Quantum Information and Computation, Vol. 3, No. 6 (2003) 635–643
© Rinton Press

TWO QCMA-COMPLETE PROBLEMS

PAWEL WOCJAN, DOMINIK JANZING and THOMAS BETH
Institut für Algorithmen und Kognitive Systeme, University Karlsruhe
Am Fasanengarten 5, 76133 Karlsruhe, Germany
email: {wocjan,janzing}@ira.uka.de

Received September 8, 2003
Revised October 23, 2003

QMA and QCMA are possible quantum analogues of the complexity class NP. In QMA the proof is a quantum state and the verification is a quantum circuit. In contrast, in QCMA the proof is restricted to be a classical state. It is not known whether QMA strictly contains QCMA. Here we show that two known QMA-complete problems can be modified to QCMA-complete problems in a natural way: (1) Deciding whether a 3-local Hamiltonian has low energy states (with energy smaller than a given value) that can be prepared with at most k elementary gates is QCMA-complete, whereas it is QMA-complete when the restriction on the complexity of preparation is dropped. (2) Deciding whether a (classically described) quantum circuit does not act as the identity on *all basis states* is QCMA-complete. It is QMA-complete to decide whether it does not act on *all states* as the identity.

Keywords: quantum complexity, quantum NP, QCMA, quantum circuit design
Communicated by: R Cleve & J Watrous

1 Introduction

The complexity class QCMA is the class of decision problems for which a "yes" answer can be verified by a quantum computer with access to a *classical* proof. It contains MA [1], and is contained in QMA [2]. The computer is restricted to be classical for MA and the proof is allowed to be quantum for QMA.

More explicitly, QMA problems read as follows: Given a quantum circuit U that acts on a quantum register consisting of $n+m$ qubits where m qubits (the "ancillas") are initialized to the state $|0\dots 0\rangle$, decide whether there is a state vector $|\psi\rangle$ on the remaining n qubits (the "input register") such that after the implementation of U a measurement of the first qubit yields "1" with high probability. We say, the circuit has accepted the input state $|\psi\rangle$.

For QCMA, the problem is to decide whether there is a *basis state* $|y\rangle$ on n qubits that is accepted with high probability. Then the classical proof consists merely of the number $0 \leq y < 2^n$ of the basis state.

Let us recall the formal definition of QCMA [3]. In the following we denote the vector space $\mathbf{C}^2$ by $\mathcal{B}$ and the length of any binary string $y \in \{0,1\}^*$ by $|y|$.

Definition 1 (QCMA)

Fix $\epsilon = \epsilon(|x|)$ such that $2^{-\Omega(|x|)} \leq \epsilon \leq 1/3$. Then a language L is in QCMA 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 property that

1. If $x \in L$ there exists a classical string $y \in \{0,1\}^{n_x}$ such that the corresponding computational basis state $|y\rangle$ is accepted by the circuit with high probability, i.e.,

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

   where P_1 is the projection corresponding to the measurement "Is the first qubit in state 1?".

2. If $x \notin L$ all computational basis states are rejected with high probability, i.e.,

$$\forall\, y \in \{0,1\}^{n_x}\,, \quad tr(U_x\,(|y\rangle\langle y| \otimes |0\ldots 0\rangle\langle 0\ldots 0|)\,U_x^\dagger\, P_1) \leq \epsilon\,.$$

2 Non-identity check on basis states

In Ref. [4] we stated the problem "non-identity check". The task is to decide whether a (classically described) quantum circuit U is far from the identity in the sense that there is no global phase ϕ such that the operator norm $\|U - \exp(i\phi)\mathbf{1}\|$ is smaller than a certain bound.

This problem (strictly speaking, its negation) arises naturally in the design of quantum circuits: Given a quantum circuit $U_l \cdots U_1$: Decide whether another sequence of elementary gates $V_k \cdots V_1$ implements almost the same unitary transformation, i.e., whether

$$U_l \cdots U_1 V_1^\dagger \cdots V_k^\dagger$$

is almost equivalent to the identity.

But also a weaker definition of equivalence is natural. Usually, quantum algorithms start with classical input (basis states as input) and end with measurements in the computational basis to obtain the classical output. In this context one does not care whether two circuits agree on all states, it is only relevant whether they agree on the basis states. Below we shall show that these considerations lead to the formulation of a QCMA-complete problem.

So, what does make the difference between the original requirement (identity on the whole space) and the weaker formulation (identity on all basis states)? First it is clear that a unitary operator that maps every basis state $|x\rangle\langle x|$ on itself may give different phases to different basis states. But one can easily see that this *does not* make the difference between QCMA and QMA (in case these classes are indeed different): The statement that a quantum circuit gives different phases to different basis vectors has still a classical proof. It is given by two numbers of basis states with non-negligible phase difference. The verifier can check the phase difference efficiently by quantum phase estimation [5] (compare also [4]).

What can possibly make the difference between QMA and QCMA is the fact that there exist unitary transformations U that have large norm distance to all trivial transformations

$\exp(i\phi)\mathbf{1}$ even though the distance between $U|x\rangle$ and $|x\rangle$ is exponentially small on all basis states $|x\rangle$. Let $U = HDH$, where H is the Hadamard transformation on n qubits and $D = \text{diag}(-1, 1, 1, \ldots, 1)$ is a controlled phase shift on the first qubit. The norm distance $\|\mathbf{1} - D\|$ is 2. But for all computational basis states $|y\rangle$ we have

$$\|(\mathbf{1} - HDH)|y\rangle\| = \|H(\mathbf{1} - D)H|y\rangle\| = \|(2/2^n)\sum_{\tilde{y}} |\tilde{y}\rangle\| = 2/2^{n/2}$$

since $H\,\text{diag}(1, 0, 0, \ldots, 0)\,H$ is the all-one-matrix.

Let us define the problem non-identity check on basis states.

Definition (Non-identity check on basis states)
Let $\{Z_x\}_{x\in\Sigma^*}$ be a polynomial-time uniformly generated family of quantum circuits acting on n_x qubits. It is promised that

1. either there is a binary string $z \in \{0, 1\}^{n_x}$ such that
$$|\langle z|Z_x|z\rangle|^2 \leq 1 - \mu_x\,,$$
i.e., Z_x does not act as the identity on the basis states,
2. or for all binary strings $z \in \{0, 1\}^{n_x}$
$$|\langle z|Z_x|z\rangle|^2 \geq 1 - \delta_x\,,$$
i.e., Z_x acts “almost” as the identity on all computational basis states,

where $\mu_x - \delta_x \geq 1/poly(|x|)$. The problem of non-identity check on basis states is to decide which case is true.

It is easily seen that this problem is contained in QCMA since the proof for case 1 is given by a string that describes the basis state $|z\rangle$. Then we perform the quantum circuit Z_x. An n-fold controlled-NOT can be used to flip an additional ancilla qubit if and only if the output is $|y\rangle$. The additional ancilla is the output qubit of the verifier.

QCMA-completeness of this problem can be proved in strong analogy to the proof for QMA-completeness of identity check. Let U be a quantum circuit as in Definition 1. We construct the quantum circuit Z that uses U and $U^\dagger$ as subroutines.

Let R be the rotation
$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix},$$
with $0 < \varphi < \pi/2$ and R_a be the rotation R controlled by the m ancilla qubits corresponding to U. R_a is implemented if and only if the ancillas are correctly initialized in the state $|0\ldots0\rangle$. Let R_o be the same rotation R controlled by the output qubit of U. (To prove QMA-completeness of identity check we have used controlled phase shifts that are diagonal in the computational basis.) The whole circuit $Z := U^\dagger R_o U R_a$ is shown in Figure 1.

The following theorem shows that the problem of deciding whether there are basis states that are likely to be accepted by U can be reduced to identity check on basis states.

Theorem (QCMA-completeness):
Let $\{U_x\}_{x\in\Sigma^*}$ be a polynomial-time uniformly generated family of quantum circuits as in the

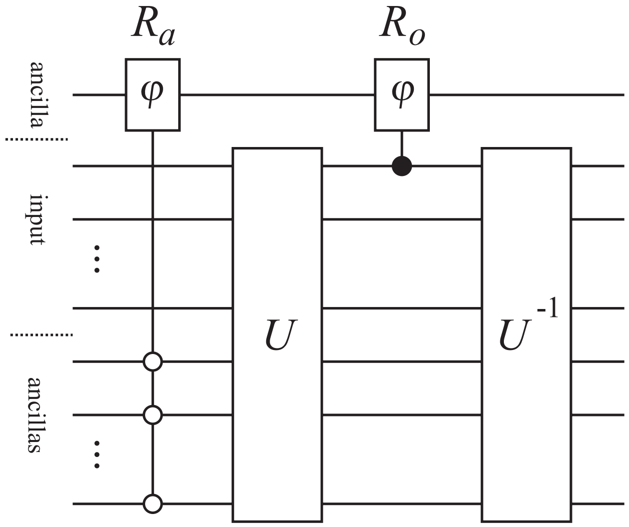

Fig. 1. The circuit Z does not act as the identity on all basis states if and only if there is a witness that is accepted by U.

definition of QCMA (Definition 1). Then the following statement holds for the corresponding circuit Z_x:

If case the first case of Definition 1 is true then there is a binary string z such that

$$|\langle z|Z|z\rangle|^2 \leq (\cos(2\varphi) + \sqrt{\epsilon})^2 \,,$$

where $|z\rangle = |0\rangle \otimes |y\rangle \otimes |00\cdots 0\rangle$ and y is the classical certificate for the the circuit U.

If the second case is true then for all binary strings z we have

$$|\langle z|Z|z\rangle|^2 \geq (\cos(\varphi) - 2\sqrt{\epsilon})^2 \,.$$

The difficulty in proving this theorem stems from the fact that in the quantum setting the application of R_o changes the state of the output qubit. Therefore, $UR_oU^\dagger$ is not the identity even if there is no state that is accepted by U. Note that if we apply U to a state with not correctly initialized ancillas the output qubit may be in a superposition state or even entangled with the rest of the register. A subsequent application of R_o may therefore entangle the (upper) ancilla with the rest of the register. Consequently, the application of $U^\dagger$ does not necessarily undo the computation performed by U.

These observations make it necessary to use some geometrical arguments to show that the whole circuit is closer to the identity on basis states if there are no witness states compared to the case that there is a witness.

The proof is in strong analogy to the proof in Ref. [4]. The important difference is that no superpositions between states with correctly and wrongly initialized ancillas have to be considered. Therefore the bounds are easier to derive.

Case 1. Let $|y\rangle$ be a binary string that is accepted by U with high probability (we drop the subscripts for fixed x). We consider the binary string $|z\rangle := |0\rangle \otimes |y\rangle \otimes |00\cdots 0\rangle$ to show that Z is "far" from the identity on the basis states.

$$\begin{array}{rcl} Z|z\rangle & = & U^\dagger R_o U R_a |z\rangle \\ & = & U^\dagger R_o U (\cos\varphi)|0\rangle + \sin\varphi|1\rangle) \otimes |y\rangle \otimes |0\ldots 0\rangle \\ & = & U^\dagger R_o (\cos\varphi)|0\rangle + \sin\varphi|1\rangle) \otimes (c_1|1\rangle \otimes |\psi_1\rangle + c_0|0\rangle \otimes |\psi_0\rangle) \end{array}$$

Due to the high probability of acceptance we have $|c_0| \leq \sqrt{\epsilon}$. Now we consider only the term with c_1 and obtain

$$\begin{array}{rl} & U^\dagger R_o (\cos\varphi)|0\rangle + \sin\varphi|1\rangle) \otimes c_1|1\rangle \otimes |\psi_1\rangle \\ = & (\cos(2\varphi))|0\rangle + \sin(2\varphi)|1\rangle) \otimes c_1 U^\dagger (|1\rangle \otimes |\psi_1\rangle)\,. \end{array} \tag{1}$$

The first component is the single ancilla on which the rotation R is performed, the second component is the output of U and the third tensor component is the remaining part of the register where U acts on.

The overlap between the initial vector $|z\rangle$ and the vector of eq. (1) is at most $|c_1|\cos(2\varphi)$. Taking into account the length of the neglected vector we obtain

$$|\langle z|Z|z\rangle| \leq \cos(2\varphi) + \sqrt{\epsilon}\,.$$

Case 2. Let z be a string such that the bits corresponding to ancillas of U are all set to 0. Let P_1 as in Definition 1 be the projection onto the state $|1\rangle$ of the output qubit corresponding to U. Note that $R_o(\mathbf{1} - P_1) = \mathbf{1} - P_1$. Therefore, we have

$$\begin{array}{rcl} |\langle z|Z|z\rangle| & = & |\langle z|U^\dagger R_o U R_a|z\rangle| \\ & = & |\langle z|U^\dagger R_o (P_1 + \mathbf{1} - P_1) U R_a|z\rangle| \\ & = & |\langle z|U^\dagger R_o P_1 U R_a + R_a - U^\dagger P_1 U R_a|z\rangle| \\ & \geq & |\langle z|R_a|z\rangle| - |\langle z|U^\dagger R_o P_1 U R_a|z\rangle| - |\langle z|U^\dagger P_1 U R_a|z\rangle| \\ & \geq & \cos\varphi - 2\sqrt{\epsilon}\,. \end{array}$$

The latter inequality follows from the fact that the length of the vector $P_1 U R_a|z\rangle$ is at most $\sqrt{\epsilon}$ due to the small probability of acceptance.

Let z be a string such that the bits corresponding to the ancillas of U are not all set to 0. Then we have

$$\begin{array}{rcl} |\langle z|U^\dagger R_o U R_a|z\rangle| & = & |\langle z|U^\dagger R_o U|z\rangle| \\ & \geq & \cos(\varphi)\,. \end{array}$$

This can be seen by writing $|z\rangle$ as

$|\Psi_{-\varphi}\rangle \oplus |\Psi_0\rangle \oplus |\Psi_\varphi\rangle$, where $|\Psi_{-\varphi}\rangle, |\Psi_0\rangle$ and $|\Psi_\varphi\rangle$ are vectors in the eigenspaces of $U^\dagger R_o U$ corresponding to the eigenvalues $e^{-i\varphi}, 1$ and $e^{i\varphi}$, respectively. Therefore, we have

$$|\langle z|U^\dagger R_o U|z\rangle| = |pe^{-i\varphi} + qe^{i\varphi} + r|$$

with $p := \|\,|\Psi_{-\varphi}\rangle\|^2$, $q := \|\,|\Psi_0\rangle\|^2$ and $r := \|\,|\Psi_\varphi\rangle\|^2$. By elementary geometry the shortest vector in the convex span of the complex values $e^{-i\varphi}, 1, e^{i\varphi}$ has length $\cos(\varphi)$. This completes the proof $\Box$.

3 Low energy states with low complexity

The problem of determining the ground state energy and spectral gaps of many-particle systems is a highly non-trivial task. In [6] (based on results in [2]) it was shown that even the following instance is QMA-complete: Given a 3-local Hamiltonian, i.e., a selfadjoint operator on n-qubits which is a sum of operators that act on only 3 qubits. Furthermore, let the promise be given that either all eigenvalues of H are at least b or there exists an energy value smaller or equal to a. Decide which statement of both is true.

But there is a slightly different question which is interesting as well: It is to decide whether there exist states with energy at most a which are *simple* to prepare. Here simplicity will be defined by the number of required elementary gate operations. This problem arises naturally when one addresses the question whether extremely efficient cooling mechanisms could prepare states that are difficult to obtain with a reasonable number of quantum gates [7, 8].

Note that it is not clear that it should be easier to decide whether there exist low-complexity states with low energy than to decide whether low energy states (with energy at most a) do exist at all. In special instances one may possibly have arguments showing that low eigenvalues exist although one has no idea how to prepare them. However, here we show that the *problem class* of deciding whether a general 3-local Hamiltonian has low-energy states includes the problem of deciding whether there are low complexity low energy states. This follows from the fact that the first problem class is QMA and the latter one is QCMA.

Now we state the considered problem class formally.

Definition (Low complexity low energy states)
Let $\{H_x\}$ be a family of 3-local Hamiltonians acting on $n = poly(|x|)$ qubits, $\{a_x\}$ and $\{b_x\}$ two sequences of real numbers with $b_x - a_x \geq 1/poly(|x|)$ and $\{k_x\}$ a sequence of integers with $k_x = poly(|x|)$. Then the problem "low complexity low energy states" is to decide which one of the following cases is true given the promise that either of two holds:

1. There is a quantum circuit V_x of a most of k_x elementary gates (of the Shor basis [9]) such that
$$|\psi_x\rangle := V_x|0\dots 0\rangle$$
is a state with energy less than a, i.e.,
$$\langle\psi|H_x|\psi\rangle < a_x\,.$$
2. All quantum circuits V that consist of at most k gates can only prepare states $|\psi\rangle$ with energy at least b, i.e.,
$$\langle\psi|H_x|\psi\rangle > b\,.$$

We obtain the following theorem:

Theorem: The problem "low complexity low energy states" is QCMA-complete.

Proof: It is easy to see that the problem is in QCMA: the witness is a classical string describing the preparation procedure composed of at most k elementary gates. The fact that the so prepared state $|\psi\rangle$ is indeed a state with energy not greater than a can be checked as in [2].

Now we show that the problem encompasses QCMA. We consider a quantum circuit U and the task is to decide whether there is a basis state that is accepted with high probability. Let n be the number of qubits of the input register and m be the number of ancilla qubits. Then we construct a circuit $\tilde{U}$ with n input qubits and $n+m$ ancillas as follows: n C-NOT gates copy the input to the n additional ancillas. It is easy to see that $\tilde{U}$ has a state that is accepted with high probability if and only if U accepts a basis state with high probability.

Now we use the construction of [6] and obtain a 3-local Hamiltonian H associated with $\tilde{U}$. Let L be the number of gates of $\tilde{U}$. The exact form of H is not important here, we only rephrase the following four results of [6, 2] which are necessary for our proof:

1. The Hamiltonian corresponding to $\tilde{U}$ acts on $\tilde{n}+\tilde{m}+L$ qubits where $\tilde{n}+\tilde{m}$ is the size of the register where $\tilde{U}$ acts on (the input is an $\tilde{n}$-qubit state and the ancilla register of $\tilde{U}$ consists of $\tilde{m}$ qubits. The additional register with size L is a so-called "clock" register. Its role is not relevant here.

2. Whenever the circuit $\tilde{U}$ rejects all states with probability at least $1-\epsilon$ there is no eigenvalue of H smaller or equal to c/L^3 for an appropriate constant c.

3. If the state $|\psi\rangle$ is accepted by $\tilde{U}$ with probability $1-\epsilon$ the state
$$|\eta\rangle := \frac{1}{\sqrt{L+1}}\sum_{j=0}^{L} U_j \cdots U_1(|\psi\rangle \otimes |0\dots 0\rangle) \otimes |2^j - 1\rangle$$
is a low energy state, i.e.,
$$\langle\eta|H|\eta\rangle \leq \frac{\epsilon}{L+1}\,.$$

4. In case that the "confidence value" ϵ is too large such that $\epsilon/(L+1) \geq c/L^3$ or the gap between both values is too small, one may use probability amplification [2] and define a new circuit $\tilde{U}'$. This circuit is given by many parallel implementations of $\tilde{U}$ with majority vote in the end such the promise in Definition 1 holds for a smaller value ϵ'. Then the method of [6] is applied to obtain a Hamiltonian H corresponding to $\tilde{U}'$ such that $\epsilon/(L+1)$ is sufficiently smaller than c/L^3.

Consider the case that there is no basis state input of U that is accepted with probability greater than ϵ. Then there is also no input state at all that is accepted by $\tilde{U}$ with probability greater than ϵ. As rephrased above, there is no eigenvalue of H smaller than c/L^3.

Consider the case that there is a basis state $|x\rangle$ that is accepted by U with probability at least $1-\epsilon$. It is accepted by $\tilde{U}$ with the same probability. Then the state $|\eta\rangle$ defined above is a low energy state. It can be prepared efficiently, i.e. there is a polynomial p such that $|\eta\rangle$ can be obtained by $p(|x|)$ elementary gates. We omit technical details but it is not difficult to show that the superposition
$$\frac{1}{\sqrt{L+1}}\sum_{j=0}^{L} |2^j - 1\rangle$$

can be prepared efficiently. By applying $L+1$-fold controlled U_j-gates one obtains the state $|\eta\rangle$.

The question whether there is a low energy state that can be prepared with at most $p(|x|)$ elementary gates is hence equivalent to the question whether there is a basis state that is accepted by U□.

4 Remark on other problems in QCMA

To find simple procedures for preparing certain entangled multi-particle states from unentangled initial states is an interesting question of quantum information theory. Once one has found a procedure that prepares a desired state $|\psi\rangle$ from the state $|0\ldots0\rangle$, for instance, one may want to know whether there is also a simpler way to prepare $|\psi\rangle$.

Hence the following type of problems seems natural: Given a classical description of a quantum circuit U, decide whether there is also a simpler preparation procedure for $|\psi\rangle := U|0\ldots0\rangle$ in the following sense:

1. Given an elementary set of universal quantum gates. Decide whether there exists a quantum circuit V consisting of at most k gates preparing almost the same state (norm difference at most $1-\delta$) or all states prepared using at most k gates have at least the norm distance $1-\mu$ from $|\psi\rangle$

2. Let l and T be given, decide whether there is a l-local Hamiltonian preparing $|\psi\rangle$ approximatively by its autonomous evolution within the time T, i.e.,

$$\exp(-iHt)|0\ldots0\rangle$$

   is almost the same state as $|\psi\rangle$ for an appropriate value $t \leq T$.

3. Consider the control-theoretic setting as, for instance, the one appearing in NMR-experiments [10]: Given a pair-interaction Hamiltonian H and a maximal running time T. Let a state $|\Psi\rangle$ be specified by a quantum circuit as above, decide if it is possible to intersperse the natural time-evolution by at most k fast local operations (i.e. one-qubit rotations) such that the resulting unitary prepares the desired state such that the maximal running time T is not exceeded.

These types of problems are clearly in QCMA when the desired accuracies are defined as in Definition 1 since the proof consists of a classical description of the preparation procedure (i.e. the gate sequence, the Hamiltonian or the control sequence). The verifier can check that the procedure does indeed prepare the desired state by simulating the described preparation procedure on a quantum computer and applying $U^\dagger$. Then he measures the obtained state in the computational basis.

We do not know whether these problems are contained in any lower complexity class.

Acknowledgments

This work was supported by the BMBF-project 01/BB01B.

References

1. L. Babai and S. Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.
2. A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47. Am. Math. Soc., Providence, Rhode Island, 2002.
3. D. Aharonov and T. Naveh. Quantum NP - a survey. *quant-ph/0210077*.
4. D. Janzing, P. Wocjan, and T. Beth. "Identity check" is QMA-complete. *quant-ph/0305050*.
5. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. Roy. Soc. London A*, 454:339–354, 1998.
6. J. Kempe and O. Regev. 3-local Hamiltonian is QMA-complete. *quant-ph/0302079*, 2003.
7. B. Terhal and D. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer. *quant-ph/9810063*.
8. D. Aharonov and A. Ta-Shma Adiabatic quantum state generation and statistical zero knowledge. *quant-ph/0301023*.
9. P. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing: A novel basis and a new constructive proof of universality for Shor's basis. *Proceedings of the 40th Annual Symposium on foundations of Computer Science*, pages 486–494, 1999.
10. N. Khaneja, R. Brockett, and S. Glaser Time optimal control in spin systems. *Phys. Rev. A*, 63(3):032308–1–13, 2001.