in N}$ of quantum circuits, each C_n recognizes $L \cap \Sigma^n$.
- This gives two different ways to define the same complexity class BQP.
- Can we get rid of the requirements of "well-formedness" and "uniformity"?

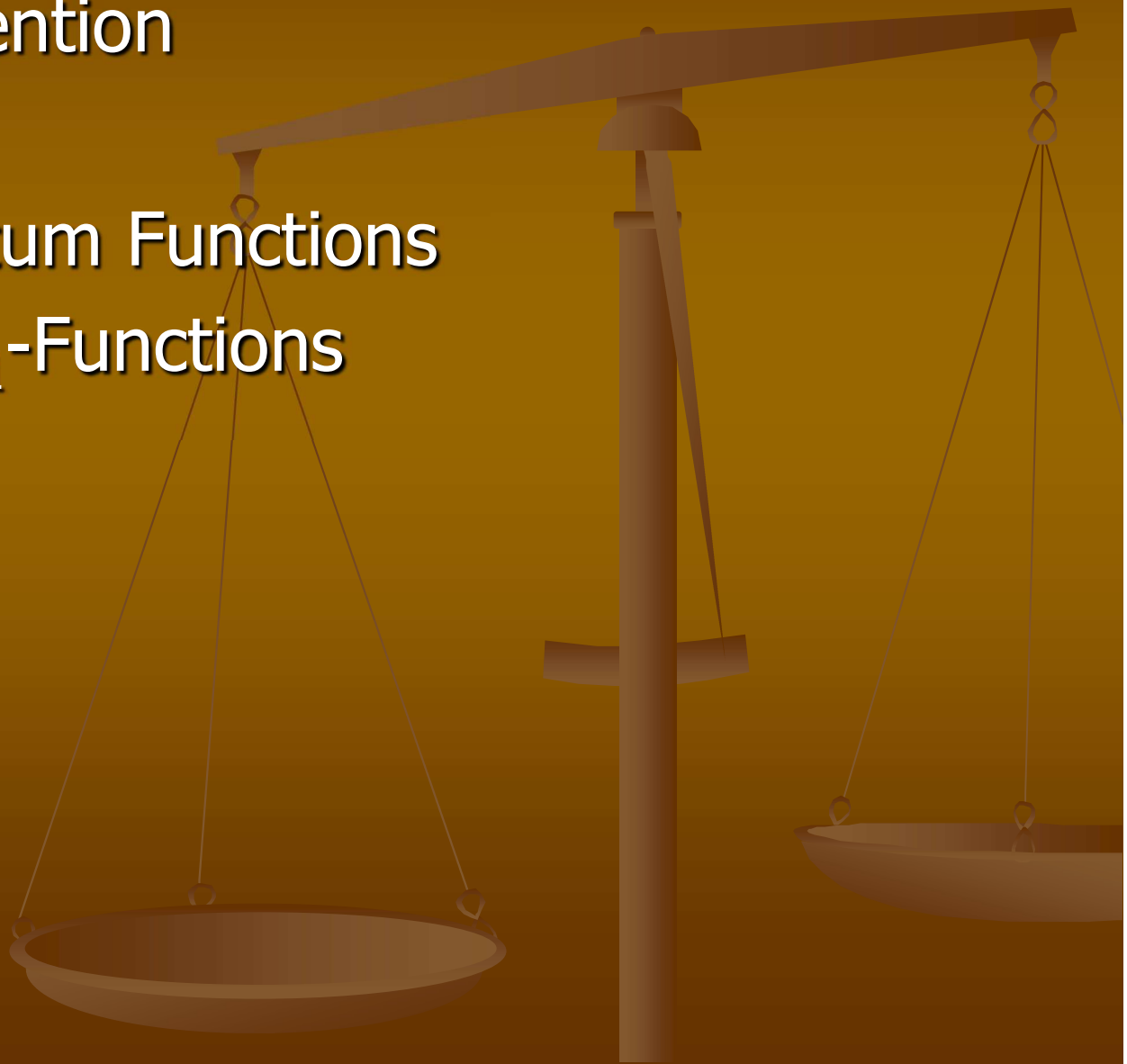
Quantum Functions

- H_k : Hilbert space of dimension k
- Computational basis: $\{ |s\rangle : s \in \{0,1\}^n \}$
- $H_k = \text{span}\{ |s\rangle : s \in \{0,1\}^n \}$, where $k = 2^n$
- Qustring of length n : vector in H_k ($k = 2^n$)
- $H_\infty = \cup_{k \in A} H_k$, where $A = \{2^n : n \geq 1 \}$
- A quantum function is a mapping from H_∞ to H_∞.
- This terminology is different from that of Yamakami (2003).

T. Yamakami. Analysis of quantum functions. Int. J. Found. Comput. Sci. 14 (2003) 815-852.

III. A New Recursive Definition

1. Notational Convention
2. New Definition
3. Classes of Quantum Functions
4. Examples of $\square^{QP}_1$-Functions



Notational Convention

- For measurement, we use the following notional convention.
- Let $t \in \{0,1\}^n$.
- $\langle t|\varphi\rangle$ = a quantum state obtained from $|\varphi\rangle$ by observing the first $|t|$ qubits on $|t\rangle$
- If either $|\varphi\rangle$ or $|\psi\rangle$ is the null vector, then $\langle\psi|\varphi\rangle$ is also the null vector.

New Definition – Initial Functions

- We define a class $\square^{QP}{}_1$ of quantum functions as follows.

- Initial quantum functions
  1) I (identity) $I(|\varphi\rangle) = |\varphi\rangle$
  2) AMP (phase shift) $AMP_\theta(|\varphi\rangle) = e^{i\theta}|\varphi\rangle$
  3) ROT rotation) $ROT_\theta(|\varphi\rangle) = \cos\theta|\varphi\rangle + \sin\theta(|0\rangle \otimes \langle 1|\varphi\rangle - |1\rangle \otimes \langle 0|\varphi\rangle)$
  4) NOT (negation) $NOT(|\varphi\rangle) = |0\rangle \otimes \langle 1|\varphi\rangle + |1\rangle \otimes \langle 0|\varphi\rangle$
  5) REMOVE (relocation) $REMOVE(|\varphi\rangle) = \sum_{b\in\{0,1\}} \langle b|\varphi\rangle \otimes |b\rangle$
  6) SWAP (swapping) $SWAP(|\varphi\rangle) = |\varphi\rangle$ or $\sum_{a,b\in\{0,1\}} |ab\rangle \otimes \langle ba|\varphi\rangle$
  7) MEAS (partial measurement) $MEAS[i](|\varphi\rangle) = \langle i|\varphi\rangle$

- Here, we explicitly describe how these functions work.
- Let $a_1, a_2, \ldots, a_n$ be strings.

- I: $|a_1 a_2 \ldots a_n\rangle \rightarrow |a_1 a_2 \ldots a_n\rangle$
- AMP: $|a_1 a_2 \ldots a_n\rangle \rightarrow e^{i\theta}|a_1 a_2 \ldots a_n\rangle$
- ROT: rotation
- REMOVE: $|a_1 a_2 a_3 \ldots a_n\rangle \rightarrow |a_2 a_3 \ldots a_n a_1\rangle$
- SWAP: $|a_1 a_2 a_3 \ldots a_n\rangle \rightarrow |a_2 a_1 a_3 \ldots a_n\rangle$
- MEAS: $|a_1 a_2 \ldots a_n\rangle \rightarrow |a_2 \ldots a_n\rangle$

New Definition - Construction Rules

- Composition rule

$$Compo[g,h](|\varphi\rangle) = g \circ h(|\varphi\rangle)$$

- Branching rule

$$Branch[g,h](|\varphi\rangle) = |\varphi\rangle \qquad \text{if } l(|\varphi\rangle) \le 1$$

$$Branch[g,h](|\varphi\rangle) = |0\rangle \otimes g(\langle 0|\varphi\rangle) + |1\rangle \otimes h(\langle 1|\varphi\rangle) \quad \text{o.w.}$$

- Quantum recursion

$$QRec[h,g](|\varphi\rangle) = h(|\varphi\rangle) \qquad \text{if } |\varphi\rangle \in H_2$$

$$QRec[h,g](|\varphi\rangle) = g(|0\rangle \otimes f_0(\langle 0|\varphi\rangle) + |1\rangle \otimes f_1(\langle 1|\varphi\rangle)) \quad \text{o.w.}$$

Classes of Quantum Functions

- $\Box^{QP}_1$ = class of all quantum functions constructed from the initial functions and by applying construction rules.

- $\widetilde{\Box^{QP}}_1$ = class of all quantum functions constructed from the initial functions except for the partial measurement and by applying construction rules.

- Note that $\widetilde{\Box^{QP}}_1 \subseteq \Box^{QP}_1$ holds.

Examples of $\square^{QP}{}_1$-Functions

- CNOT (Controlled-NOT): $CNOT = Branch[I, NOT]$

$$CNOT(|\varphi\rangle) = |0\rangle \otimes \langle 0|\varphi\rangle + |1\rangle \otimes NOT(\langle 1|\varphi\rangle)$$

- $zROT_\theta$ (rotation at z-axe) : $zROT_\theta$ = Branch[AMP_θ ,$AMP_{-\theta}$]

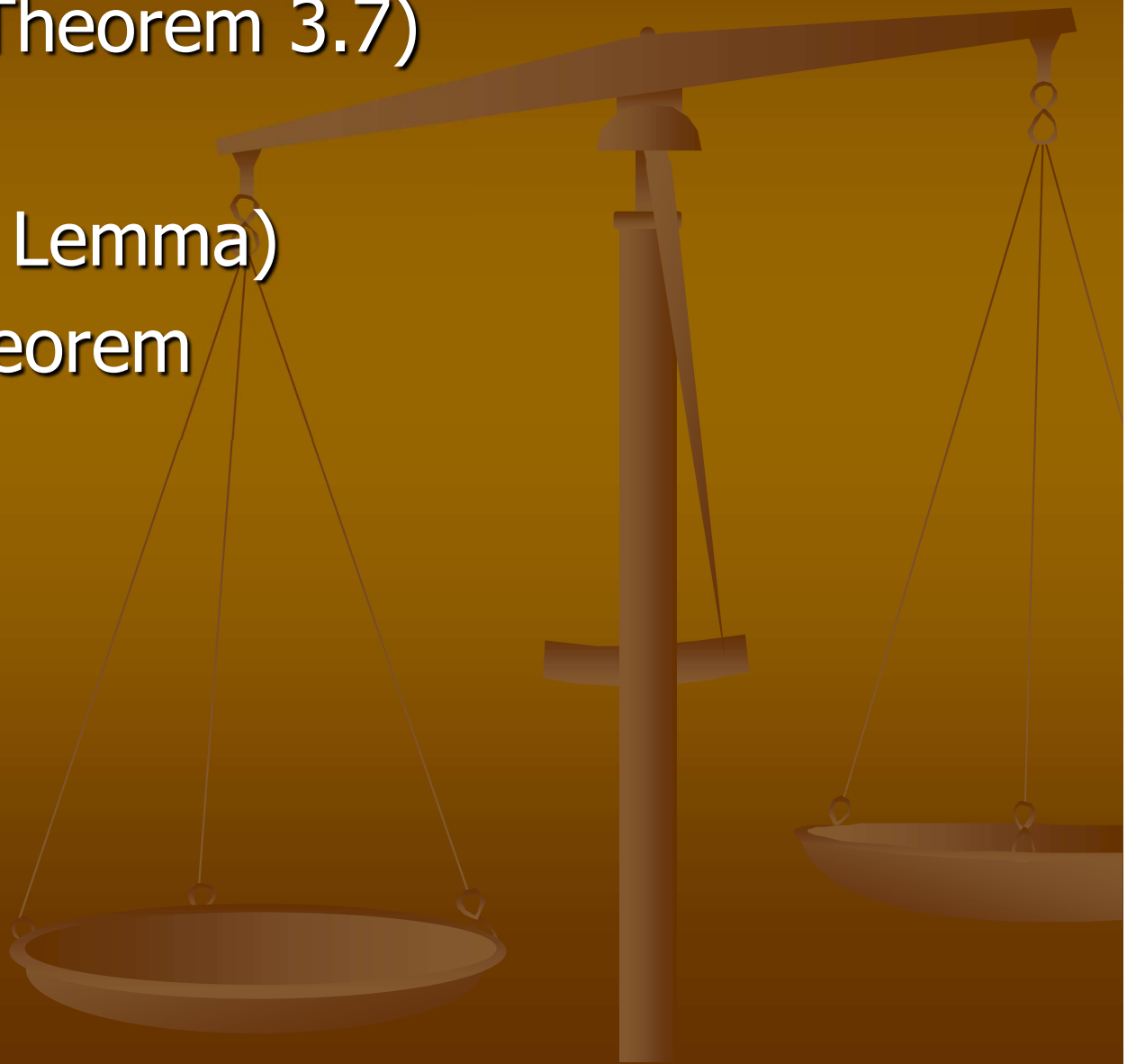
$$zROT_\theta(|\varphi\rangle) = e^{i\theta}|0\rangle \otimes \langle 0|\varphi\rangle + e^{-i\theta}|1\rangle \otimes \langle 1|\varphi\rangle$$

- WH (Walsh-Hadamard) : $WH = ROT_{\pi/4} \circ NOT$

$$WH(|\varphi\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (\langle 0|\varphi\rangle + \langle 1|\varphi\rangle) + \frac{1}{\sqrt{2}}|0\rangle \otimes (\langle 0|\varphi\rangle - \langle 1|\varphi\rangle)$$

VI. A New Characterization

1. Main Theorem (Theorem 3.7)
2. Lemma 3.8
3. Lemma 3.9 (Key Lemma)
4. Normal Form Theorem



Notational Convention

- Let g be any quantum function.
- Let p be any polynomial.
- Define $|\varphi^p_g(x)\rangle = g(|0^{p(|x|)}10^{9p(|x|)}1\rangle|x\rangle)$.
- Set $0\tilde{} = 00$, $1\tilde{} = 01$, and $2\tilde{} = 11$.
- If $s = s_1s_2\ldots s_n$ for s_i in $\{0,1\}$, then define $s\tilde{} = \text{ext}(s) = s_1\tilde{}s_2\tilde{}\ldots s_n\tilde{}2\tilde{}$.
- Note that $|s\tilde{}| = 2n+2$.

Main Theorem (Theorem 3.7)

- Main Theorem (Theorem 3.7)
  - Let f be any function from {0,1}* to {0,1}*.
  - The following three statements are logically equivalent.

1. $f \in FBQP$
2. $\forall \varepsilon \in [0,1/2) \exists g \in \widetilde{\square^{QP}}_1 \ \exists p\text{:poly s.t.}$
$$|f(x)| \le p(|x|) \text{ and } \left\| \left\langle ext(f(x)) \middle| \phi_g^p(x) \right\rangle \right\|^2 \ge 1-\varepsilon$$
3. $\forall \varepsilon \in [0,1/2) \exists g \in \square^{QP}_1 \ \exists p\text{:poly s.t.}$
$$l\left(\left|\phi_g^p(x)\right\rangle\right) = |f(x)| \text{ and } \left| \left\langle f(x) \middle| \phi_g^p(x) \right\rangle \right|^2 \ge 1-\varepsilon$$

- We split this theorem into two lemmas.

Lemma 3.8

- If $f \in \Box^{QP}_1$, then $\exists p$:poly $\exists M$:QTM s.t. M works as follows:
  - On each qustring input $|\varphi\rangle$ of length n, M starts with $|\varphi\rangle$ on inputs input tape and produces $f(|\varphi\rangle)$ on its output tape in time at most p(n).

- Proof:

By a direct simulation of f by an appropriate QTM.

Lemma 3.9 (Key Lemma)

- M*(x) = “code” of final tape contents of M on input x

PC = polynomial-time aproximable amplitudes

- Lemma 3.9
  - If M is a single-tape, polynomial-time, PC-amplitude, well-formed QTM, then, $\exists g \in \Box^{QP}_1$ $\exists p$:poly s.t. $\forall x$ $\left\| \left\langle M^*(x) \middle| \phi_g^p(x) \right\rangle \right\|^2 = 1$

- Proof:

  We need to construct the desired quantum function g to simulate the behavior of M on input x.

Normal Form Theorem

- Theorem 3.10

  $\exists f \in \square^{QP}_1 \; \forall g \in \square^{QP}_1 \; \forall \varepsilon \in [0,1) \; \exists e$ (independent of $|\varphi\rangle$) s.t. $\left\| |\tilde{e}\rangle \otimes g(|\varphi\rangle) - f(|\tilde{e}\rangle \otimes |\varphi\rangle) \right\|^2 < \varepsilon$

- f is called universal.

- Proof:

  By taking a universal QTM and applying Theorem 3.7 to it.

V. Two Applications

1. New Descriptional Complexity
2. Type-2 Quantum Functionals

New Descriptional Complexity

- Our recursive definition of a function f in $\square^{QP}_1$ provides a means of measuring the "descritional" complexity.

- $\square^{QP}_1$-descriptional complexity of f at length n = minimal number of times when we use initial functions and construction rules to build a $\square^{QP}_1$-function g s.t. $\forall x$

$$\left|\left\langle f(x)\middle|\phi_g^p(x)\right\rangle\right|^2 \geq \frac{2}{3}$$

for a certain polynomial p with $|f(x)| \leq p(|x|)$.

Type-2 Quantum Functionals

- Functions mapping Σ^* to Σ^* are conventionally categorized as type-1 functionals.
- We call quantum functions mapping from H_∞ to H_∞ type-1 quantum functionals.
- We can expand them to type-2 quantum functionals using oracles, which are basically type-1 quantum functionals.
- We hope this line of research will bring new light to the fundamentals of quantum computability.

Thank you for listening

Q & A

I’m happy to take your question!

END

Thank you for listening!