Quantum Complexity, Relativized Worlds, and Oracle Separations

Dimitrios I. Myrisiotis
blah • ntua school of mechanical engineering

Committee: Kerenidis, Zachos, Fotakis, and Pagoutrzis.

Monday 10th October, 2016

Introduction

Introduction

$$\underbrace{\square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square\ \square}_{16}$$

$$\forall \square : \square \in \{0, 1\}$$

Figure : Our 16-bit computer, with 2^{16} configurations.

Introduction

$$b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13}\ b_{14}\ b_{15}\ b_{16}$$

$$\forall i \in \{1, 2, \ldots, 16\} : b_i \in \{0, 1\}$$

Figure : Communicating a configuration of a **deterministic** computer.

Introduction

$$\underbrace{b_1\ b_2\ b_3\ b_4\ b_5\ b_6\ b_7\ b_8\ b_9\ b_{10}\ b_{11}\ b_{12}\ b_{13}\ b_{14}\ b_{15}\ b_{16}}_{\text{a 16-bit string} \Leftrightarrow k \in \mathbb{N} \Leftrightarrow p_k = 1}$$

$$\forall i \in \{1, 2, \ldots, 16\} : b_i \in \{0, 1\}$$

Figure : Communicating a configuration of a **deterministic** computer.

Introduction

$$p_1 \; p_2 \; \dots \; p_{2^{16}}$$

$$\forall i \in \left\{1, 2, \dots, 2^{16}\right\} : p_i \in \{0, 1\}$$

$$\sum_{i=1}^{2^{16}} p_i = 1 \Leftrightarrow \exists! k : p_k = 1$$

Figure : Communicating a configuration of a **deterministic** computer.

Introduction

$$p_1 \;\; p_2 \;\; \ldots \;\; p_{2^{16}}$$

$$\forall i \in \left\{1, 2, \ldots, 2^{16}\right\} : p_i \in [0, 1]$$

$$\sum_{i=1}^{2^{16}} p_i = 1$$

Figure : Communicating a configuration of a **probabilistic** computer.

Introduction

$$c_1 \;\; c_2 \;\; \ldots \;\; c_{2^{16}}$$

$$\forall i \in \left\{1, 2, \ldots, 2^{16}\right\} : c_i \in \mathbb{C}$$

$$\sum_{i=1}^{2^{16}} |c_i|^2 = 1 \qquad (*)$$

Figure : Communicating a configuration of a **quantum** computer.

Quantum Computing 101

Quantum States

Quantum Computing 101: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\begin{aligned}
\mathbf{v}_1 &= 0\ldots000 \\
\mathbf{v}_2 &= 0\ldots001 \\
&\vdots \\
\mathbf{v}_{2^{16}} &= \underbrace{1\ldots111}_{16}
\end{aligned}$$

Quantum Computing 101: Quantum States

$$\mathbf{v}_1 = \underbrace{0\dots000}_{16} = \left.\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}\right\} 2^{16}$$

$$\mathbf{v}_2 = \underbrace{0\dots001}_{16} = \left.\begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}\right\} 2^{16}$$

Quantum Computing 101: Quantum States

...

Quantum Computing 101: Quantum States

$$\mathbf{v}_{2^{16}-1} = \underbrace{1\ldots110}_{16} = \left.\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix}\right\} 2^{16}$$

$$\mathbf{v}_{2^{16}} = \underbrace{1\ldots111}_{16} = \left.\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}\right\} 2^{16}$$

Quantum Computing 101: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\begin{aligned}\mathcal{H}' &= \text{span}\left(\mathcal{B}, \mathbb{C}\right) = \left\{ \sum_{i=1}^{2^{16}} c_i \cdot \mathbf{v}_i \mid \forall i : c_i \in \mathbb{C} \text{ and } \mathbf{v}_i \in \mathcal{B} \right\} \\ &= \mathbb{C}^{2^{16}}\end{aligned}$$

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathcal{H}' \mid \|\mathbf{q}\|_2 = 1 \right\} \subseteq \mathcal{H}'$$

Quantum Computing 101: Quantum States

$$\begin{aligned}\mathcal{H} &= \left\{\mathbf{q} \in \mathbb{C}^{2^{16}} \mid \|\mathbf{q}\|_2 = 1\right\} \\ &= \text{Our world.} \\ &\subseteq \mathbb{C}^{2^{16}}\end{aligned}$$

Quantum Computing 101: Quantum States

$n \in \mathbb{N}$

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

Quantum Computing 101: Quantum States

$n \in \mathbb{N}$

$n =$ The number of qubits of our quantum system.

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

Quantum Computing 101: Quantum States

$$n \in \mathbb{N}$$

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

Quantum Computing 101: Quantum States

$$n \in \mathbb{N}$$

$$\mathcal{H} = \left\{ \mathbf{q} \in \mathbb{C}^{2^n} \mid \|\mathbf{q}\|_2 = 1 \right\}$$

$$\mathbf{q} = \left(\sum_{i=1}^{2^{16}} c_i \cdot \mathbf{v}_i \right) \in \mathcal{H} \Leftrightarrow \|\mathbf{q}\|_2 = 1 \Leftrightarrow \sum_{i=1}^{2^n} |c_i|^2 = 1 \qquad (*)$$

Quantum Computing 101: Quantum States

$$|\psi\rangle$$

Quantum Computing 101: Quantum States

$$|\psi\rangle \in \mathcal{H} \subseteq \mathbb{C}^{2^n}$$

Quantum Computing 101: Quantum States

$$
\begin{aligned}
|\psi\rangle &= \text{a ket} \\
&= \text{a column vector}
\end{aligned}
$$

$$
\begin{aligned}
\langle\psi| &= \text{a bra} \\
&= \text{the dual of the ket } |\psi\rangle \\
&= |\psi\rangle^{\dagger} \\
&= (|\psi\rangle^{*})^{T} = \left(|\psi\rangle^{T}\right)^{*} \\
&= \text{a row vector}
\end{aligned}
$$

Quantum Computing 101: Quantum States

$$\mathcal{B} = \{\mathbf{v}_i\}_{i=1}^{2^{16}}$$

$$\begin{aligned} \mathbf{v}_1 &= 0\ldots000 \\ \mathbf{v}_2 &= 0\ldots001 \\ &\vdots \\ \mathbf{v}_{2^{16}} &= 1\ldots111 \end{aligned}$$

Quantum Computing 101: Quantum States

$$\mathcal{B} = \{|v_i\rangle\}_{i=1}^{2^{16}}$$

$$\begin{aligned} |v_1\rangle &= |0\ldots000\rangle \\ |v_2\rangle &= |0\ldots001\rangle \\ &\vdots \\ |v_{2^{16}}\rangle &= |1\ldots111\rangle \end{aligned}$$

Quantum Computing 101: Quantum States

$$\mathcal{B} = \{|v_i\rangle\}_{i=1}^{2^{16}}$$

$$\begin{aligned}
|v_1\rangle &= |0\dots000\rangle = |1\rangle \\
|v_2\rangle &= |0\dots001\rangle = |2\rangle \\
&\vdots \qquad\qquad\quad \vdots \\
|v_{2^{16}}\rangle &= |1\dots111\rangle = \left|2^{16}\right\rangle
\end{aligned}$$

Quantum Computing 101: Quantum States

Example. The qubit.

$$\mathcal{B} = \{|v_i\rangle\}_{i=1}^{2}$$

$$|v_1\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|v_2\rangle = |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi_{\text{qubit}}\rangle = c_1 \cdot |v_1\rangle + c_2 \cdot |v_2\rangle \qquad \| |\psi_{\text{qubit}}\rangle \|_2 = 1$$

Quantum Computing 101: Quantum States

$$
\begin{aligned}
\mathcal{I}\left(|\psi\rangle, |\phi\rangle\right) &= \text{inner product} \\
&= \langle\psi| \cdot |\phi\rangle \\
&= \langle\psi|\phi\rangle \in \mathbb{C}
\end{aligned}
$$

$$
\begin{aligned}
\mathcal{O}\left(|\psi\rangle, |\phi\rangle\right) &= \text{outer product} \\
&= |\psi\rangle \cdot \langle\phi| \\
&= |\psi\rangle\langle\phi| \in \mathbb{C}^{2^n \times 2^n}
\end{aligned}
$$

Unitary Evolution

Quantum Computing 101: Unitary Evolution

$$U \left| q_{\text{old}} \right\rangle = \left| q_{\text{new}} \right\rangle$$

$$U^{-1} = U^{\dagger} = (U^{*})^{T} = \left(U^{T}\right)^{*}$$

Quantum Computing 101: Unitary Evolution

$$|q_{\text{initial}}\rangle \in \mathcal{H}$$

Quantum Computing 101: Unitary Evolution

$$U_1 \left| q_{\text{initial}} \right\rangle \in \mathcal{H}$$

Quantum Computing 101: Unitary Evolution

$$U_2 U_1 |q_{\text{initial}}\rangle \in \mathcal{H}$$

Quantum Computing 101: Unitary Evolution

$$m \in \mathbb{N}$$

$$U_m \cdots U_2 U_1 \left| q_{\text{initial}} \right\rangle \in \mathcal{H}$$

Quantum Computing 101: Unitary Evolution

$$m \in \mathbb{N}$$

$$|q_{\text{final}}\rangle = U_m \cdots U_2 U_1 |q_{\text{initial}}\rangle \in \mathcal{H}$$

Quantum Computing 101: Unitary Evolution

$$m \in \mathbb{N}$$

$$|q_{\text{final}}\rangle = U_m \cdots U_2 U_1 |q_{\text{initial}}\rangle \in \mathcal{H}$$

Figure : Our first quantum algorithm.

Measurements

Quantum Computing 101: Measurements

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \in \mathcal{H}$$

$n \in \mathbb{N}$

$\forall i : c_i \in \mathbb{C}$ and $|v_i\rangle \in \mathcal{B}$

$$\sum_{i=1}^{2^n} |c_i|^2 = 1 \qquad (*)$$

Quantum Computing 101: Measurements

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \overset{\text{Measurement}}{\Rightarrow} \exists j : |\psi'\rangle = |v_j\rangle$$

$$\Pr[\text{The outcome is } j.] = |c_j|^2$$

Quantum Computing 101: Measurements

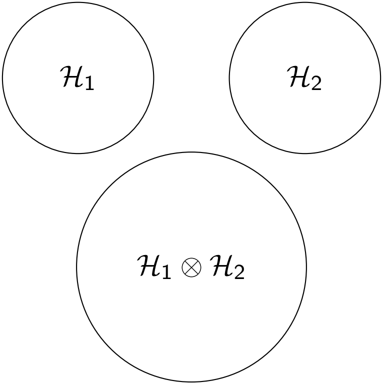
$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |v_i\rangle \overset{\text{Measurement}}{\Rightarrow} \exists j : |\psi'\rangle = |v_j\rangle$$

$$\overset{\text{Measurement}}{\Rightarrow} |\psi''\rangle = |v_j\rangle$$

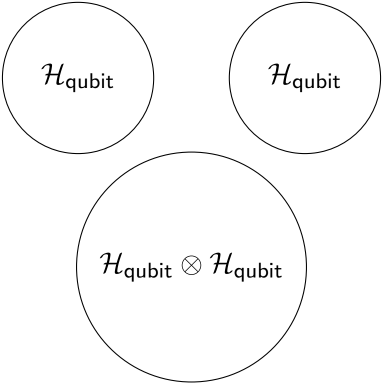
$$\begin{aligned} \Pr[\text{The outcome is } j.] &= |1|^2 \\ &= 1 \end{aligned}$$

Composition

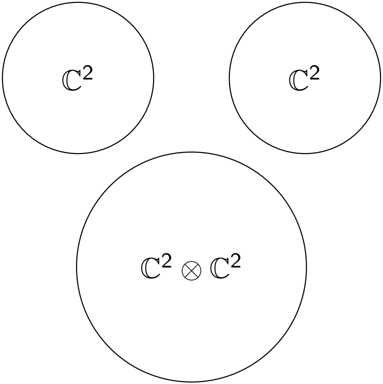
Quantum Computing 101: Composition



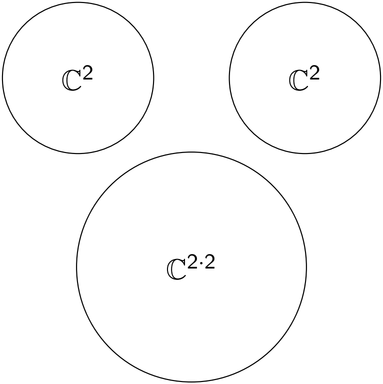
Quantum Computing 101: Composition



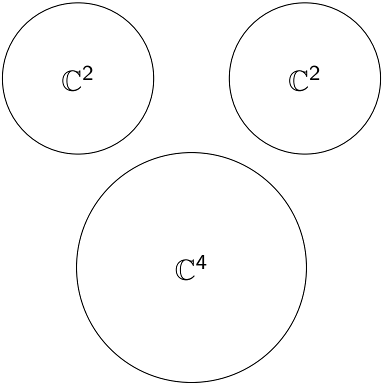
Quantum Computing 101: Composition



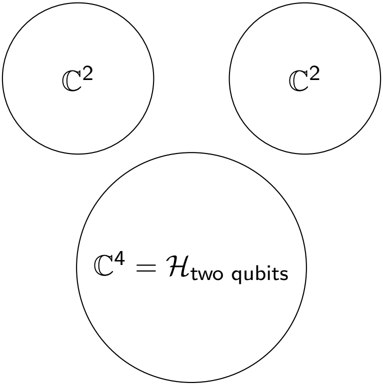
Quantum Computing 101: Composition



Quantum Computing 101: Composition



Quantum Computing 101: Composition



A Comparison

Quantum Computing 101: A Comparison

Table : Quantum mechanics and probability theory.

Probability Theory	Quantum Mechanics
Real numbers in $[0, 1]$	Complex numbers
Real numbers that sum to 1	Complex numbers that the squares of their magnitudes sum to 1
The *sum* is equal to 1	The *Euclidean norm* is equal to 1
The *sum* is preserved	The *Euclidean norm* is preserved
The L_1-norm is preserved	The L_2-norm is preserved
Use of stochastic matrices	Use of unitary matrices

Oracles

Quantum Computing 101: Oracles

classical oracle $f : \{0,1\}^n \rightarrow \{0,1\}$

unitary quantum oracle $q_1 : |\psi\rangle \mapsto U\,|\psi\rangle$

CPTP quantum oracle $q_2 : \rho \mapsto \mathscr{U}\,\rho$

$$\rho = |\psi\rangle\langle\psi| \in \mathbb{C}^{2^n \times 2^n}$$

$$\mathscr{U}\,\rho = \sum_i U_i \rho U_i^\dagger$$

Quantum Computing 101: Oracles

unitary quantum oracle $q_1 : |\psi\rangle \mapsto U\,|\psi\rangle$

CPTP quantum oracle $q_2 : \rho \mapsto \mathscr{U}\,\rho$

$$\rho = |\psi\rangle\langle\psi| \in \mathbb{C}^{2^n \times 2^n}$$

$$\mathscr{U}\,\rho = \sum_i U_i \rho U_i^\dagger$$

Quantum Computing 101: Oracles

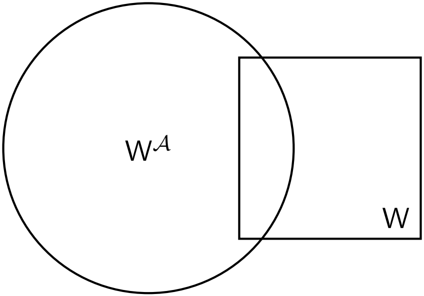


Figure : Our world, namely W, and a relativized world $W^{\mathcal{A}}$, induced by calls to some oracle $\mathcal{A}$.

Quantum Computing 101: Oracles

Examples of quantum oracle applications.

$$\exists \mathcal{A} : \mathsf{QMA}^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}} \qquad (2006)$$

$$\exists \mathcal{A} : \mathsf{QMA}^{\mathcal{A}} \not\subseteq \mathsf{QMA}_1^{\mathcal{A}} \qquad (2009)$$

$$\exists \mathcal{A} : \mathsf{SQMA}^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}} \qquad (2015)$$

Quantum Complexity

Quantum Complexity

$$\begin{aligned} \mathsf{P} &\subseteq \mathsf{NP} \\ &\subseteq \mathsf{MA} \\ &\subseteq \mathsf{QMA} \end{aligned}$$

Quantum Complexity

$$\begin{aligned} \mathsf{P} &\subseteq \mathsf{NP} \\ &\subseteq \mathsf{MA} \\ &\subseteq \mathsf{QCMA} \\ &\subseteq \mathsf{QMA} \end{aligned}$$

Quantum Complexity

$$\begin{aligned} \mathsf{P} &\subseteq \mathsf{NP} \\ &\subseteq \mathsf{MA} \\ &\subseteq \mathsf{QCMA} \\ &\subseteq \mathsf{QMA} = \mathsf{SQMA} \end{aligned}$$

Quantum Complexity

What is SQMA?

$$\mathcal{B} = \{|i\rangle\}_{i=1}^{2^n}$$

$$|\psi\rangle = \sum_{i=1}^{2^n} c_i \cdot |i\rangle = \text{a generic state} \in \mathcal{H}$$

$$S \subseteq [2^n] = \{1, 2, 3, \ldots, 2^n\}$$

$$|S\rangle = \sum_{i \in S} \frac{1}{\sqrt{|S|}} \cdot |i\rangle = \text{a subset state} \in \mathcal{H}$$

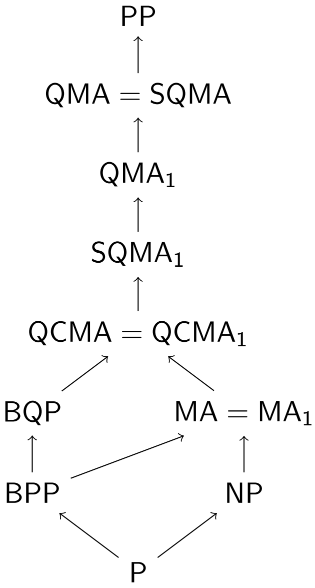
Quantum Complexity

$$
\begin{aligned}
\mathsf{P} &\subseteq \mathsf{NP} \\
&\subseteq \mathsf{MA} = \mathsf{MA}_1 \\
&\subseteq \mathsf{QCMA} = \mathsf{QCMA}_1 \\
&\subseteq \mathsf{SQMA}_1 \\
&\subseteq \mathsf{QMA}_1 \\
&\subseteq \mathsf{QMA} = \mathsf{SQMA} \\
&\subseteq \mathsf{PP}
\end{aligned}
$$

Quantum Complexity

$(A \to B) \equiv (A \subseteq B)$

Polynomial-time classes.



Our Result

$\exists\mathcal{A} : \mathsf{SQMA}_1^{\mathcal{A}} \not\subseteq \mathsf{QCMA}^{\mathcal{A}}$

Dimitrios I. Myrisiotis
blah • ntua school of mechanical engineering

Committee: Kerenidis, Zachos, Fotakis, and Pagoutrzis.

Monday 10th October, 2016