Formation of multipartite entanglement using random quantum gates

Yonatan Most, Yishai Shimoni, and Ofer Biham

Racah Institute of Physics, The Hebrew University, Jerusalem 91904, Israel

(Received 11 June 2007; published 23 August 2007)

The formation of multipartite quantum entanglement by repeated operation of one- and two-qubit gates is examined. The resulting entanglement is evaluated using two measures: the average bipartite entanglement and the Groverian measure. A comparison is made between two geometries of the quantum register: a one-dimensional chain in which two-qubit gates apply only locally between nearest neighbors and a nonlocal geometry in which such gates may apply between any pair of qubits. More specifically, we use a combination of random single-qubit rotations and a fixed two-qubit gate such as the controlled-phase gate. It is found that in the nonlocal geometry the entanglement is generated at a higher rate. In both geometries, the Groverian measure converges to its asymptotic value more slowly than the average bipartite entanglement. These results are expected to have implications on different proposed geometries of future quantum computers with local and nonlocal interactions between the qubits.

PACS number(s): 03.67.Lx, 03.67.Mn, 89.70.+c

I. INTRODUCTION

Quantum algorithms such as Shor's factoring algorithm [1] and Grover's search algorithm [2,3] exemplify the potential speedup offered by quantum computers. Although the origin of this speedup is not fully understood, there are indications that quantum entanglement plays a crucial role [4–6]. Therefore, it is of interest to quantify the entanglement of the quantum states of multiple qubits that appear in quantum algorithms, using suitable measures. The special case of bipartite entanglement has been studied extensively in recent years and was established as a resource for quantum teleportation. The entanglement of pure bipartite states is completely determined by their Schmidt coefficients. Thus, any measure of bipartite entanglement must be a function of these coefficients. For example, the von Neumann entropy is expressed in terms of the eigenvalues of the reduced density matrix, which are the squares of the Schmidt coefficients. For mixed bipartite states, several measures were proposed, namely, the entanglement of formation and the entanglement of distillation [7,8]. In particular, for states of two qubits an exact formula for the entanglement of formation was obtained [9,10]. The more general case of multipartite entanglement, in a register of $n > 2$ qubits, is not as well understood, partly because no analog of the Schmidt decomposition was found for multipartite systems. Axiomatic considerations have provided a set of properties that entanglement measures should satisfy [11–14]. These properties include the requirement that any entanglement measure should vanish for product (or separable) states; it should be invariant under local unitary operations and should not increase as a result of any sequence of local operations complemented by only classical communication between the parties. Quantities that satisfy these properties are called entanglement monotones. These properties provide useful guidelines in the search for entanglement measures for multipartite quantum states. Entanglement measures based on metric properties of the Hilbert space [11,12,15] and on polynomial invariants [16,17] were proposed and shown to satisfy these requirements. Although some measures have been studied extensively, the connection between such measures and the efficiency of quantum algorithms remains unclear.

The common framework of quantum computation is based on a universal set of one and two qubit gates [18,19]. Repeated operations of these gates enable to obtain any desired quantum state of the register. To generate multipartite entanglement encompassing all the qubits in a register, one applies a series of two qubit gates between pairs of qubits, in addition to single qubit gates. One can visualize this process as a network in which the qubits are represented by nodes and two qubit operations are represented by edges that connect the corresponding nodes. Quantum entanglement is transitive in the sense that if we apply a gate that entangles qubits i and j and then a gate that entangles qubits j and k, this typically also gives rise to entanglement between qubits i and k. By entanglement between qubits i and k we mean that any two parties, each including one of these qubits, cannot be in a product state with each other. Thus, in order for the entanglement to encompass all the qubits in the register, the nodes associated with any pair of qubits must be connected, either directly or indirectly.

In recent years, several possible implementations of quantum computers have been proposed. In some of these schemes the interactions between qubits are nonlocal in the sense that two-qubit gates may apply between any pair of qubits. Other schemes are based on a rigid geometry in which only nearest-neighbor qubits may interact. In particular, they may be arranged in a one-dimensional chain, similar to solid state quantum computers using quantum dots [20]. In a one-dimensional geometry, two-qubit gates may apply on only $n-1$ or n pairs of qubits (depending on the boundary conditions), out of the $n(n-1)/2$ possible pairs. It is interesting to examine to what extent the geometrical restriction reduces the efficiency of the quantum computer. This limitation was addressed in the context of certain quantum algorithms [21–26].

In this paper we consider the rate of formation of multipartite entanglement in a register of n qubits by repeated operations of one and two-qubit gates. Starting from a product state, we repeatedly apply a combination of random

single qubit rotations and a fixed two-qubit gate on pairs of qubits. Two geometries are considered: a nonlocal geometry in which any pair of qubits may interact with each other and a one-dimensional chain, in which two-qubit gates may apply only between nearest-neighbor qubits. The resulting entanglement is evaluated using two measures: the average bipartite entanglement [27–29] and the Groverian measure [30]. It is found that the nonlocal scheme is more effective, namely, it requires fewer steps to produce a certain level of multipartite entanglement compared to the local scheme.

The paper is organized as follows. The entanglement measures used in this paper are briefly presented in Sec. II. The entanglement generating schemes, with local and nonlocal geometries are shown in Sec. III. The simulations and results are presented in Sec. IV, followed by a discussion in Sec. V and a summary in Sec. VI.

II. ENTANGLEMENT MEASURES OF MULTIPLE QUBITS

A. The average bipartite entanglement measure

Consider a quantum register of n qubits in a pure state $|\psi\rangle$. The bipartite entanglement between a given qubit and all the other qubits is given by a single parameter [31], namely, all the entanglement monotones for such a partition are the same up to a monotonic function. One of these monotones is the largest eigenvalue P of the reduced density matrix ρ of the single qubit. This eigenvalue is also the square of the largest Schmidt coefficient. Another monotone is $\mathrm{Tr}(\rho^2) = P^2 + (1-P)^2$, which is a monotonically increasing function of P in the relevant interval $1/2 \le P \le 1$. To evaluate the entanglement in a register of n qubits we average this measure over all n choices of the single qubit, where ρ_i, $i = 1, 2, \ldots, n$ is the reduced density matrix of the ith qubit, obtained by taking a partial trace over all the other qubits. After a suitable normalization and shift, one obtains the entanglement measure [27,28]

$$Q(\psi) = 2 - \frac{2}{n}\sum_{i=1}^{n} \mathrm{Tr}(\rho_i^2). \tag{1}$$

This measure was used in order to evaluate the entanglement generated by repeated operations of random gates [29,32]. $Q(\psi)$ is an entanglement monotone only for the most refined partition, where each qubit is considered as a separate party. It is thus commonly considered as a measure of multipartite entanglement.

In fact, the measure $Q(\psi)$ essentially quantifies bipartite entanglement, which is averaged over n different partitions. In each partition, one party consists of a single qubit while the other party consists of $n-1$ qubits. One may define other partitions of the register into two parties, where one party includes k qubits and the other party includes $n-k$ qubits. For a given value of k, the entanglement measure is obtained by averaging $\mathrm{Tr}(\rho^2)$ over all possible partitions of this type. In a more general framework, the register can be partitioned into any number of parties between 2 and n [16,33].

B. The Groverian measure

Grover's algorithm performs a search for a marked element m in a search space D containing N elements [2,3]. We assume, for convenience, that $N = 2^n$, where n is an integer. This way, the elements of D can be represented by an n-qubit register $|x\rangle = |x_1, x_2, \ldots, x_n\rangle$ with the computational basis states $|i\rangle$, $i = 0, \ldots, N-1$. The meaning of marking the element m is that there is a function $f : D \to \{0,1\}$, such that $f = 1$ for the marked element, and $f = 0$ for the rest. To solve this search problem on a classical computer one needs to evaluate f for each element, one by one, until the marked state is found. In the worst case, this requires N evaluations of f. On a quantum computer, where f can be evaluated coherently, Grover's algorithm, represented by the unitary operator U_G, can locate a marked element using only $O(\sqrt{N})$ coherent queries of f [2,3]. The algorithm is based on a quantum oracle, with the ability to recognize the marked states [2,3]. Starting with the equal superposition state

$$|\eta\rangle = \sum_{i=0}^{N-1} |i\rangle \tag{2}$$

and applying the operator U_G, one obtains the state $U_G|\eta\rangle = |m\rangle + O(1/N)$, which is then measured. The success probability of the algorithm is almost unity. The adjoint equation takes the form $\langle\eta| = \langle m|U_G + O(1/N)$. If an arbitrary pure state $|\psi\rangle$ is used as the initial state instead of the state $|\eta\rangle$, the success probability is reduced to $P_s = |\langle m|U_G|\psi\rangle|^2 + O(1/N)$ or $P_s = |\langle \eta|\psi\rangle|^2 + O(1/N)$. The success probability is thus determined by the fidelity between $|\psi\rangle$ and $|\eta\rangle$ [30,34].

Consider Grover's search algorithm, in which an arbitrary pure state $|\psi\rangle$ is used as the initial state. Before applying the operator U_G, there is a preprocessing stage in which arbitrary local unitary operators $U_1, U_2, \ldots, U_n$ are applied on the n qubits in the register. These operators are chosen such that the success probability of the algorithm will be maximized. The maximal success probability is thus given by

$$P_{\max}(\psi) = \max_{U_1, U_2, \ldots, U_n} |\langle m|U_G(U_1 \otimes \cdots \otimes U_n)|\psi\rangle|^2, \tag{3}$$

which can be rewritten as

$$P_{\max}(\psi) = \max_{|\phi\rangle \in T} |\langle \phi|\psi\rangle|^2, \tag{4}$$

where T is the space of all tensor product states of the form $|\phi\rangle = |\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle$. The Groverian measure is given by $G(\psi) = \sqrt{1 - P_{\max}(\psi)}$ [30]. In the case of pure states, for which $G(\psi)$ is defined, it is closely related to the entanglement measure introduced in Refs. [11,12,15] for both pure and mixed states and was shown to be an entanglement monotone. Based on these results, it was shown [30] that $G(\psi) \ge 0$, with equality when $|\psi\rangle$ is a product state; $G(\psi)$ is invariant under local unitary operations and cannot be increased using local operations and classical communication. Therefore, $G(\psi)$ is an entanglement monotone for pure states. A related result was obtained in Ref. [35], where it was shown that the evolution of the quantum state during the iteration of Grover's algorithm corresponds to the shortest path in the Hilbert space using a suitable metric.

The Groverian measure was used in order to evaluate the entanglement generated by quantum algorithms such as Grover's algorithm [36] and Shor's algorithm [37]. It was also generalized to the case of mixed states [38] and to arbitrary partitions of the register [33]. Here we use a different version of the Groverian measure, referred to as the logarithmic Groverian measure, given by

$$G(\psi) = -\ln[P_{\max}(\psi)]. \tag{5}$$

This is an entanglement monotone because the logarithmic function is monotonically increasing and it vanishes for product states for which $P_{\max}=1$. Unlike the measure introduced in Ref. [30], which is restricted to the range of $[0, 1)$, the logarithmic Groverian measure may take values in the range $0 \le G(\psi) < \infty$. This enables one to better distinguish and compare between highly entangled states which involve a large number of qubits.

Furthermore, the logarithmic Groverian measure exhibits the additivity property described below. Consider the state $|\psi\rangle = |\psi_A\rangle |\psi_B\rangle$ where $|\psi_A\rangle$ and $|\psi_B\rangle$ are pure states of two different registers of n_A and n_B qubits, respectively, and $n_A + n_B = n$. One can express the product state $|\phi\rangle$ of n qubits in the form $|\phi\rangle = |\phi_A\rangle |\phi_B\rangle$, where $|\phi_A\rangle$ and $|\phi_B\rangle$ are product states of n_A and n_B qubits, respectively. Since $|\psi\rangle$ is a tensor product of $|\psi_A\rangle$ and $|\psi_B\rangle$, we obtain that $\langle\phi|\psi\rangle = \langle\phi_A|\psi_A\rangle\langle\phi_B|\psi_B\rangle$. Thus, using Eq. (4) we find that $P_{\max}(\psi) = P_{\max}(\psi_A) P_{\max}(\psi_B)$. As a result, the logarithmic Groverian measure satisfies

$$G(\psi) = G(\psi_A) + G(\psi_B). \tag{6}$$

The additivity enables one to compare between the entanglement in registers which include different numbers of qubits.

III. THE ENTANGLEMENT GENERATING SCHEME

To examine the rate of multipartite entanglement formation in quantum circuits we consider a scheme for the production of pseudorandom states of n qubits [29]. The number of random amplitudes in a random state of n qubits is exponential in n. While the randomization of the state of each qubit alone requires only linear resources, the formation of entanglement between them is more costly. Nevertheless, it can be achieved by a combination of random single-qubit gates and a fixed two-qubit gate, which apply repeatedly on pairs of qubits. It was shown that this rotate-entangle-rotate scheme provides pseudorandom states with only polynomial resources [29,39]. The random single qubit rotation is obtained using

$$U_1 = \begin{pmatrix} e^{2\pi i \gamma_1}\sqrt{1-x} & e^{2\pi i \gamma_2}\sqrt{x} \\ -e^{-2\pi i \gamma_2}\sqrt{x} & e^{-2\pi i \gamma_1}\sqrt{1-x} \end{pmatrix}, \tag{7}$$

where at each step x, γ_1, and γ_2 are drawn from a uniform distribution over the unit interval $[0, 1)$. This parametrization provides operators drawn uniformly from the Haar measure [40]. For the two-qubit gate, we use the controlled-phase gate [29]

$$U_2 = e^{i\pi/4 \sigma_z \otimes \sigma_z} \tag{8}$$

expressed in the canonical decomposition form given in Ref. [31]. This is a sensible choice because this operator can produce maximally entangled states.

The initial state of the entanglement generating scheme is a random product state $|\psi_0\rangle$ of n qubits, where the state of each qubit is drawn from a uniform distribution on the Bloch sphere. Each iteration of this scheme consists of the following operations.

(1) Choose a random pair of qubits i and j from the n qubits in the register. In the nonlocal scheme, any pair of qubits may be chosen with equal probabilities. In the local scheme the qubits are arranged in a one-dimensional chain with periodic boundaries and only nearest-neighbor pairs are chosen with equal probabilities.

(2) Apply the controlled phase operator on qubits i and j.

(3) Apply random single-qubit rotations, drawn uniformly from the Haar measure [40], on qubits i and j.

The state obtained after t iterations, or time steps, is denoted by $|\psi_t\rangle$. To examine the rate of entanglement formation and to compare between the two schemes, we evaluate the following three functions of $|\psi_t\rangle$: (a) the fidelity $F(\psi_0, \psi_t) = |\langle\psi_0|\psi_t\rangle|$, (b) the average bipartite entanglement $Q(\psi_t)$, and (c) the logarithmic Groverian measure $G(\psi_t)$. Unlike $Q(\psi_t)$ and $G(\psi_t)$ which are entanglement measures, $F(\psi_0, \psi_t)$ is not an entanglement monotone. To put it on a common footing with the Groverian measure, we define

$$K(\psi_0, \psi_t) = -\ln F(\psi_0, \psi_t), \tag{9}$$

which is a monotonically decreasing function of the fidelity and takes values between zero and infinity.

IV. SIMULATIONS AND RESULTS

Each simulation of the entanglement-generating scheme creates a series of quantum states $|\psi_t\rangle$, $t = 1, 2, \ldots$. We examine the variation of $K(\psi_0, \psi_t)$, $Q(\psi_t)$, and $G(\psi_t)$ vs t. Due to the random nature of the operations, these three functions strongly fluctuate when evaluated for a single run of the entanglement generating scheme. To reduce the noise and elucidate the systematic trends, we perform a large number of runs using different initial states $|\psi_0\rangle$ and calculate the averages $\langle K(\psi_0, \psi_t)\rangle$, $\langle Q(\psi_t)\rangle$, and $\langle G(\psi_t)\rangle$ vs t.

In Fig. 1 we present $\langle K(\psi_0, \psi_t)\rangle$ vs t averaged over 2000 realizations for the local scheme [Fig. 1(a)] and for the nonlocal scheme [Fig. 1(b)]. The sharp increase of $\langle K(\psi_0, \psi_t)\rangle$ is explained by the fact that the fidelity is highly sensitive not only to two-qubit operations but also to single-qubit operations. Hence, the first few steps of the scheme can decrease the fidelity substantially. To explain the overshot, notice that product states have smaller fidelity with each other than entangled states, since the fidelity of two product states is simply the multiplication of the fidelities of the tensor components (all smaller then 1). In the beginning of the scheme, the register is still nearly separable so its fidelity with the (also separable) initial state is smaller than when it is completely entangled. After a sufficient number of steps, the state of the register is uncorrelated with the input state and $\langle K(\psi_0, \psi_t)\rangle$
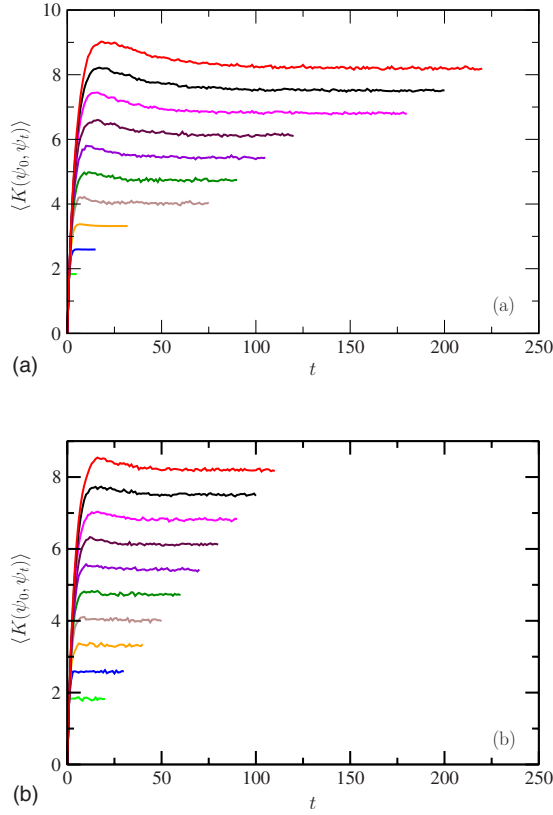
FIG. 1. (Color online) The average of $K(\psi_0,\psi_t)=-\ln F(\psi_0,\psi_t)$ vs time in the local scheme (a) and in the nonlocal scheme (b). The number of qubits in the register is $n=2,3,\dots,11$ qubits (from bottom to top).

saturates. As the number of qubits in the register increases, it takes more steps to bring $\langle K(\psi_0,\psi_t)\rangle$ to saturation. However, there is no significant difference between the two geometries.

The average bipartite entanglement $\langle Q(\psi_t)\rangle$ is shown in Fig. 2(a) for the local scheme and in Fig. 2(b) for the nonlocal scheme. It increases more slowly than $\langle K(\psi_0,\psi_t)\rangle$. The asymptotic value of $\langle Q(\psi_t)\rangle$ is the same for both geometries, but it is reached much faster in the nonlocal geometry than in the local one-dimensional geometry. The results for the one-dimensional geometry are consistent with those presented in Ref. [29]. The Groverian measure $G(\psi_t)$ vs t is shown in Figs. 3(a) and 3(b) for the local and nonlocal geometries, respectively. Clearly, $\langle G(\psi_t)\rangle$ converges to its asymptotic value more slowly than $\langle Q(\psi)\rangle$. The asymptotic value of $\langle G(\psi)\rangle$ is the same for both geometries but it is reached much faster in the nonlocal geometry.

The number of steps required for $\langle K(\psi_0,\psi_t)\rangle$, $\langle Q(\psi_t)\rangle$, and $\langle G(\psi_t)\rangle$, to reach 90% of their saturation values, vs n, is shown in Figs. 4(a), 4(b), and 4(c), respectively. The results for $\langle K(\psi_0,\psi_t)\rangle$ are almost identical in the local and nonlocal schemes. The time it takes $\langle Q(\psi_t)\rangle$, to reach 90% of its saturation values appears to be linear in n, for both geometries. However, the slope is lower for the nonlocal geometry, which means that the average bipartite entanglement builds up more quickly when nonlocal interactions are allowed. Similarly, in the nonlocal geometry the saturation time of
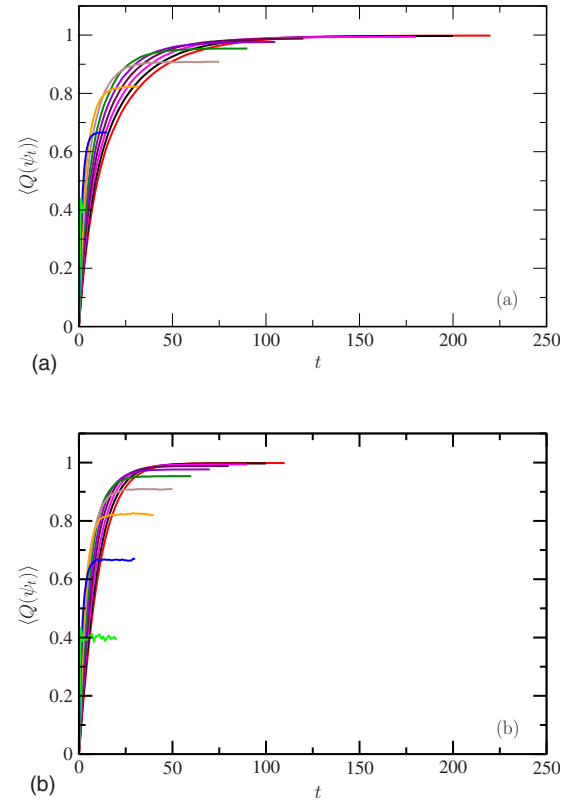

FIG. 2. (Color online) The average of the entanglement measure $Q(\psi_t)$ vs t in the local scheme (a) and in the nonlocal scheme (b), for a register with $2,3,\dots,11$ qubits, from bottom to top. Clearly, the entanglement builds up faster in the nonlocal scheme.

$\langle G(\psi)\rangle$ is linear in n. In the local geometry, the saturation time is longer, and deviates from linear dependence on n, and is well fitted by a quadratic function of n.

In the analysis above we focused on the averages of functions K, Q, and G. Each data point was obtained by averaging over at least 2000 runs of the entanglement forming procedure described above. These averages were taken from the distributions $f(K)$, $f(Q)$, and $f(G)$ for the quantum states $|\psi_t\rangle$ obtained after t iterations of the procedure. As t increases, these distributions are found to approach the distribution obtained for random states of the register [29]. In Fig. 5 we present the probability densities $f(G)$ of the Groverian measure $G(\psi_t)$ for $t=10$ (dashed-dotted line), 20 (dashed line), and 100 (solid line) steps, for a register with $n=8$ qubits. As the number of steps increases, these distributions approach the distribution $f(G)$ obtained for pseudorandom states of the eight-qubit register (dotted line).

These results indicate that building up bipartite as well as multipartite entanglement using two-qubit gates is more efficient when nonlocal interactions are allowed. Furthermore, in both geometries it seems that multipartite entanglement, evaluated by $G(\psi)$ builds up more slowly than the bipartite-like entanglement quantified by $Q(\psi)$.

V. DISCUSSION

Quantum algorithms are typically designed under the assumption that two-qubit operations are possible between any
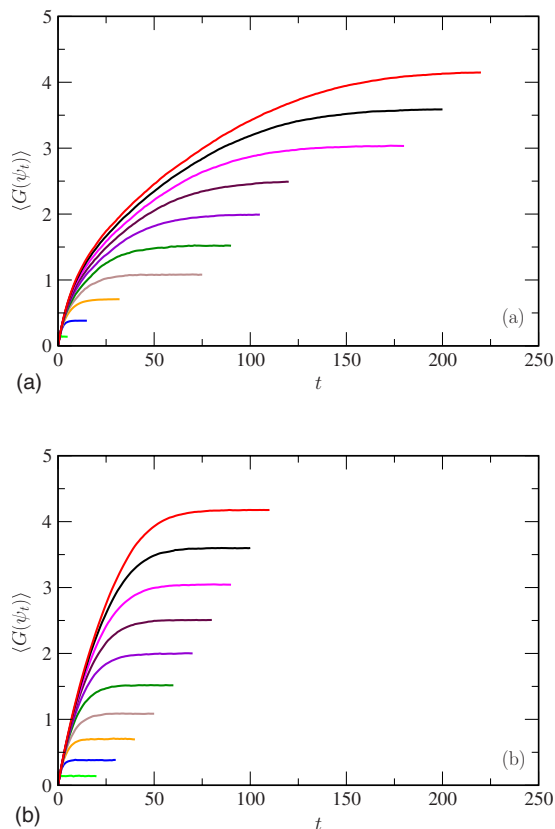
FIG. 3. (Color online) The average of the Groverian measure $G(\psi_t)$ vs t in the local scheme (a) and in the nonlocal scheme (b), for a register with $2,3,\ldots,11$ qubits. The Groverian measure increases faster in the nonlocal scheme.

FIG. 4. The number of steps required for the averages of $K(\psi_0,\psi_t)$ (a), $Q(\psi_t)$ (b), and $G(\psi_t)$ (c) to reach 90% of their saturation values in the local (+) and nonlocal (○) schemes vs the number of qubits in the register. While the results for $K(\psi_0,\psi_t)$ are nearly identical in both schemes, the time required for $Q(\psi_t)$ and $G(\psi_t)$ to converge is shorter in the nonlocal scheme. The solid lines are linear fits and the dashed line is a quadratic fit.

pair of qubits. However, some of the physical realizations of quantum computation allow only local interactions between neighboring qubits [20]. In these realizations, nonlocal operations are achieved using swap gates [21] which may involve a significant overhead [41]. To put the results of this paper in the context of known physical realizations, we briefly review below several such realizations and specify whether they are based on local or nonlocal interactions.

Ion-trap quantum computing devices [42,43] consist of laser-cooled ions, which are electromagnetically confined in ultrahigh vacuum. The spin states of the ions are used as qubits. Single-qubit gates are preformed by selectively applying electromagnetic fields on the different ions. Two-qubit gates are realized through a global phonon state, which makes use of the collective vibrational degree of freedom of the ions. The ground state and the first excited state of the phonon comprise a two-level system, which is used as an additional qubit. Using carefully tuned laser-induced transitions, two-qubit gates can be applied between each ion and the global phonon. Specifically, a swap gate can be applied between them, enabling one to apply two-qubit gates between any pair of qubits. Ion traps thus provide a nonlocal implementation of quantum computation. Linear optics provides another nonlocal realization of quantum computation [44,45].

Quantum computation can also be performed using solid-state devices [46,47]. Several proposals are comprised of qu-
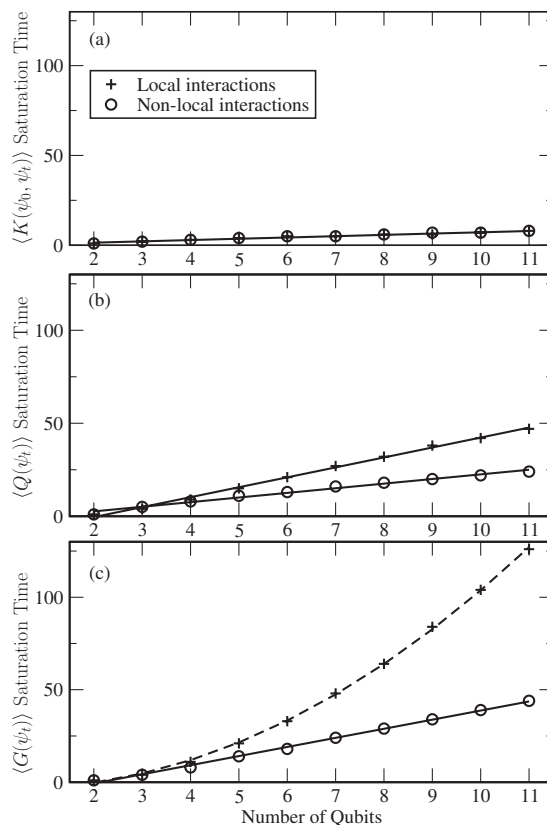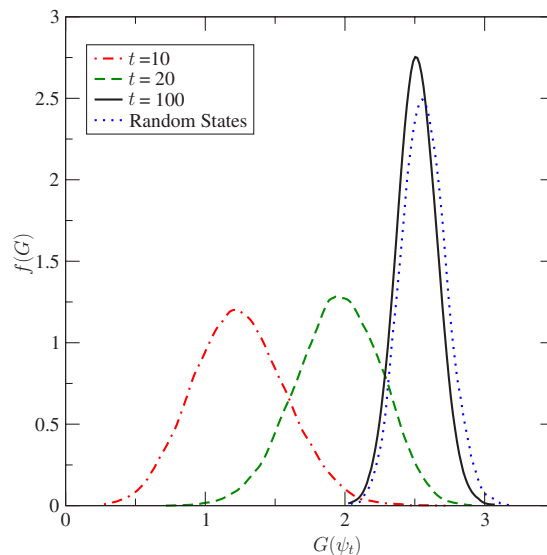

FIG. 5. (Color online) The probability density $f(G)$ of the Groverian measure $G(\psi_t)$ for the states obtained after $t=10$ (dashed-dotted line), 20 (dashed line), and 100 (solid line) iterations of the entanglement forming procedure, for $n=8$ qubits. As t increases, the distribution converges to the one obtained for pseudorandom states (dotted line).

bits based on superconducting Josephson junctions [48]. One such proposal uses the two states of a superconducting single-charge box as a charge qubit. The possibility of connecting all the qubits in parallel to an inductor-capacitor circuit (commonly referred to as an LC-oscillator) mode was suggested as a way to apply two-qubit gates [49]. This parallel connection, together with the ability to simultaneously control the Josephson coupling for each qubit, allows two-qubit interaction between any pair of qubits, giving rise to a nonlocal scheme. A different superconducting scheme is based on Josephson flux qubits, which interact through magnetic induction. Unlike the charge-qubit scheme, the flux-qubit scheme is a local one. Another implementation is based on electron spins as qubits, confined to quantum dots [50]. Two-qubit gates are applied using a time-dependent Heisenberg exchange coupling between adjacent dots, providing a local scheme for quantum computation. Solid-state realizations may be most suitable for scalable implementation of quantum computations. Some of these realizations are based on local interactions. Local interactions appear form multiple-qubit entanglement at a lower rate than nonlocal interactions. However, the connection between the entanglement as quantified by the Groverian and related measures and the speedup offered by quantum algorithms is not yet clear.

VI. SUMMARY

We have studied the formation of multipartite quantum entanglement by repeated operation of one- and two-qubit gates. The resulting entanglement was evaluated using the average bipartite and the Groverian measures. A comparison was made between two geometries of the quantum register: a nonlocal geometry in which any pair of qubits may interact and a local geometry in which the qubits are arranged in a one-dimensional chain, where only nearest-neighbor interactions are allowed. More specifically, we used a combination of random single qubit rotations and a fixed two-qubit operation, namely, the controlled phase gate. We found that in this scheme, entanglement is generated more quickly in the nonlocal geometry than in the one-dimensional chain. Thus, nonlocal implementations of quantum computation are expected to be more efficient in generating highly entangled states.

[1] P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994), p. 124.
[2] L. Grover, in *Proceedings of the Twenty-Eighth Annual Symposium on the Theory of Computing* (ACM, New York, 1996), p. 212.
[3] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[4] R. Jozsa and N. Linden, Proc. R. Soc. London, Ser. A **459**, 2011 (2003).
[5] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[6] D. Aharonov and M. Ben-Or, in *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1996), p. 46.
[7] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[9] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).
[10] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[11] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).
[12] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[13] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
[14] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).
[15] V. Vedral, M. B. Plenio, K. Jacobs, and P. L. Knight, Phys. Rev. A **56**, 4452 (1997).
[16] H. Barnum and N. Linden, J. Phys. A **34**, 6787 (2001).
[17] M. S. Leifer, N. Linden, and A. Winter, Phys. Rev. A **69**, 052304 (2004).
[18] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[19] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[20] D.P. DiVincenzo, Fortschr. Phys. **48**, 771 (2000).
[21] D. Aharonov and M. Ben-Or, in *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing*, El Paso, Texas, 1997 (ACM, New York, 1997), p. 176.
[22] D. Gottesman, J. Mod. Opt. **47**, 333 (1999).
[23] A. G. Fowler, C. D. Hill, and L. C. L. Hollenberg, Phys. Rev. A **69**, 042314 (2004).
[24] A. G. Fowler, S. J. Devitt, and L. C. L. Hollenberg, Quantum Inf. Comput. **4**, 237 (2004).
[25] M. Möttönen and J. J. Vartiainen, e-print arXiv:quant-ph/0504100.
[26] M. B. Plenio and F. L. Semião, New J. Phys. **7**, 73 (2005).
[27] D. A. Meyer and N. R. Wallach, J. Math. Phys. **43**, 4273 (2002).
[28] G. K. Brennen, Quantum Inf. Comput. **3**, 619 (2003).
[29] J. Emerson, Y. S. Winstein, M. Saraceno, S. Lloyd, and D. G. Cory, Science **302**, 2098 (2003).
[30] O. Biham, M. A. Nielsen, and T. J. Osborne, Phys. Rev. A **65**, 062312 (2002).
[31] B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001).
[32] Y. S. Weinstein and C. S. Hellberg, Phys. Rev. Lett. **95**, 030501 (2005).
[33] Y. Shimoni and O. Biham, Phys. Rev. A **75**, 022308 (2007).
[34] O. Biham, D. Shapira, and Y. Shimoni, Phys. Rev. A **68**, 022326 (2003).
[35] A. Miyake and M. Wadati, Phys. Rev. A **64**, 042317 (2001).
[36] Y. Shimoni, D. Shapira, and O. Biham, Phys. Rev. A **69**, 062303 (2004).
[37] Y. Shimoni, D. Shapira, and O. Biham, Phys. Rev. A **72**,

062308 (2005).

[38] D. Shapira, Y. Shimoni, and O. Biham, Phys. Rev. A **73**, 044301 (2006).

[39] R. Oliveira, O. C. O. Dahlsten, and M. B. Plenio, Phys. Rev. Lett. **98**, 130502 (2007).

[40] K. Życzkowski and M. Kuś, J. Phys. A **27**, 4235 (1994).

[41] N. Schuch and J. Siewert, Phys. Rev. A **67**, 032301 (2003).

[42] J. I. Cirac and P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).

[43] D. Kielpinski, J. Opt. B: Quantum Semiclassical Opt. **5**, 121 (2003).

[44] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[45] P. Kok, W. J. Munro, K. Nemoto, J. P. Dowling, and G. J. Milburn, Rev. Mod. Phys. **79**, 135 (2007).

[46] V. Cerletti, W. A. Coish, O. Gywat, and D. Loss, Nanotechnology **16**, R27 (2005).

[47] G. Burkard, e-print arXiv:cond-mat/0409626.

[48] Y. Makhlin, G. Schön, and A. Shnirman, Rev. Mod. Phys. **73**, 357 (2001).

[49] Y. Makhlin, G. Schön, and A. Shnirman, Nature (London) **398**, 305 (1999).

[50] D. Loss and D. P. DiVincenzo, Phys. Rev. A **57**, 120 (1998).