ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 320 (2004) 15–33

Theoretical Computer Science

www.elsevier.com/locate/tcs

Quantum computing without entanglement☆

Eli Biham[a], Gilles Brassard[b], Dan Kenigsberg[a], Tal Mor[a]

[a] *Computer Science Department, Technion, Haifa 32000, Israel*

[b] *Département d'informatique et de recherche opérationnelle, Université de Montréal, Montréal, Qué., Canada, H3C 3J7*

Abstract

It is generally believed that entanglement is essential for quantum computing. We present here a few simple examples in which quantum computing *without* entanglement is better than anything classically achievable, in terms of the reliability of the outcome after a fixed number of oracle calls. Using a separable (that is, unentangled) state, we show that the Deutsch–Jozsa problem and the Simon problem can be solved more reliably by a quantum computer than by the best possible classical algorithm, even probabilistic. We conclude that: (a) entanglement is not essential for quantum computing; and (b) some advantage of quantum algorithms over classical algorithms persists even when the quantum state contains an arbitrarily small amount of information—that is, even when the state is arbitrarily close to being totally mixed.

Keywords: Quantum computation, Entanglement, Pseudo-pure states

1. Introduction

Quantum computing is a new fascinating field of research in which the rules of quantum mechanics are used to solve various computing problems more efficiently than any classical algorithm could do [16,13]. This has been rigourously demonstrated in oracle settings [2] and there is significant evidence that it is true in unrelativized

☆ The work of E.B., D.K. and T.M. is supported in parts by the Israel MOD Research and Technology Unit. The work of E.B. is supported in parts also by the fund for the promotion of research at the Technion, and by the European Commission through the IST Programme under contract IST-1999-11234. The work of T.M. is supported in parts also by the Institute for Futer Defense Research and by the Israel Science Foundation – FIRST (grant#4088103). The work of G.B. is supported in parts by Canada's NSERC, Québec's FQRNT, The Canada Research Chair Programme, the Canadian Institute for Advanced Research and the MITACS Network of Centres of Excellence.

E-mail addresses: biham@cs.technion.ac.il (E. Biham), brassard@iro.umontreal.ca (G. Brassard), danken@cs.technion.ac.il (D. Kenigsberg), talmo@cs.technion.ac.il (T. Mor).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2004.03.041

cases as well [20]. The quantum unit of information is called the *qubit*. In addition to the "classical" states $|0\rangle$ and $|1\rangle$, a qubit can be in any superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\cdot\rangle$ is the standard Dirac notation for quantum states, and α and β are complex numbers subject to $|\alpha|^2 + |\beta|^2 = 1$. For instance, $|\pm\rangle = \frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle$ and $|\pm_i\rangle = \frac{1}{\sqrt{2}}|0\rangle \pm \frac{i}{\sqrt{2}}|1\rangle$ are some specific pure states that we shall use later on. When n qubits are used, their state can be in a superposition of all "classical" n-bit states, that is, $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i|i\rangle$, where i is written in binary representation and $\sum_i |\alpha_i|^2 = 1$. These states are called *pure states*.

If qubits $|\psi\rangle$ and $|\varphi\rangle$ are in states $\alpha|0\rangle + \beta|1\rangle$ and $\gamma|0\rangle + \delta|1\rangle$, respectively, the state of a two-qubit system composed of those two qubits is given by their *tensor product*:

$$|\psi\rangle \otimes |\varphi\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \tag{1}$$

This notion generalizes in the obvious way to the tensor product of arbitrarily many quantum systems. Perhaps the most nonclassical aspect of quantum information processing stems from the fact that not all two-qubit states can be written in the form of Eq. (1). For instance, the states $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle$ and $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle$, known as the *Bell states*—or perhaps more appropriately the Braunstein–Mann–Revzen states [5]—do not factor out as a tensor product. In general, state $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ can be written in the form of Eq. (1) if and only if $ad = bc$. Multiple-qubits pure states that can be written as a tensor product of the individual qubits are said to be *separable*, or *product* states. Otherwise they are *entangled.*

When information is lacking about the state of a qubit, we say that this qubit is in a *mixed state*. This is described by a matrix $\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$, called the *density matrix*, with p_j being the probability of each (pure) state $|\psi_j\rangle$. The representation of ρ as a sum is not unique. For instance, an equal mixture of $|\psi_+(\theta)\rangle = (\cos\theta)|0\rangle + (\sin\theta)|1\rangle$ and $|\psi_-(\theta)\rangle = (\cos\theta)|0\rangle - (\sin\theta)|1\rangle$ is written as $\rho_\theta = \frac{1}{2}|\psi_+(\theta)\rangle\langle\psi_+(\theta)| + \frac{1}{2}|\psi_-(\theta)\rangle\langle\psi_-(\theta)|$. Simple algebra shows that this is in fact exactly the *same* as $(\cos^2\theta)|0\rangle\langle 0| + (\sin^2\theta)|1\rangle\langle 1|$, which is in general an unequal mixture of $|0\rangle$ and $|1\rangle$. A quantum mixed state ρ of several qubits is called a *product state* if it can be written as a tensor product of the states of the individual qubits, such as $\rho = \rho_A \otimes \rho_B$.

Recall that in the case of pure states, any product state is separable and any non-product state is entangled. The situation with mixed states is different—and more interesting—because there are separable states that are not product states. We say that a multiple-qubit mixed state is *separable* if it can be written as $\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$ such that each of the $|\psi_j\rangle$ is a separable pure state. Equivalently, a mixed state ρ is separable if it can be written in the form $\rho = \sum_j p_j\rho_j$ such that each of the ρ_j is a product state.

The intuition behind this definition is that a state (pure or mixed) is separable if and only if it can be prepared in remote locations with the help of classical communication only. For instance, Alice and Bob can remotely prepare the separable bipartite state $\frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|$ as follows. Alice tosses a fair coin and tells the outcome to Bob over a classical channel. If the coin comes up heads, Alice and Bob prepare their qubits in states $|0\rangle$ and $|1\rangle$, respectively; if it comes up tails, they prepare their qubits

in states $|1\rangle$ and $|0\rangle$. Then, *provided Alice and Bob forget the outcome of the coin*, they are left with the desired state.

If a mixed state is not separable, then we say that it is *entangled*. Deciding if a mixed state is entangled or separable is not an easy task in the general case because its representation is not unique. For instance, the state $\frac{1}{2}|\Psi^+\rangle\langle\Psi^+| + \frac{1}{2}|\Psi^-\rangle\langle\Psi^-|$ is separable, despite being a mixture of two entangled pure states, because it can be written equivalently as $\frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|$. As a more sophisticated example, a *Werner state* [23]

$$\chi = \lambda|\Psi^-\rangle\langle\Psi^-| + \frac{1-\lambda}{3}[|\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Phi^+\rangle\langle\Phi^+|],$$

which can also be written as

$$\chi = \varepsilon|\Psi^-\rangle\langle\Psi^-| + (1-\varepsilon)\,\mathrm{I}/4 \tag{2}$$

with $\varepsilon = (4\lambda - 1)/3$ and I a 4×4 identity matrix, is entangled if and only if $\lambda > \frac{1}{2}$, or equivalently $\varepsilon > \frac{1}{3}$. For $\lambda = \frac{1}{4}$ ($\varepsilon = 0$) the state is fully mixed, hence it contains no information. For $\lambda = \frac{1}{2}$ ($\varepsilon = \frac{1}{3}$) the state can be rewritten as

$$\begin{aligned}&\tfrac{1}{6}(|\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|) + \tfrac{1}{6}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-|)\\ &\quad + \tfrac{1}{6}(|\Phi^+\rangle\langle\Phi^+| + |\Psi^-\rangle\langle\Psi^-|),\end{aligned}$$

which makes its separability immediately apparent because

$$|\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-| = |+-\rangle\langle+-| + |-+\rangle\langle-+|$$

and

$$|\Phi^+\rangle\langle\Phi^+| + |\Psi^-\rangle\langle\Psi^-| = |+_i-_i\rangle\langle+_i-_i| + |-_i+_i\rangle\langle-_i+_i|.$$

Note that, although separable, this state is far from being classical, as only a nontrivial mixture of states written in different bases exposes its separability.

Quantum computers can manipulate quantum information by means of unitary transformations [13,16,8]. In particular, they can work with superpositions. For instance, a single-qubit Walsh–Hadamard operation H transforms a qubit from $|0\rangle$ to $|+\rangle$ and from $|1\rangle$ to $|-\rangle$. When H is applied to a superposition such as $|+\rangle$, it follows by the linearity of quantum mechanics that the resulting state is $\frac{1}{2}((|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)) = |0\rangle$. This illustrates the phenomenon of destructive *interference*, by which component $|1\rangle$ of the state is erased. Starting from an n-qubit quantum register initialized to $|0^n\rangle$, the application of a Walsh–Hadamard transform to each of these qubits yields an equal superposition of all n-bit classical states

$$|0^n\rangle \xrightarrow{\mathsf{H}} \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle.$$

Consider now a function $f:\{0,1\}^n \longrightarrow \{0,1\}$ that maps n-bit strings to a single bit. On a quantum computer, because unitary transformations are *reversible*, it is natural to

implement it as a unitary transformation U_f that maps $|x\rangle|b\rangle$ to $|x\rangle|b \oplus f(x)\rangle$, where x is an n-bit string, b is a single bit, and "$\oplus$" denotes the exclusive-or. Schematically,

$$|x\rangle|b\rangle \xrightarrow{U_f} |x\rangle|f(x) \oplus b\rangle. \tag{3}$$

The linearity of quantum mechanics gives rise to two important phenomena. (1) *Quantum parallelism*: We can compute f on arbitrarily many classical inputs by a single application of U_f to a suitable superposition:

$$\sum_x \alpha_x|x\rangle|b\rangle \xrightarrow{U_f} \sum_x \alpha_x|x\rangle|f(x) \oplus b\rangle.$$

When this is done, the additional output qubit may become entangled with the input register.

(2) *Phase kick-back*: The outcome of f can be recorded in the *phase* of the input register rather than being XOR-ed to the additional output qubit:

$$|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle, \quad \left(\sum_x \alpha_x|x\rangle\right)|-\rangle \xrightarrow{U_f} \left(\sum_x \alpha_x(-1)^{f(x)}|x\rangle\right)|-\rangle.$$

Much of the current interest in quantum computation was spurred by Peter Shor's momentous discovery that quantum computers can, in principle, factor large numbers and extract discrete logarithms in polynomial time [20] and thus break much of contemporary cryptography, such as the RSA cryptosystem [17] and the Diffie–Hellman public-key distribution system [10]. However, this does not provide a proven advantage of quantum computation because nobody knows for sure that these problems are genuinely hard for classical computers. On the other hand, it has been demonstrated that quantum computers can solve some problems exponentially faster than any classical computer provided the input is given as an *oracle* [9,2], and even if we allow bounded errors [21]. In this model, some function $f : \{0,1\}^n \to \{0,1\}$ is given as a black-box, which means that the only way to obtain knowledge about f is to query the black-box on chosen inputs. In the corresponding quantum oracle model, a function f is provided by a black-box that applies unitary transformation U_f to any chosen quantum state, as described by Eq. (3). The goal of the algorithm is to learn some property of the function.

A fundamental question is: where does the surprising computational advantage provided by quantum mechanics come from? What is the nonclassical property of quantum mechanics that leads to such an advantage? Do superposition and interference provide the quantum advantage? Probably the most often heard answer is that the power of quantum computing comes from the use of entanglement, and indeed there are very strong arguments in favour of this belief. (See [14,4,15,11,18] for a discussion.)

We show in this paper that this common belief is inaccurate. To this effect, we present two simple examples in which quantum algorithms are better than classical algorithms even when no entanglement is present. Furthermore, we show that quantum algorithms can be better than classical algorithms even when the state of the computer is almost totally mixed—which means that it contains an arbitrarily small amount of information.

The most usual measure of efficiency for computer algorithms is the amount of *time* required to obtain the solution, as a function of the input size. In the oracle setting, this usually means the number of queries needed to gain a predefined amount of information about the solution. Departing from this usual setting, we fix a maximum number of oracle calls and we try to obtain as much Shannon information as possible about the correct answer. In this model, we analyse two famous problems due to Deutsch–Jozsa [9] and Simon [21]. We show that, when a single oracle query is performed, the probability to obtain the correct answer is better for the quantum algorithm than for the optimal classical algorithm, and that the information gained by that single query is higher. This is true even when no entanglement is ever present throughout the quantum computation and even when the state of the quantum computer is arbitrarily close to being totally mixed. The case of more than one query is left for future research, as well as the case of a fixed *average* number of queries rather than a fixed *maximum* number. The quantum "advantage" we found exists for any size n of the problem but is exponentially small with n. The question of the existence of a non-negligible advantage of Quantum Computing Without Entanglement is left as our main open question.

2. Pseudo-pure states

To show that no entanglement occurs throughout our quantum computation, we use a special quantum state known as *pseudo-pure state* (PPS) [12]. This state occurs naturally in the framework of nuclear magnetic resonance (NMR) quantum computing [7], but the results presented in our paper are inherently interesting, regardless of the original NMR motivation. Consider any pure state $|\psi\rangle$ on n-qubits and some real number $0 \leqslant \varepsilon \leqslant 1$. A pseudo-pure state has the following form:

$$\rho_{\mathrm{PPS}}^{\{n\}} \equiv \varepsilon|\psi\rangle\langle\psi| + (1-\varepsilon)\mathscr{I}. \tag{4}$$

It is a mixture of pure state $|\psi\rangle$ with the totally mixed state $\mathscr{I} = (1/2^n)\mathrm{I}_{2^n}$ (where I_{2^n} denotes the identity matrix of order 2^n). For example, the Werner state (Eq. (2)) is a special case of a PPS.

To understand why these states are called *pseudo-pure*, consider what happens if a unitary operation U is performed on state $\rho = \rho_{\mathrm{PPS}}^{\{n\}}$ from Eq. (4).

Proposition 1. *The purity parameter ε of pseudo-pure states is conserved under unitary transformations.*

Proof. Since $\rho \xrightarrow{U} U\rho U^\dagger$ and $U\mathscr{I}U^\dagger = \mathscr{I}$,

$$U\rho U^\dagger = \varepsilon U|\psi\rangle\langle\psi|U^\dagger + (1-\varepsilon)U\mathscr{I}U^\dagger = \varepsilon|\varphi\rangle\langle\varphi| + (1-\varepsilon)\mathscr{I},$$

where $|\varphi\rangle = U|\psi\rangle$. In other words, unitary operations affect only the pure part of these states, leaving the totally mixed part unchanged and leaving the pure proportion ε intact. □

The main interest of pseudo-pure states in our context comes from the fact that there exists some bias ε below which these states are never entangled. The following theorem was originally proven in [4, Eq. (11)] but an easier proof was subsequently given in [19].

Theorem 2 ([4]). *For any number n of qubits, a state* $\rho_{\mathrm{PPS}}^{\{n\}}$ *is separable whenever*

$$\varepsilon < \frac{1}{1+2^{2n-1}}, \tag{5}$$

regardless of its pure part $|\psi\rangle$.

When $|\psi\rangle$ is entangled but $\rho_{\mathrm{PPS}}^{\{n\}}$ is separable, we say that the PPS exhibits *pseudo-entanglement*. (Please note that Eq. (5) is sufficient for separability but not necessary.) The key observation is provided by the Corollary below, whose proof follows directly from Theorem 2 and Proposition 1.

Corollary 3. *Entanglement will* never *appear in a quantum unitary computation that starts in a separable PPS whose purity parameter* ε *obeys Eq.* (5). *A final measurement in the computational basis will not make entanglement appear either.*

3. The Deutsch–Jozsa problem

The problem considered by Deutsch and Jozsa [9] was the following. We are given a function $f:\{0,1\}^n \to \{0,1\}$ in the form of an oracle (or a black-box), and we are promised that either this function is *constant*—$f(x)=f(y)$ for all x and y—or that it is *balanced*—$f(x)=0$ on exactly half the n-bit strings x. Our task is to decide which is the case. Historically, this was the first problem ever discovered for which a quantum computer would have an exponential advantage over any classical computer, in terms of computing time, provided the correct answer must be given with certainty. In terms of the number of oracle calls, the advantage is in fact much better than exponential: a single oracle call (in which the input is given in superposition) suffices for a quantum computer to determine the answer with certainty, whereas no classical computer can be sure of the answer before it has asked $2^{n-1}+1$ questions in the worst case. More to the point, no information *at all* can be derived from the answer to *a single* classical oracle call.

The quantum algorithm of Deutsch and Jozsa (DJ) solves this problem with a single query to the oracle by starting with state $|0^n\rangle|1\rangle$ and performing a Walsh–Hadamard transform on all $n+1$ qubits before and after the application of U_f. A measurement of the first n-qubits is made at the end (in the computational basis), yielding classical n-bit string z. By virtue of phase kickback, the initial Walsh–Hadamard transforms and

the application of U_f result in the following state:

$$|0^n\rangle|1\rangle \xrightarrow{\mathsf{H}} \left(\frac{1}{2^{n/2}}\sum_x |x\rangle\right)|-\rangle \xrightarrow{U_f} \left(\frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle\right)|-\rangle. \tag{6}$$

Then, if f is constant, the final Walsh–Hadamard transforms revert the state back to $\pm|0^n\rangle|1\rangle$, in which the overall phase is $+$ if $f(x)=0$ for all x and $-$ if $f(x)=1$ for all x. In either case, the result of the final measurement is necessarily $z=0$. On the other hand, if f is balanced, the phase of half the $|x\rangle$ in the right-hand side of Eq. (6) is $+$ and the phase of the other half is $-$. As a result, the amplitude of $|0^n\rangle$ is zero after the final Walsh–Hadamard transforms because each $|x\rangle$ is sent to $+|0^n\rangle/2^{n/2}+\cdots$ by those transforms. Therefore, the final measurement cannot produce $z=0$. It follows from the promise that if we obtain $z=0$ we can conclude that f is constant and if we obtain $z\neq 0$ we can conclude that f is balanced. Either way, the probability of success is 1 and the algorithm provides full information on the desired answer.

On the other hand, due to the nature of the DJ problem, a single classical query does not change our probability of guessing correctly whether the function is balanced or constant. Therefore the following proposition holds.

Proposition 4. *When restricted to a single DJ oracle call, a classical computer learns no information about the type of f.*

In sharp contrast, the following theorem shows the advantage of quantum computing even without entanglement.

Theorem 5. *When restricted to a single DJ oracle call, a quantum computer whose state is never entangled can learn a positive amount of information about the type of f.*

Proof. Starting with a PPS in which the pure part is $|0^n\rangle|1\rangle$ and its probability is ε, we can still follow the Deutsch–Jozsa strategy, but now it becomes a guessing game. We obtain the correct answer with different probabilities depending on whether f is constant or balanced. If f is constant, we obtain $z=0$ with probability

$$P(z=0\,|\,f \text{ is constant}) = \varepsilon + (1-\varepsilon)/2^n$$

because we started with state $|0^n\rangle|1\rangle$ with probability ε, in which case the Deutsch–Jozsa algorithm is guaranteed to produce $z=0$ since f is constant, or we started with a completely mixed state with complementary probability $1-\varepsilon$, in which case the Deutsch–Jozsa algorithm produces a completely random z whose probability of being zero is 2^{-n}. Similarly,

$$P(z\neq 0\,|\,f \text{ is constant}) = \frac{2^n-1}{2^n}(1-\varepsilon).$$

If f is balanced we obtain a non-zero z with probability

$$P(z \neq 0 \mid f \text{ is balanced}) = \varepsilon + \frac{2^n - 1}{2^n}(1 - \varepsilon),$$

and $z = 0$ is obtained with probability

$$P(z = 0 \mid f \text{ is balanced}) = (1 - \varepsilon)/2^n.$$

For all positive ε and all n, we still observe an advantage over classical computation. In particular, this is true for $\varepsilon \leqslant 1/(1 + 2^{2n+1})$, in which case the state remains separable throughout the entire computation (Eq. (5) with $n + 1$ qubits).

Let the a priori probability of f being constant be p (and therefore the probability that it is balanced is $1 - p$). The probability p_0 of obtaining $z = 0$ is $(1 - \varepsilon)/2^n + \varepsilon p$. We would like to quantify the amount of information we gain about the function, given the outcome of the measurement. In order to do this, we calculate the mutual information between X and Y, where X is a random variable signifying whether f is constant or balanced, and Y is a random variable signifying whether $z = 0$ or not. By definition, the *mutual information* between X and Y is the reduction of entropy of X due to learning Y. Mathematically,

$$I(X;Y) = h(P(X = \text{const})) - \sum_y P(Y = y) h(P(X = \text{const} \mid Y = y)),$$

where the *entropy function* of a probability q is defined as $h(q) = -q \lg q - (1 - q) \lg(1 - q)$. The detailed calculation of the mutual information is given in Appendix A.

To make the calculation more transparent we first present the natural case of $p = \frac{1}{2}$. Then, $p_0 = (1 - \varepsilon)/2^n + \varepsilon/2$, and the information gained by a single quantum query is

$$I(X;Y) = 1 - \frac{1 + \varepsilon(2^{n-1} - 1)}{2^n} h\left(\frac{1 + \varepsilon(2^n - 1)}{2(1 + \varepsilon(2^{n-1} - 1))}\right) - \frac{2^n - 1 - \varepsilon(2^{n-1} - 1)}{2^n} h\left(\frac{(\varepsilon - 1)(2^n - 1)}{2(1 + \varepsilon(2^{n-1} - 1) - 2^n)}\right) > 0. \tag{7}$$

The fact that $I(X;Y) > 0$ for all positive ε concludes the proof of the theorem. This is illustrated in Fig. 1 for the case $n = 10$. For a specific example, consider $n = 3$ and $\varepsilon = 1/(1 + 2^{2n+1}) = 1/129$. In this case, we gain 0.0000972 bits of information. □

For very small $\varepsilon \ll 1/2^n$, using the facts that $h(\frac{1}{2} + x) = 1 - 2x^2/\ln 2 + O(x^4)$ and $(1 + \varepsilon(2^n - 1))/2^n = 1/2^n + O(1/2^{n+1})$, the expression for the mutual information when $p = \frac{1}{2}$, as given by Eq. (7), can be approximated by

$$I(X;Y) = \frac{2^{2n}\varepsilon^2}{8(2^n - 1)\ln 2} + O(2^{2n}\varepsilon^3). \tag{8}$$

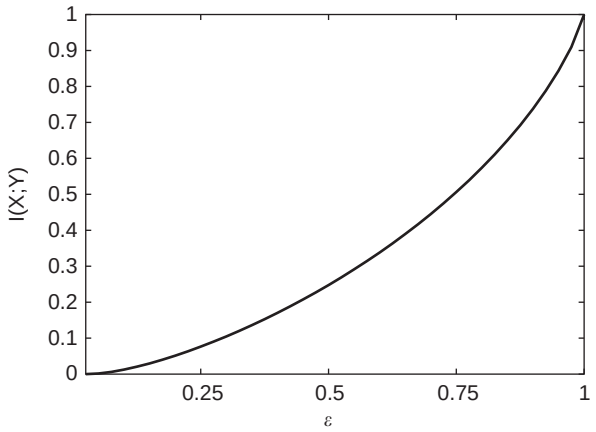

Fig. 1. Information gained by one quantum Deutsch–Jozsa query when the a priori probability of the function being balanced is $\frac{1}{2}$ and $n = 10$. Always positive, even for extremely small positive ε.

In the general case of $0 \leqslant p \leqslant 1$, the calculation is more cumbersome. It is shown in Appendix A that the information gained by a single quantum query is

$$I(X;Y) = h(p) - p_0 h\left(\frac{p}{p_0}\left(\varepsilon + \frac{1-\varepsilon}{2^n}\right)\right) - (1-p_0)\, h\left(\frac{p(1-\varepsilon)}{1-p_0}\left(1 - \frac{1}{2^n}\right)\right).$$

As shown by Fig. 2, the mutual information is positive for every $\varepsilon > 0$, unless $p = 0$ or $p = 1$. This is obviously more than the zero amount of information gained by a single classical query.

We conclude that some information is gained even for separable PPSs, in contrast to the classical case where the mutual information is always zero. Furthermore, some information is gained even when ε is arbitrarily small.

We can further improve the expected amount of information that is obtained by a single call to the oracle if we measure the $(n+1)$st qubit and take it into account. Indeed, this qubit should be $|1\rangle$ if the contribution comes from the pure part. Therefore, if that extra bit is $|0\rangle$, which happens with probability $(1-\varepsilon)/2$, we know that the PPS contributes the fully mixed part, hence no useful information is provided by z and we are no better than in the classical case. However, knowing that you do not know something is better than not knowing at all, because it makes the other case more revealing! Indeed, when that extra bit is $|1\rangle$, which happens with probability $(1+\varepsilon)/2$, the probability of the pure part is enlarged from ε to $\hat{\varepsilon} = 2\varepsilon/(1+\varepsilon)$, and the probability of the mixed part is reduced from $1-\varepsilon$ to $1-\hat{\varepsilon} = (1-\varepsilon)/(1+\varepsilon)$. The probability of

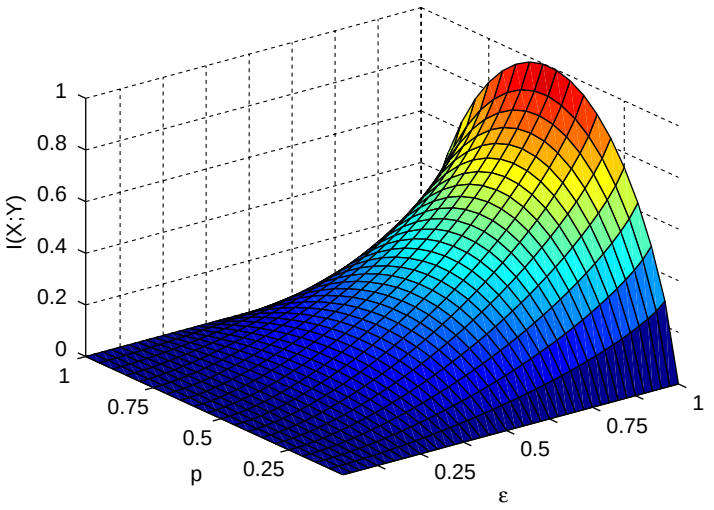

Fig. 2. Information gained by one quantum Deutsch–Jozsa query when $n=8$. Always positive for $0<p<1$, even for extremely small positive ε.

$z=0$ changes to $\hat{p}_0=(1-\hat{\varepsilon})/2^n+\hat{\varepsilon}p$, and the mutual information to

$$I(X;Y)=\frac{1+\varepsilon}{2}\left[h(p)-\hat{p}_0 h\left(\frac{p}{\hat{p}_0}\left(\hat{\varepsilon}+\frac{1-\hat{\varepsilon}}{2^n}\right)\right)\right.$$
$$\left.-(1-\hat{p}_0)\,h\left(\frac{p(1-\hat{\varepsilon})}{1-\hat{p}_0}\left(1-\frac{1}{2^n}\right)\right)\right]$$

which, for $p=\frac{1}{2}$ and very small ε, gives

$$I(X;Y)=\frac{2^{2n}\varepsilon^2}{4(2^n-1)\ln 2}+\mathrm{O}(2^{2n}\varepsilon^3).$$

This is essentially twice as much information as in Eq. (8). For the earlier specific example of $p=\frac{1}{2}$, $n=3$ and $\varepsilon=\frac{1}{129}$, this is 0.000189 bits of information.

4. The Simon problem

An oracle calculates a function $f(x)$ from n bits to n bits. We are promised that f is a two-to-one function, so that for any x there exists a unique $y\neq x$ such that $f(x)=f(y)$. Furthermore, we are promised the existence of an $s\neq 0$ such that $f(x)=f(y)$ for $x\neq y$ if and only if $y=x\oplus s$ (where $\oplus$ denotes the bitwise exclusive-or operator). The goal is to find s, while minimizing the number of times f is calculated.

Classically, even if one calls function f exponentially many times, say $2^{n/4}$ times, the probability of finding s is still exponentially small with n, that is less than $2^{-n/2}$. However, there exists a quantum algorithm that requires only $O(n)$ computations of f. The algorithm, due to Simon [21], is initialized with $|0^n\rangle|0^n\rangle$. It performs a Walsh–Hadamard transform on the first register and calculates f for all inputs to obtain

$$|0^n\rangle|0^n\rangle \xrightarrow{\mathsf{H}} \frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle \xrightarrow{U_f} \frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle,$$

which can be written as

$$\frac{1}{2^{n/2}} \sum_{x<x\oplus s} (|x\rangle + |x \oplus s\rangle)|f(x)\rangle.$$

Then, the Walsh–Hadamard transform is performed again on the first register (the one holding the superposition of all $|x\rangle$), which produces state

$$\frac{1}{2^n} \sum_{x<x\oplus s} \sum_j ((-1)^{j\cdot x} + (-1)^{j\cdot x\oplus j\cdot s})|j\rangle|f(x)\rangle,$$

where '$\cdot$' denotes the inner product modulo 2 between binary strings. Finally the first register is measured. Notice that the outcome j is guaranteed to be orthogonal to s ($j \cdot s = 0$) since otherwise $|j\rangle$'s amplitude $(-1)^{j\cdot x}(1 + (-1)^{j\cdot s})$ is zero. After an expected number of such queries in $O(n)$, one obtains n linearly independent j's that uniquely determine s.

Let S be a random variable that describes parameter s, and J be a random variable that describes the outcome of a single measurement. We would like to quantify how much information about S is gained by a *single* query. Assuming that S is distributed uniformly in the range $[1\,..\,2^n - 1]$, its entropy before the first query is $H(S) = \lg(2^n - 1) \approx n$. In the classical case, a single evaluation of f gives no information about S: the value of $f(x)$ on any specific x says nothing about its value in different places, and therefore nothing about s. However, in the case of the quantum algorithm, we are assured that s and j are orthogonal. If the measured j is zero, s could still be any one of the $2^n - 1$ non-zero values and no information is gained. But in the overwhelmingly more probable case that j is non-zero, only $2^{n-1} - 1$ values for s are still possible. Thus, given the outcome of the measurement, the entropy of S drops to approximately $n - 1$ bits and the expected information gain is nearly one bit (see Appendix B for a detailed calculation). More formally, based on the conditional probability

$$P(J = j \mid S = s) = \begin{cases} \dfrac{2}{2^n} & \text{if } j \cdot s = 0, \\ 0 & \text{if } j \cdot s = 1, \end{cases}$$

it follows that the conditional entropy $H(J \mid S = s) = n - 1$, which does not depend on the specific s and therefore $H(J \mid S) = n - 1$ as well. In order to find the a priori entropy

of J, we calculate its marginal probability

$$P(J=j)=\sum_s P(s)P(j|s),$$
$$=\begin{cases}\frac{1-\frac{2}{2^n}}{2^n-1} & \text{if } j\neq 0,\\ \frac{2}{2^n} & \text{if } j=0.\end{cases}$$

Thus,

$$H(J)=-\sum_j P(J=j)\lg P(J=j)=-\left(1-\frac{2}{2^n}\right)\lg\frac{1-\frac{2}{2^n}}{2^n-1}-\frac{2}{2^n}\lg\frac{2}{2^n}$$
$$=\left(1-\frac{2}{2^n}\right)\left(n+\lg\frac{2^n-1}{2^n-2}\right)+\frac{n-1}{2^{n-1}}$$

and the mutual information

$$I(S;J)=1-\frac{2-(2^n-2)\lg((2^n-1)/(2^n-2))}{2^n}=1-\mathrm{O}(2^{-n})$$

is almost one bit.

On the other hand, a single query to a classical oracle provides no information about s.

Proposition 6. *When restricted to a single oracle call, a classical computer learns no information about Simon's parameter s.*

Again in sharp contrast, the following theorem shows the advantage of quantum computing without entanglement, compared to classical computing.

Theorem 7. *When restricted to a single oracle call, a quantum computer whose state is never entangled can learn a positive amount of information about Simon's parameter s.*

Proof. Starting with a PPS in which the pure part is $|0^n\rangle|0^n\rangle$, and its probability is ε, the acquired j is no longer guaranteed to be orthogonal to s. In fact, an orthogonal j is obtained with probability $(1+\varepsilon)/2$ only. For any value of S, the conditional distribution of J is

$$P(J=j\,|\,S=s)=\begin{cases}\frac{1+\varepsilon}{2^n} & \text{if } j\cdot s=0,\\ \frac{1-\varepsilon}{2^n} & \text{if } j\cdot s=1,\end{cases}$$

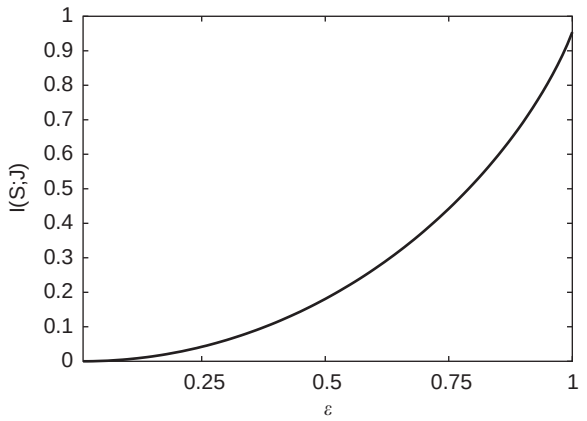

Fig. 3. Information gained by one quantum Simon query when $n = 10$. Always positive, even for extremely small positive ε.

from which we calculate (see Appendix B) that the information gained about S given the value of J is

$$I(S;J) = -\left(1 - \frac{1+\varepsilon}{2^n}\right) \lg \frac{1-(1+\varepsilon)/2^n}{2^n - 1} + (2^{n-1} - 1)\frac{1+\varepsilon}{2^n} \lg \frac{1+\varepsilon}{2^n} + \frac{1-\varepsilon}{2} \lg \frac{1-\varepsilon}{2^n} > 0.$$

Fig. 3 illustrates the fact that the amount of information is larger than the classical zero for every $\varepsilon > 0$.

This result applies even for ε as small as $1/(1 + 2^{4n-1})$, in which case the state of the computer is never entangled throughout the computation by virtue of Corollary 3. For example, when $n = 3$ and $\varepsilon = 1/(1 + 2^{4\times 3-1}) = 1/2049$, we gain 147×10^{-9} bits of information. □

5. Conclusions and directions for further research

We have shown that quantum computing without entanglement is more powerful than classical computing. We achieved this result by using two well-known problems due to Deutsch–Jozsa and to Simon, and by comparing quantum-without-entanglement to classical behaviour. Our measure of performance was the amount of Shannon information that can be obtained when a single oracle query is allowed.

In the paper [4] that gave us Theorem 2, Braunstein, Caves, Jozsa, Linden, Popescu and Schack claimed that "… current NMR experiments should be considered as simulations of quantum computation rather than true quantum computation, since no

entanglement appears in the physical states at any stage of the process".[1] Much to the contrary, we showed here that pseudo-entanglement is sufficient to beat all possible classical algorithms, which proves our point since pseudo-entangled states are *not* entangled! In conclusion, a few final remarks are in order:

- The quantum advantage that we have found is negligible (exponentially small). A much better advantage might be obtained by increasing ε and investigating the separability of the *specific* states obtained throughout the unitary evolution of the algorithms.
- The case of more than one query is left for future research.
- The case of a fixed *average* number of oracle calls, rather than a fixed *maximum* number of oracle calls, is also left for future research. Indeed, it was pointed out by Jozsa that a classical strategy can easily outperform our unentangled quantum strategy when solving the Deutsch–Jozsa problem if we restrict the number of oracle calls to be 1 on the average. For this, the classical computer tosses a coin. With probability $\frac{1}{2}$, it does not query the oracle at all and learns no information. But otherwise, also with probability $\frac{1}{2}$, it queries the oracle *twice* on random inputs and learns full information—that the function is balanced—if it obtains two distinct outputs. This happens with overall probability $\frac{1}{8}$ if the a priori probability of the function being balanced is $\frac{1}{2}$, which is much better than the exponentially small amount of information gleaned from our unentangled quantum strategy after one oracle call.
- What is the connection between this work and quantum communication complexity? (A survey of this topic can be found in [3].) Could quantum communication have an advantage over classical communication even when entanglement is not used?

Several papers dealing with speed-up and its connection to entanglement have been written, such as [1,14,6,22]. Let us mention two of these that appear at first to contradict our results: Jozsa and Linden [14] showed that for a large class of computational problems, entanglement *is* required in order to achieve an exponential advantage over classical computation *when the quantum state is pure throughout the computation*. Ambainis, Schulman and Vazirani [1] showed that quantum computation with a certain mixed state, other than the pseudo-pure state used by us, has no advantage over classical computation. But obviously, there is no real contradiction between our paper and these important results. We provide a case in which there exists a positive advantage of unentangled quantum computation over classical computation.

Appendix A. Details for the Deutsch–Jozsa problem

Figs. 4 and 5 describe the probability that zero (or non-zero) is measured, given a constant (or balanced) function, in the pure and the totally mixed cases. The case of pseudo-pure initial state is the weighted sum of the previous cases (see Fig. 6).

[1] Note, however, that later on Schack and Caves [18] qualified their earlier claim and stated that "... we speculate that the power of quantum-information processing comes not from entanglement itself, but rather from the information processing capabilities of entangling unitaries."

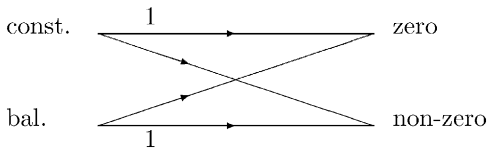

Fig. 4. Pure initial state.

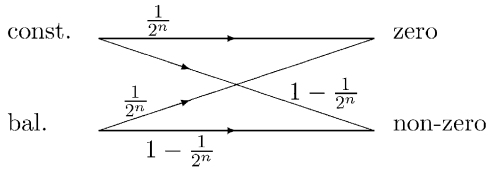

Fig. 5. Totally mixed initial state.

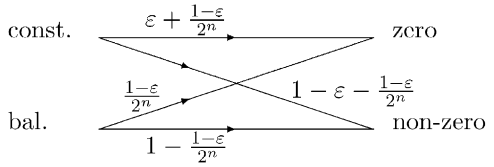

Fig. 6. Pseudo-pure initial state.

Table 1
Joint probability of function type (X) and measurement (Y)

X	$y=$ zero	$y=$ non-zero
const.	$p\left(\varepsilon+\frac{1-\varepsilon}{2^n}\right)$	$p(1-\varepsilon)\left(1-\frac{1}{2^n}\right)$
bal.	$(1-p)\frac{1-\varepsilon}{2^n}$	$(1-p)\left(1-\frac{1-\varepsilon}{2^n}\right)$
$P(Y=y)$	$p_0=p\varepsilon+\frac{1-\varepsilon}{2^n}$	$1-p_0$

The details of the pseudo-pure case are summarized in Table 1. The marginal probabilities of Y and X can be calculated from Table 1, and using Bayes rule, $P(X|Y)=P(Y|X)P(X)/P(Y)$, we find the conditional probabilities

$$P(X=\text{const}\,|\,Y=\text{zero})=\frac{p}{p_0}\left(\varepsilon+\frac{1-\varepsilon}{2^n}\right)$$

and

$$P(X = \text{const}|Y = \text{nonzero}) = \frac{p(1-\varepsilon)}{1-p_0}\left(1-\frac{1}{2^n}\right)$$

where $p_0 = P(Y = \text{zero}) = p\varepsilon + (1-\varepsilon)/2^n$. The conditional entropy is

$$\begin{aligned} H(X|Y) &= \sum_y P(Y=y)h(P(X=\text{const}|Y=y)) \\ &= p_0 h\left(\frac{p}{p_0}\left(\varepsilon+\frac{1-\varepsilon}{2^n}\right)\right) + (1-p_0)h\left(\frac{p(1-\varepsilon)}{1-p_0}\left(1-\frac{1}{2^n}\right)\right) \end{aligned}$$

and the mutual information is, therefore,

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= h(p) - p_0 h\left(\frac{p}{p_0}\left(\varepsilon+\frac{1-\varepsilon}{2^n}\right)\right) - (1-p_0)h\left(\frac{p(1-\varepsilon)}{1-p_0}\left(1-\frac{1}{2^n}\right)\right). \end{aligned}$$

For $p = \frac{1}{2}$ this reduces to

$$\begin{aligned} I(X;Y) = 1 &- \frac{1+\varepsilon(2^{n-1}-1)}{2^n} h\left(\frac{1+\varepsilon(2^n-1)}{2(1+\varepsilon(2^{n-1}-1))}\right) \\ &- \frac{2^n-1-\varepsilon(2^{n-1}-1)}{2^n} h\left(\frac{(\varepsilon-1)(2^n-1)}{2(1+\varepsilon(2^{n-1}-1)-2^n)}\right) > 0 \end{aligned}$$

and for very small $\varepsilon \ll 1/2^n$, using the fact that $h(\frac{1}{2}+x) = 1-(2x^2/\ln 2)+\mathrm{O}(x^4)$, this expression may be approximated by

$$\begin{aligned} I(X;Y) &= 1 - \frac{1+\varepsilon(2^{n-1}-1)}{2^n} h\left(\frac{1}{2}+\frac{2^n\varepsilon}{4}+\mathrm{O}(2^n\varepsilon^2)\right) \\ &\quad - \frac{2^n-1-\varepsilon(2^{n-1}-1)}{2^n} h\left(\frac{1}{2}-\frac{\varepsilon}{1-4/2^n}+\mathrm{O}(2^n\varepsilon^2)\right) \\ &= \frac{2^{2n}\varepsilon^2}{8(2^n-1)\ln 2} + \mathrm{O}(2^{2n}\varepsilon^3). \end{aligned}$$

Appendix B. Details for the Simon problem

Let S be a random variable that represents the sought-after parameter of Simon's function, so that $\forall x: f(x) = f(x \oplus s)$. Throughout this discussion, we assume that S is distributed uniformly in the range $[1..2^n-1]$. Given that $S = s$, and starting with a PPS whose purity is ε, one may find the distribution of the measurement after a single query. With probability ε we have started with the pure part and measured a j that is

orthogonal to s. With probability $1-\varepsilon$ we have started with the totally mixed state and measured a random j. Thus for j so that $j \cdot s = 0$, $P(J = j \mid S = s) = 2\varepsilon/2^n + (1-\varepsilon)/2^n$, and for j so that $j \cdot s = 1$, $P(J = j \mid S = s) = (1-\varepsilon)/2^n$. Putting this together,

$$P(J = j \mid S = s) = \begin{cases} \dfrac{1+\varepsilon}{2^n} & \text{if } j \cdot s = 0, \\ \dfrac{1-\varepsilon}{2^n} & \text{if } j \cdot s = 1. \end{cases}$$

The marginal probability of J for any $j \neq 0$ is

$$\begin{aligned} P(J = j) &= \sum_s P(s)P(j \mid s) \\ &= \frac{1}{2^n - 1}\left(\sum_{s \perp j} P(j \mid s) + \sum_{s \not\perp j} P(j \mid s)\right) \\ &= \frac{(2^{n-1}-1)(1+\varepsilon)/2^n + 2^{n-1}(1-\varepsilon)/2^n}{2^n - 1} \\ &= \frac{1-(1+\varepsilon)/2^n}{2^n - 1}, \end{aligned}$$

while for $J = 0$, all values of s are orthogonal, and

$$\begin{aligned} P(J = 0) &= \sum_s P(s)P(J = 0|s) \\ &= \frac{1}{2^n - 1}\sum_{s \perp j} P(J = 0|s) \\ &= \frac{1}{2^n - 1}(2^n - 1)\frac{1+\varepsilon}{2^n} \\ &= \frac{1+\varepsilon}{2^n}. \end{aligned}$$

By definition, the entropy of the random variable J is

$$\begin{aligned} H(J) &= -\sum_j P(J = j)\lg P(J = j) \\ &= -\left(1 - \frac{1+\varepsilon}{2^n}\right)\lg\frac{1-(1+\varepsilon)/2^n}{2^n - 1} - \frac{1+\varepsilon}{2^n}\lg\frac{1+\varepsilon}{2^n} \end{aligned}$$

and the conditional entropy of J given $S = s$ is

$$H(J \mid S = s) = -\sum_j P(J = j \mid S = s)\lg P(J = j \mid S = s)$$

$$= -2^{n-1}\,\frac{1+\varepsilon}{2^n}\lg\left(\frac{1+\varepsilon}{2^n}\right) - 2^{n-1}\,\frac{1-\varepsilon}{2^n}\lg\left(\frac{1-\varepsilon}{2^n}\right)$$

$$= -\frac{1+\varepsilon}{2}\lg\left(\frac{1+\varepsilon}{2^n}\right) - \frac{1-\varepsilon}{2}\lg\left(\frac{1-\varepsilon}{2^n}\right). \tag{B.1}$$

Since Eq. (B.1) is independent of the specific value s, it also equals $H(J\,|\,S)$, which is $\sum_s P(S=s)H(J\,|\,S=s)$. Finally, the amount of knowledge about S that is gained by knowing J is their mutual information:

$$I(S;J) = I(J;S) = H(J) - H(J|S)$$

$$= -\left(1 - \frac{1+\varepsilon}{2^n}\right)\lg\frac{1-(1+\varepsilon)/2^n}{2^n-1} + (2^{n-1}-1)\,\frac{1+\varepsilon}{2^n}\lg\frac{1+\varepsilon}{2^n}$$

$$+ \frac{1-\varepsilon}{2}\lg\left(\frac{1-\varepsilon}{2^n}\right).$$

Notice the two extremes: in the pure case ($\varepsilon=1$), $I(S;J)=1-\mathrm{O}(2^{-n})$ and in the totally mixed case ($\varepsilon=0$), $I(S;J)=0$. Finally, it can be shown that for small ε

$$I(S;J) = \frac{(2^n-2)\,\varepsilon^2}{2(2^n-1)\ln 2} + \mathrm{O}(\varepsilon^3).$$

References

[1] A. Ambainis, L.J. Schulman, U.V. Vazirani, Computing with highly mixed states, Proc. 32nd Annu. ACM Symp. on the Theory of Computing, 2000, pp. 697–704.

[2] A. Berthiaume, G. Brassard, Oracle quantum computing, J. Modern Opt. 41 (12) (1994) 2521–2535.

[3] G. Brassard, Quantum communication complexity, Found. Phys. 33 (11) (2003) 1593–1616.

[4] S.L. Braunstein, C.M. Caves, R. Jozsa, N. Linden, S. Popescu, R. Schack, Separability of very noisy mixed states and implications for NMR quantum computing, Phys. Rev. Lett. 83 (1999) 1054–1057.

[5] S.L. Braunstein, A. Mann, M. Revzen, Maximal violation of Bell inequalities for mixed states, Phys. Rev. Lett. 68 (1992) 3259–3261.

[6] S.L. Braunstein, A.K. Pati, Speed-up and entanglement in quantum searching, Quantum Inform. Comp. 2 (2002) 399–409.

[7] D.G. Cory, A.F. Fahmy, T.F. Havel, Ensemble quantum computing by nuclear magnetic resonance spectroscopy, Proc. US Nat. Acad. Sci. 94 (1997) 1634–1639.

[8] D. Deutsch, Quantum computational networks, Proc. Roy. Soc. London A 425 (1989) 73–90.

[9] D. Deutsch, R. Jozsa, Rapid solution of problems by quantum computation, Proc. Roy. Soc. London A 439 (1992) 553–558.

[10] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory IT-22 (6) (1976) 644–654.

[11] A. Ekert, R. Jozsa, Quantum algorithms: entanglement enhanced information processing, Philos. Trans. Roy. Soc. London A 356 (1998) 1779–1782.

[12] N.A. Gershenfeld, I.L. Chuang, Bulk spin-resonance quantum computation, Science 275 (1997) 350–356.

[13] J. Gruska, Quantum Computing, McGraw-Hill, London, 1999.

[14] R. Jozsa, N. Linden, On the role of entanglement in quantum computational speed-up, Proc. Roy. Soc. London A 459 (2003) 2011–2032.

[15] N. Linden, S. Popescu, Good dynamics versus bad kinematics: is entanglement needed for quantum computation?, Phys. Rev. Lett. 87 (2001) 047901.
[16] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2000.
[17] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Comm. ACM 21 (2) (1978) 120–126.
[18] R. Schack, C.M. Caves, Classical model for bulk-ensemble NMR quantum computation, Phys. Rev. A 60 (1999) 4354–4362.
[19] R. Schack, C.M. Caves, Explicit product ensembles for separable quantum states, J. Modern Opt. 47 (2000) 387–399.
[20] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484–1509.
[21] D.R. Simon, On the power of quantum computation, SIAM J. Comput. 26 (1997) 1474–1483.
[22] G. Vidal, Efficient classical simulation of slightly entangled quantum computations, Phys. Rev. Lett. 91 (14) (2003) 14.
[23] R.F. Werner, Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model, Phys. Rev. A 40 (8) (1989) 4277–4281.