International Journal of Quantum Information
Vol. 3, No. 3 (2005) 463–473
© World Scientific Publishing Company

"NON-IDENTITY-CHECK" IS QMA-COMPLETE

DOMINIK JANZING[*], PAWEL WOCJAN[†] and THOMAS BETH

Universität Karlsruhe, Am Fasanengarten 5,
76 131 Karlsruhe, Germany
[*]*janzing@ira.uka.de*
[†]*wocjan@ira.uka.de*

Received 22 July 2004
Revised 20 October 2004

We describe a computational problem that is complete for the complexity class QMA, a quantum generalization of NP. It arises as a natural question in quantum computing and quantum physics. "Non-identity-check" is the following decision problem: Given a classical description of a quantum circuit (a sequence of elementary gates), determine whether it is almost equivalent to the identity. Explicitly, the task is to decide whether the corresponding unitary is close to a complex multiple of the identity matrix with respect to the operator norm. We show that this problem is QMA-complete. A generalization of this problem is "non-equivalence check": given two descriptions of quantum circuits and a description of a common invariant subspace, decide whether the restrictions of the circuits to this subspace almost coincide. We show that non-equivalence check is also in QMA and hence QMA-complete.

Keywords: Quantum complexity theory.

1. The Complexity Class QMA

In classical computer science, an important complexity class is NP. Roughly speaking, it is the class of decision problems which have the following property: if the answer is "yes" there is a proof (classical string of polynomial length) whose validity can be checked on a classical computer in polynomial time. In other words, finding the proof may be difficult but checking it is easy. Meanwhile, there are a lot of problems known with practical relevance which are NP-complete.[1]

With the invention of the quantum computing model, which is conjectured to be more powerful than the classical (Turing) computing model, the question was addressed as to how NP generalizes to quantum computing.[2,3] The idea is that a decision problem is in "quantum-NP" if there is a proof of polynomial size that can be verified efficiently on a quantum computer. There are two natural ways to define the notion of a proof in the quantum setting. On the one hand, the proof may still be a classical string; on the other hand, it may be a quantum state. In the first case, one obtains the complexity class QCMA, in the second the class QMA. Due to the fact that important quantum algorithms[4] are probabilistic, the classes QCMA and

QMA are, strictly speaking, generalizations of the classical complexity MA. The class MA refers to so-called Arthur–Merlin games,[2] where the proof is generated by Merlin (endowed with unlimited computational power) and checked by Arthur (endowed with polynomially bounded computational power). In this setting, Arthur can check the proof only with a certain probability. Furthermore, even if the answer of the decision problem is "no", there may be (incorrect) proofs that are accepted by Arthur with small non-zero probability.

Here, we focus on the class QMA, which is formally defined in Sec. 3. It is straightforward to ask whether there are natural problems which are QMA-complete. So far, the only known example of a natural problem is the so-called k-local Hamiltonian problem (for $k \geq 2$).[2–7] It is motivated by quantum statistical physics and is, roughly speaking, the problem of deciding whether the minimal energy value of an interacting many-particle quantum system is smaller than a certain bound a or greater than b with a sufficient separation between a and $b > a$. In this article, we give another QMA-complete problem which arises in controlling complex quantum systems by elementary transformations. It is, intuitively speaking, the problem of deciding whether a sequence of operations on the quantum system acts trivially. Our formulation of non-identity check and the generalization non-equivalence check refers to the standard model of a quantum computer where complex transformations (unitary operations on the Hilbert space of the quantum register) are implemented by a sequence of elementary operations (acting on two quantum bits only). However, the transformations acting on the system Hilbert space need not necessarily be interpreted as quantum algorithms. Implementing complex processes by sequences of elementary operations (enabled by natural interactions) may be a general principle for controlling micro- and nano-scopic systems in the future.

This paper is organized as follows. In Sec. 2, we define the problem "non-equivalence check" formally. In Sec. 3, we prove that it is contained in the complexity class QMA. In Sec. 4, we show that even a specific instance of "non-equivalence check," namely "non-identity check," is QMA-complete.

2. Stating the Problem "Non-Equivalence Check"

In order to state the problem "non-equivalence check," we briefly rephrase the standard model of a quantum computer.[8] The state of its register is given by a one-dimensional subspace of the vector space $\mathcal{H} := (\mathbb{C}^2)^{\otimes n}$, where every tensor component describes the state space of one quantum bit ("qubit"). A quantum gate is usually described by a unitary transformation on $\mathcal{H}$ which acts only on one or two tensor components non-trivially ("one-qubit gates" or "two-qubit gates", respectively). The computation is performed by sequences of one- or two-qubit gates such that a certain unitary transformation on the register is implemented. The read-out of the register is a measurement of the qubits which leads probabilistically to some classical binary word as the answer to the computational problem. Designing a desired unitary transformation such that it implements a desired computation is actually the problem of inventing quantum algorithms.

More specifically, consider the following situation: let U be a quantum network acting on n qubits that consists of two-qubit gates:

$$U = U_k \cdots U_2 U_1 .$$

Someone claims that the same transformation U could also be implemented by another sequence

$$V_l \cdots V_2 V_1 .$$

Assume that he did not tell us why he thinks that this sequence also implements U. How difficult is it to determine whether it really does? Also the following slight modification of the problem is natural. Usually, we are not interested in the whole physical state space but rather in a computational subspace. This subspace may, for instance, be defined by a quantum error correcting code[9] or a decoherence free subspace.[10,11] Then, it is not relevant whether the alternative network coincides with the original one on the whole space but only on the code space. Assume that we already know (for example, by construction) that both networks leave this subspace invariant. Does the alternative circuit agree with the original one when it is restricted to the subspace? This is obviously equivalent to the question whether the restriction of

$$V_1^\dagger V_2^\dagger \cdots V_l^\dagger U_k \cdots U_2 U_1$$

is the identity. Since we are talking about complexity theory, it would not be natural to allow that the considered subspace $\mathcal{V}$ to be arbitrary; we would rather demand that it can be specified by a circuit in an efficient way. More explicitly, we demand that the circuit checks whether the state is in $\mathcal{V}$ or its orthogonal complement and writes the answer to some output qubit. Since the dimension of $\mathcal{V}$ is not necessarily half of the total dimension of the register where U acts on, the check will in general need ancilla qubits. It seems reasonable to assume that every decomposition $\mathcal{V} \oplus \mathcal{V}^\perp$ of the register space which allows an efficient yes-no measurement can be performed by a circuit with polynomial size (acting on an extended register) which writes the answer to one specific qubit.

First, we introduce some notation that will be used throughout the paper. We denote the Hilbert space of a qubit by $\mathcal{B} := \mathbb{C}^2$. Let $x \in \{0,1\}^*$ be an arbitrary binary string. We denote the length of x by $|x|$. For any Hilbert space $\mathcal{H}$, we denote the set of density matrices acting on $\mathcal{H}$ by $S(\mathcal{H})$.

We define formally:

Definition 1 (Non-Equivalence Check). Let x, y be classical descriptions of quantum networks consisting of $\text{poly}(|x|)$ and $\text{poly}(|y|)$ many two-qubit gates, respectively. Let U_x and U_y be the unitary transformations implemented by the circuits acting on n qubits with $n \in O(\text{poly}(|x|))$ and $n \in O(\text{poly}(|y|))$. Consider a common invariant subspace $\mathcal{V}$ of $\mathcal{B}^{\otimes n}$. Let $\mathcal{V}$ be specified by a quantum circuit

V on $\mathcal{B}^{\otimes(n+m)}$ with polynomial complexity such that $V\mathcal{V} = W_1$, where W_1 is the space of all states of $\mathcal{B}^{\otimes(n+m)}$ and where the last qubit is in the state $|1\rangle$. The non-equivalence check problem is to decide whether the restrictions of U_x and U_y to $\mathcal{V}$ coincide approximatively. Explicitly, we assume that it is promised that for some known $\delta, \mu > 0$ (depending on $|x|$ and $|y|$) with $1/(\delta - \mu) \in O(\text{poly}(|x| + |y|))$ either

(i) there is a vector $|\Psi\rangle \in \mathcal{V}$ such that

$$\|(U_x U_y^\dagger - e^{i\phi}\mathbf{1})|\Psi\rangle\| \geq \delta$$

for all $\phi \in [0, 2\pi)$, or

(ii) there exists an angle $\phi \in [0, 2\pi)$ such that for all vectors $|\Psi\rangle \in \mathcal{V}$

$$\|(U_x U_y^\dagger - e^{i\phi}\mathbf{1})|\Psi\rangle\| \leq \mu.$$

Note that the non-equivalence check has some analogy to a classical NP-complete problem. For a classical boolean circuit, the problem SAT is to decide whether there is a truth assignment that the circuit output is “true.”[12] To see the analogy, one may rephrase it as the problem of deciding whether the circuit is equivalent to the circuit that always outputs “false.”

3. Non-Equivalence Check is in QMA

The complexity class QMA consists of the problems of deciding whether a given string is in a certain language in QMA. We define the set of QMA languages in the following[5]:

Definition 2 (QMA). Fix $\epsilon = \epsilon(|x|)$ such that $\epsilon \in 2^{-o(|x|)}$ and $\epsilon \leq 1/3$. Then a language L is in QMA if for every classical input $x \in \{0,1\}^*$, one can efficiently generate (by classical precomputation) a quantum circuit U_x (“verifier”) consisting of at most $p(|x|)$ elementary gates for an appropriate polynomial p such that U_x acts on the Hilbert space

$$\mathcal{H} := \mathcal{B}^{\otimes n_x} \otimes \mathcal{B}^{\otimes m_x},$$

where n_x and m_x grow at most polynomially in $|x|$. The first part is the input register and the second is the ancilla register. Furthermore, U_x has the following properties:

(i) If $x \in L$ there exists a quantum state ρ that is accepted by the circuit with high probability, i.e.

$$\exists\, \rho \in S(\mathcal{B}^{n_x}), \quad \text{tr}(U_x\,(\rho \otimes |0\ldots 0\rangle\langle 0\ldots 0|)\,U_x^\dagger\, P_1) \geq 1 - \epsilon,$$

where P_1 is the projection corresponding to the measurement “Is the first qubit in state 1?”

(ii) If $x \notin L$ all quantum states are rejected with high probability, i.e.

$$\forall\, \rho \in S(\mathcal{B}^{n_x}), \quad \mathrm{tr}(U_x\,(\rho \otimes |0\ldots 0\rangle\langle 0\ldots 0|)\,U_x^\dagger\,P_1) \leq \epsilon.$$

Note that our "witnesses" are mixed states in contrast to the definitions in Refs. 2 and 5. Due to linearity arguments, this modification does not change the language L. Note furthermore that it is always possible to construct a verifier for the same language with ϵ' arbitrarily close to 0. This "amplification of probabilities" is described in Ref. 2 in detail. This may be necessary in Sec. 4: in order to show that every problem in QMA can be reformulated as the problem "non-identity-check" we will require that the given QMA-problem is formulated in such a way that ϵ is sufficiently small.

To prove that the non-equivalence check is in QMA, we have to describe how to give a witness state that proves that U_x and U_y do not coincide. For an arbitrary unitary operator W, the difference from multiples of the identity is a normal operator. Hence, its operator norm is given by the greatest modulus of the eigenvalues. Therefore, the operator norm distance between W and the set of trivial transformations (global phases) can be determined as follows.

Whenever there exist eigenvalues $\exp(i\alpha)$ and $\exp(i\beta)$ of W, the norm distance to $\exp(i\phi)\mathbf{1}$ is at least

$$\max\{|e^{i\alpha} - e^{i\phi}|, |e^{i\beta} - e^{i\phi}|\}. \tag{1}$$

If $|\alpha - \beta| \leq \pi$, the minimum of expression (1) is achieved for $\phi := (\alpha - \beta)/2$ and the norm distance to the trivial transformations implementing global phases is hence at least

$$|1 - e^{i(\alpha-\beta)/2}| = \sqrt{2(1 - \cos((\alpha - \beta)/2))}.$$

Let U_x', U_y' be the restrictions of U_x and U_y to $\mathcal{V}$. If Case (i) of Definition 1 is true, there exists eigenvectors $|\psi_a\rangle$ and $|\psi_b\rangle$ of $U_x'(U_y')^\dagger$ with eigenvalues $e^{i\alpha}$ and $e^{i\beta}$, respectively such that

$$\delta \leq \sqrt{2(1 - \cos((\alpha - \beta)/2))}.$$

In order to check that the eigenvalues corresponding to the given eigenvectors satisfy this criterion, one can use the phase estimation procedure.[13]

Due to the promise that in Case (ii) one has $\sqrt{2(1 - \cos((\alpha - \beta)/2)} \leq \mu$, the accuracy of the phase estimation has to be chosen such that $\cos((\alpha - \beta)/2)$ can be determined up to an error of $(\delta^2 - \mu^2)/4$. It remains to check whether $|\psi_a\rangle$ and $|\psi_b\rangle$ are elements of $\mathcal{V}$. This can be done using the given circuit V.

In fact, the setting of QMA problems (see Definition 2) requires that the witness is one quantum state instead of two. Formulated as an Arthur–Merlin game,[2] Merlin proves to Arthur that a string x is in QMA by sending the witness quantum state. Here, he may prove that $U_x U_y^\dagger$ has eigenvalues of non-negligible distance by sending the state $|\psi_a\rangle \otimes |\psi_b\rangle$. *A priori*, it is not clear that Merlin cannot cheat by sending entangled (incorrect) witnesses. However, one can easily check that the circuit in Fig. 1 treats any state

$$\sum_j c_j |\psi_a^j\rangle \otimes |\psi_b^j\rangle$$

as an incoherent mixture of product states $|\psi_a^j\rangle \otimes |\psi_b^j\rangle$ with weights $|c_j|^2$. Note that it is also irrelevant whether the witness states $|\psi_a\rangle$ and $|\psi_b\rangle$ are really eigenstates of $U_x U_y^\dagger$. The phase estimation procedure can only produce output that really exists as eigenvalues (up to an accuracy that is determined by the size of the ancilla register used). In Fig. 1, one can see the whole circuit.

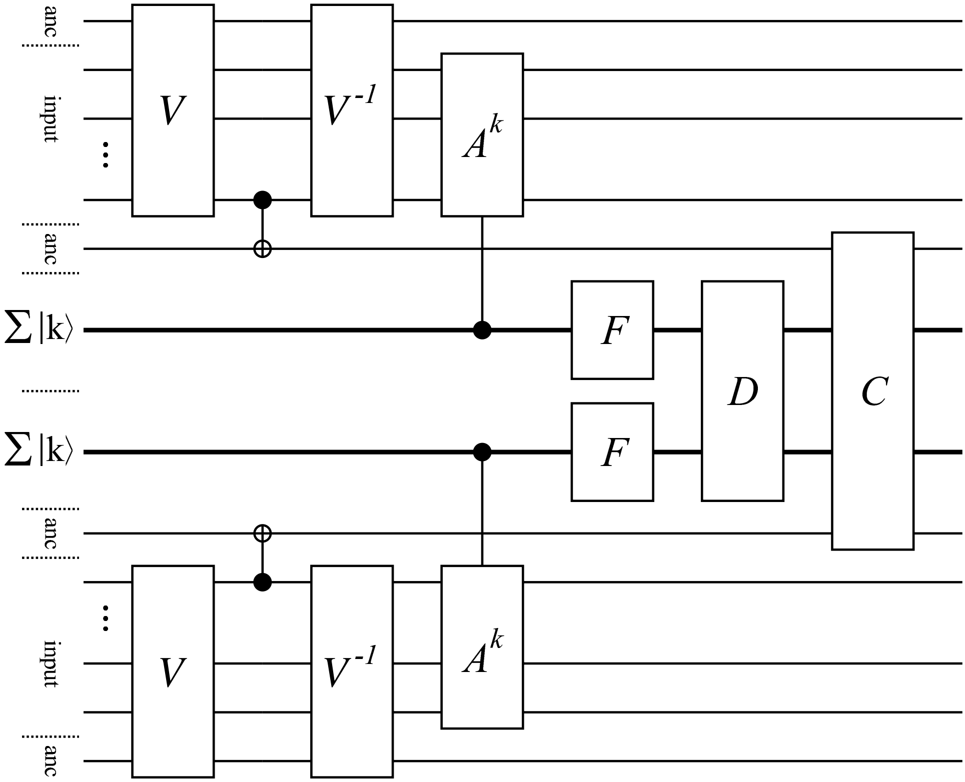

Fig. 1. Circuit used to verify that $U_x U_y^\dagger$ is not close to the identity on the subspace $\mathcal{V}$. The two copies of V check that the witness states are really elements of $\mathcal{V}$. The results of this check are copied to additional ancilla qubits by Controlled-NOT gates. The main part of the circuit (A^k and F) is the usual phase estimation procedure. The ancilla registers are initialized into the superposition state $(1/\sqrt{m})\sum_{k\leq m}|k\rangle$ and control the implementation of $A^k := (U_x U_y^\dagger)^k$. The state $|k\rangle$ obtains a phase according to the eigenvalues of A^k. By Fourier transformations F the phases can be read out from the ancilla registers. A circuit D computes the phase difference and C checks whether the difference is sufficiently large and the witness states are elements of the subspace $\mathcal{V}$.

4. “Non-Identity-Check” is QMA-Complete

First, we state the problem “non-identity-check” formally.

Definition 3 (Non-Identity-Check). Let x be a classical description of a quantum circuit U_x of complexity polynomial in $|x|$. Decide whether U_x is close to the trivial transformation in the following sense. Decide which of the two following cases is true given the promise that either of (i) or (ii) is satisfied:

(i) for all $\phi \in [0, 2\pi)$ one has $\|U_x - e^{i\phi}\mathbf{1}\| \geq \delta$, or
(ii) there exists an angle $\phi \in [0, 2\pi)$ such that $\|U_x - e^{i\phi}\mathbf{1}\| \leq \mu$.

Assume furthermore that $1/(\delta - \mu) \in O(\text{poly}(|x|))$.

Note that this problem is a specific instance of the non-equivalence check.

The general QMA setting is that a quantum circuit U is given and the problem is to decide whether there is a state $|\psi\rangle$ such that the state

$$U(|\psi\rangle \otimes |0 \ldots 0\rangle)$$

has the property that the first qubit is with high probability in the state $|1\rangle$. In order to show that Non-Identity-Check encompasses QMA, we construct a circuit Z that implements a unitary close to the identity whenever there is no state that is accepted by U and a circuit less close to the identity if there is a witness. The register is extended by one qubit and the whole circuit is the transformation

$$Z := U^\dagger W U V.$$

The transformation V is a phase shift controlled by the states of the ancillas. Whenever the ancilla part of the register is initialized in the state $|0 \ldots 0\rangle$, the additional qubit gets a phase $\exp(i\varphi)$. The gate W is a phase shift controlled by the output qubit of U. The additional qubit gets a phase $\exp(i\varphi)$ whenever the circuit has accepted (see Fig. 2). Even though this idea is straightforward, there is a subtle difficulty that makes the proof quite technical. Assume that the ancilla register is not initialized correctly. Then the output qubit of U may be in a superposition or even entangled with the rest of the register. In this case, the application of the second conditional phase shift in Fig. 2 creates entanglement with the uppermost ancilla qubit. Therefore, U^{-1} does not reverse the action of U. Nevertheless, the whole network is close enough to the identity as geometric arguments prove below.

Theorem 1. *Let U be a quantum circuit on $\mathcal{B}^{\otimes(n+m)}$ with the promise that either of two cases in Definition* 2 *is true. Then, for the circuit Z in Fig.* 2, *the following statements hold*:

If Case (i) *is true then we have*

$$\|Z - e^{i\gamma}\mathbf{1}\| \geq \sqrt{2(1 - \cos\varphi)} - 2\sqrt{\epsilon}$$

for all $\gamma \in \mathbb{R}$.

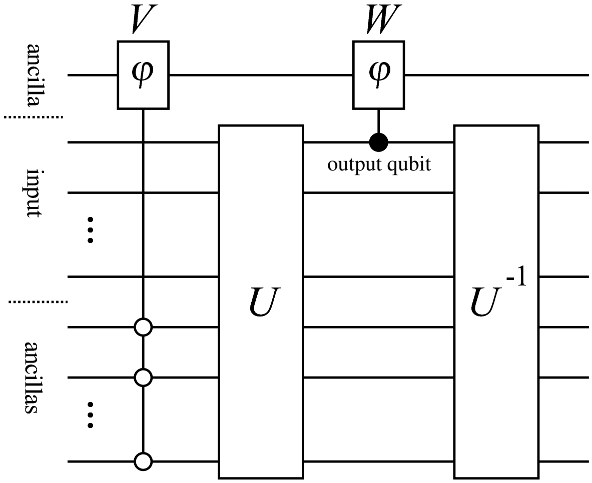

Fig. 2. Circuit Z consisting of U, $U^\dagger$ and two controlled phase shifts V and W with phase φ. If U rejects all states with high probability the circuit is closer to the identity than in the case that there is a state that is likely to be accepted. The first ancilla can only obtain a phase shift 2φ if the other ancilla register has been correctly initialized and the input has been accepted by U. Acceptance or not is defined by the logical state of the output qubit. Here it is the uppermost qubit where U acts on.

If Case (ii) *is true then we have*

$$\|Z - e^{i\varphi/2}\mathbf{1}\| \leq 2\sqrt{1-\cos(\varphi/2)} + 2\sqrt{2\epsilon}.$$

Proof. The effect of Z on a general state $|\Psi\rangle$ can be understood if we express $|\Psi\rangle$ as

$$|\Psi\rangle = |\Psi_1\rangle + |\Psi_2\rangle,$$

where $|\Psi_1\rangle$ is a state with ancillas all set to 0 and $|\Psi_2\rangle$ a state with ancilla register in states different from $|0\ldots0\rangle$. We have

$$Z|\Psi\rangle = U^\dagger WUV|\Psi_1\rangle + U^\dagger WUV|\Psi_2\rangle.$$

Consider Case (ii) and the effect of Z on the summand $|\Psi_1\rangle$:

$$U^\dagger WUV|\Psi_1\rangle = U^\dagger WP_1UV|\Psi_1\rangle + U^\dagger W(\mathbf{1}-P_1)UV|\Psi_1\rangle,$$

where P_1 is (see Definition 2) the projection onto the state $|1\rangle$ of the output qubit. By definition of W, one has

$$W(\mathbf{1}-P_1) = (\mathbf{1}-P_1).$$

Hence, we have

$$\begin{aligned} Z|\Psi_1\rangle &= U^\dagger WP_1UV|\Psi_1\rangle + U^\dagger(\mathbf{1}-P_1)UV|\Psi_1\rangle \\ &= U^\dagger WP_1UV|\Psi_1\rangle + V|\Psi_1\rangle - U^\dagger P_1UV|\Psi_1\rangle. \end{aligned}$$

Since the probability of acceptance is at most ϵ, the length of the vector $P_1UV|\Psi_1\rangle$ is at most $\sqrt{\epsilon}\|\,|\Psi_1\rangle\|$. We conclude that

$$\|Z|\Psi_1\rangle - V|\Psi_1\rangle\| \le 2\sqrt{\epsilon}\|\,|\Psi_1\rangle\|\,.$$

Note that $\|V-\exp(i\varphi/2)\mathbf{1}\| = |1-\exp(i\varphi/2)\|$ due to the arguments at the end of Sec. 3. Due to $\|V|\Psi_1\rangle - e^{i\varphi/2}|\Psi_1\rangle\| \le |1-\exp(i\varphi/2)|\,\|\,|\Psi_1\rangle\|$, we have

$$\|Z|\Psi_1\rangle - e^{i\varphi/2}|\Psi_1\rangle\| \le (2\sqrt{\epsilon}+|1-\exp(i\varphi/2)|)\,\|\,|\Psi_1\rangle\|. \tag{3}$$

Consider the effect of Z on $|\Psi_2\rangle$:

$$\begin{aligned}\|Z|\Psi_2\rangle - e^{i\varphi/2}|\Psi_2\rangle\| &= \|U^\dagger WUV|\Psi_2\rangle - e^{i\varphi/2}|\Psi_2\rangle\| \\ &= \|U^\dagger(W-e^{i\varphi/2}\mathbf{1})U|\Psi_2\rangle\| \le \|W-e^{i\varphi}\mathbf{1}\|\,\|\,|\Psi_2\rangle\|.\end{aligned}$$

Together with inequality (3), we have

$$\begin{aligned}\|Z|\Psi\rangle - e^{i\varphi/2}|\Psi\rangle\| &\le (|1-\exp(i\varphi/2)|+2\sqrt{\epsilon})(\|\,|\Psi_1\rangle\| + |\Psi_2\rangle\|) \\ &\le \sqrt{2}(|1-\exp(i\varphi/2)|+2\sqrt{\epsilon}).\end{aligned}$$

With $|1-\exp(i\varphi/2)| = \sqrt{2(1-\cos\varphi/2)}$, we have

$$\|Z-e^{i\varphi/2}\mathbf{1}\| \le 2\sqrt{1-\cos(\varphi/2)} + 2\sqrt{2\epsilon}.$$

Consider Case (i). Let $|\psi\rangle$ be a state that is accepted by U with probability $1-\epsilon$. Define $P_0 := \mathbf{1} - P_1$. We take the state vector

$$|\Psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle.$$

We have

$$\begin{aligned}Z|\Psi\rangle &= U^\dagger WUV\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &= U^\dagger WU\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &= U^\dagger W(\mathbf{1}-P_0)U\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &\quad + U^\dagger WP_0U\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &= U^\dagger(\mathbf{1}-P_0)U\frac{1}{\sqrt{2}}(|0\rangle+e^{i2\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &\quad + U^\dagger WP_0U\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle+e^{i2\varphi}|\mathbf{1}\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &\quad - U^\dagger P_0U\frac{1}{\sqrt{2}}(|0\rangle+e^{i2\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &\quad + U^\dagger P_0U\frac{1}{\sqrt{2}}(|0\rangle+e^{i\varphi}|1\rangle)\otimes|\psi\rangle\otimes|0\ldots0\rangle \\ &=: |\hat{\Psi}\rangle - |\varphi_1\rangle + |\varphi_2\rangle.\end{aligned}$$

Note that the vectors $|\varphi_1\rangle$ and $|\varphi_2\rangle$ have at most norm $\sqrt{\epsilon}$ due to the high probability of acceptance. One can check easily that

$$\min_{\gamma\in\mathbb{R}} \| \, |\hat{\Psi}\rangle - e^{i\gamma}|\Psi\rangle \| = \| \, |\hat{\Psi}\rangle - e^{i\varphi}|\Psi\rangle \| = |1 - \exp(i\varphi)| \, .$$

We conclude that

$$\min_{\gamma\in\mathbb{R}} \|Z|\Psi\rangle - e^{i\gamma}|\Psi\rangle\| \geq |1 - \exp(i\varphi)| - 2\sqrt{\epsilon} \, .$$

With $|1-\exp(i\varphi)| = \sqrt{2(1-\cos\varphi)}$, we conclude that the minimal norm difference between Z and $e^{i\gamma}\mathbf{1}$ is at least $\sqrt{2(1-\cos\varphi)} - 2\sqrt{\epsilon}$.

As mentioned in the remark after Definition 2, the value ϵ can be made arbitrarily small. For small φ the lower and upper bounds on the norm distances between U and the trivial transformations are approximatively given by

$$\varphi + 2\sqrt{2\epsilon}$$

and

$$\sqrt{2}\varphi - 2\sqrt{\epsilon},$$

respectively. This shows that for sufficiently small ϵ there is a sufficient separation between the lower and upper bound. This shows that every oracle that is able to decide whether $Z = U_x^\dagger W U_x V$ is close to a trivial transformation can be used to decide whether x is in L.

5. Conclusions

Due to our formulation, the problems "non-identity-check" and "non-equivalence check" seem to arise only from problems of quantum *computing* as we refer to the notion of a quantum *circuit* composed from elementary *gates*. However, the following point of view may consider both problems as general questions in quantum control and quantum physics.

Independent from computational problems, the notion of quantum gates formalizes the concept of elementary micro-physical processes that can be used to generate complex processes. Quantum control may, for instance, be used to generate entangled states, for algorithmic cooling.[14] Although most of these control problems appear (presently) also in the context of quantum *computing*, future applications of sophisticated quantum control problems are at the moment hard to predict. However, it seems to be a natural problem to decide whether a sequence of elementary physical processes implements a closed-loop process, i.e. the whole operation is the identity on the relevant part of the state space. This could, for instance, be related to issues of thermodynamic reversibility.

Acknowledgments

The authors thank Thomas Decker for helpful discussions. This work was supported by grants of the BMBF-project 01/BB01B.

References

1. M. Garey and D. Johnson, *Computers and Intractibility* (Freeman and Company, New York, 1979).
2. A. Kitaev, A. Shen and M. Vyalyi, *Classical and Quantum Computation*, Vol. 47 (American Mathematical Society, Providence, Rhode Island, 2002).
3. D. Aharonov and T. Naveh, Quantum NP — A survey, quant-ph/0210077.
4. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26**(5), 1484–1509 (1997).
5. J. Kempe and O. Regev, 3-local Hamiltonian is QMA-complete, *Quant. Inf. Comput.* **3**, 258–264 (2003).
6. J. Kempe, A. Kitaev and O. Regev, The complexity of the local Hamiltonian problem, in *Proc. 24th FSTTCS* (2004), pp. 372–383.
7. S. Aaronson, The complexity zoo, http://www.cs.berkeley.edu/∼aaronson/zoo.html.
8. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
9. A. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* **77**, 793–797 (1996).
10. P. Zanardi and M. Rasetti, Noiseless quantum codes, *Phys. Rev. Lett.* **79**, 3306–3309 (1997).
11. E. Fortunato, L. Viola, J. Hodges, G. Teklemariam and D. Cory, Implementation of universal control on a decoherence-free qubit, *New J. Phys.* **4**, 5.1–5.20 (2002).
12. Ch. Papamitrou, *Computational Complexity* (Addison Wesley, Reading, MA, 1994).
13. R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, Quantum algorithms revisited, *Proc. Roy. Soc. London* **A454**, 339–354 (1998).
14. R. Schulman and U. Vazirani, Scalable NMR quantum computers, quant-ph/9804060.