Efficient Generation of Generic Entanglement

R. Oliveira*
IBM Watson Research Center, Yorktown Heights, NY, USA 10598.

O.C.O. Dahlsten and M.B. Plenio†
Institute for Mathematical Sciences, Imperial College London, 53 Exhibition Rd, London SW7 2PG, UK and QOLS, Blackett Laboratory, Imperial College London, Prince Consort Rd, London SW7 2BW, UK

(Dated: December 16, 2006)

We find that generic entanglement is physical, in the sense that it can be generated in polynomial time from two-qubit gates picked at random. We prove as the main result that such a process generates the average entanglement of the uniform (Haar) measure in at most $O(N^3)$ steps for N qubits. This is despite an exponentially growing number of such gates being necessary for generating that measure fully on the state space. Numerics furthermore show a variation cut-off allowing one to associate a specific time with the achievement of the uniform measure entanglement distribution. Various extensions of this work are discussed. The results are relevant to entanglement theory and to protocols that assume generic entanglement can be achieved efficiently.

PACS numbers: 03.67.Mn, 05.70.-a

Introduction — Entanglement is a key resource in quantum information tasks. As a consequence, the quantitative exploration of entanglement as a resource is a central concern of quantum information science; see [1] for a recent review. While a great deal of insight into the structure of two-particle entanglement has been gained, it has become equally clear that the complexity and diversity of multi-particle entanglement grows exponentially with the number of particles. It is therefore difficult to imagine a structurally simple theory that perfectly characterizes and quantifies all details of multi-particle entangled states. On the other hand, it may be expected that a much simplified theory exists for the properties of generic quantum states if, in some appropriate sense, most states behave similarly. This intuition gives hope that significant progress can be made by restricting attention to classes that are typical (generic) relative to the uniform (Haar) measure. In fact, it was demonstrated that relative to the Haar measure, practically all pure states of large numbers of spins exhibit maximal bipartite [2, 3, 4, 5, 6] as well as multi-partite entanglement [2]. This suggests that the exploration of the entanglement properties of generic states is a promising approach. But a big question mark exists as to whether statements about generic states relative to the Haar measure are physical. This is because most unitaries are generated by a sequence of 2-qubit unitaries whose length grows exponentially in the number of qubits [7], even if one allows for a finite fixed fidelity. This implies that if we want to achieve the uniform distribution to a fixed accuracy, the number of applications of random 2-qubit unitaries necessary grows exponentially with the size of the system, and quickly becomes unphysical, see for example discussion in [8, 9, 10, 11]. It may therefore turn out that there is no efficient procedure for the generation of generic quantum states, leaving their properties mathematically sound and interesting but physically irrelevant. On the other hand, entanglement properties represent a restricted class of physical properties of a quantum state. Accordingly the faithful reproduction of generic entanglement properties may be possible with far fewer physical resources, i.e. 2-qubit gates, than those required for the precise generation of the expectation value for an arbitrary observable.

It is thus crucial to explore whether generic entanglement properties can be obtained efficiently, i.e. polynomially in the number of qubits, using only one- and two-qubit gates. The present work answers this question positively.

We prove that the number of steps necessary (c.f. Figure 1) to achieve the expected entanglement of the uniform Haar measure distribution is polynomial in the

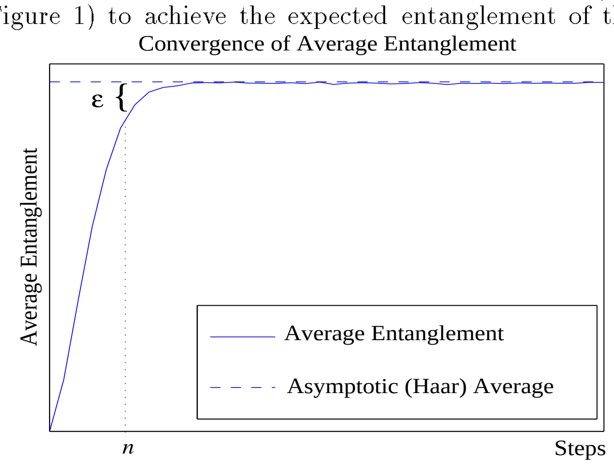

FIG. 1: Typical numerical simulation using the random circuit. The entanglement average of the Haar measure is reached to an accuracy ε in n steps. We prove that it suffices with $n = O(N^3)$ to achieve a fixed *arbitrary* ε accuracy when increasing N.

*Electronic address: riolivei@us.ibm.com
†Electronic address: oscar.dahlsten@ic.ac.uk, m.plenio@ic.ac.uk

number of qubits and therefore physical.

The results support the physical relevance of the exploration of generic entanglement towards a simplified entanglement theory and have direct practical relevance since certain quantum information processing protocols such as [2, 12, 13, 14] assume that generic entanglement can be generated efficiently.

The presentation proceeds as follows. We firstly define the key process that is used throughout this work: random two qubit interactions, modelled as random circuits on a quantum computer. We then prove that the generic entanglement average as well as the purity of a subsystem are achieved efficiently and that the so generated states are close to a maximally entangled state with high probability. In a second part of this work we give numerical evidence that the achievement of generic entanglement can be associated with a specific time, the variation cut-off, for large systems. We finish with a discussion and conclusion.

Definition of the random circuit – We consider N-qubit quantum circuits that are built from random two-qubit unitaries W chosen in the following way: A pair of distinct integers $c \neq t$ is chosen uniformly and at random from $\{1, \dots, N\}$. Next, single-qubit unitaries $U[c]$ and $V[t]$ acting on qubit c and t respectively are drawn independently from the Haar measure on $U(2)$. Then we set $W = CNOT[c,t]U[c]V[t]$ where $CNOT[c,t]$ is the controlled-NOT gate with control c and target t [21]. The circuit C_n is simply the product $W_n \cdot \dots \cdot W_1$, where each W_i is picked as W above, but with independent choices of c, t, U, V at each time.

Asymptotics of random circuit — The circuit, acting on N qubits, will asymptotically induce the uniform measure on states. See [8] for a detailed discussion. Now split the N qubits into two subsets A (with N_A qubits) and B with N_B qubits). Then, for states distributed according to the Haar measure the average bipartite entanglement can be found exactly [5, 6] and is bounded from below such that $\mathbb{E}[E(\psi_n)] \geq N_A - \frac{1}{ln 2}2^{-t}$ where $N_B - N_A = t \geq 0$ [2]. Likewise we find that the average purity of the subsystem A is given by $(2^{N_A} + 2^{N_B})/(2^N + 1)$ consistent with [10]. Furthermore, the distributions for entanglement and purity concentrate around their average with increasing N [2, 3, 4, 5, 6]. Thus one is overwhelmingly likely to find near-maximal entanglement for large systems. In the following however we will be concerned with the approach to the asymptotic regime.

Main Theorem — Consider a set of N-qubits split into two subsets A (with N_A qubits) and B (with N_B qubits). Let $|\psi_0\rangle$ be a initial state in AB and consider a random circuit C_n consisting of n randomly chosen two-qubit quantum gates. Define $|\psi_n\rangle = C_n|\psi_0\rangle$ and the reduced density matrix $\rho_{A,n} = Tr_B(|\psi_n\rangle\langle\psi_n|)$ of system A. Then the entanglement in the state is given by $E(\psi_n) = S(\rho_{A,n})$.

Our main rigorous result demonstrates that, independently of $|\psi_0\rangle$, convergence of the expected entanglement to its asymptotic value to an arbitrary fixed accuracy ε is achieved within the application of $n = O(N^3 + N^2 \ln \epsilon^{-1})$ random two-qubit gates. More precisely we find:

Theorem 1 *Suppose that $N_B - N_A = t \geq 0$ and that some arbitrary $\varepsilon \in (0,1)$ is given. Then for a number n of gates in C_n satisfying*

$$n \geq \frac{9N(N-1)[(4\ln 2)N + \ln \varepsilon^{-1}]}{4},$$

we have

$$\mathbb{E}[E(\psi_n)] \geq N_A - \frac{2^{-t} + \varepsilon}{\ln 2}.$$

as well as $\mathbb{E}[\max_{|\Psi\rangle_{AB} = maxent} |\langle\psi_n|\Psi\rangle|] = 1 - \sqrt{\frac{2^{-t}+\epsilon}{2\ln 2}}$

The last statement in Theorem 1 follows from the second directly from Corollary IV.1 in [2]. To prove the first part of Theorem 1 we proceed with the proof of a Lemma that considers the quantity $\mathbb{E}\left[Tr(\rho_{A,n}^2)\right]$.

Lemma 1 *For arbitrary N, N_A, N_B and all n we have*

$$\left|\mathbb{E}\left[Tr(\rho_{A,n}^2)\right] - \frac{2^{N_A} + 2^{N_B}}{2^N + 1}\right| \leq 8^N e^{-\frac{4n}{9N(N-1)}}.$$

Notice that $E(\psi_n) = S(\rho_{A,n}) \geq -\log_2 Tr(\rho_{A,n}^2)$ because the Rényi-2 entropy is bounded by $S(\rho_{A,n})$. By convexity we find $\mathbb{E}\left[-\log_2 Tr(\rho_{A,n}^2)\right] \geq -\log_2(\mathbb{E}\left[Tr(\rho_{A,n}^2)\right])$ and a direct computation using $\ln(1+x) \leq x$ for $x \geq 0$ shows that Lemma 1 implies Theorem 1. Therefore it only remains to be shown that Lemma 1 indeed holds.

We proceed to outline the proof of Lemma 1 below, omitting some tedious but straightforward calculations to enhance clarity.

Proof of Lemma 1 —We begin with a useful representation of quantum states in terms of Pauli-operators[21]. One can always write $|\psi_n\rangle\langle\psi_n| = \sum_{p\in\{0,x,y,z\}^N} \xi_n(p) 2^{-N/2} \otimes_{i=1}^N \sigma^{p_i}[i]$, where each $\xi_n(p) = 2^{-N/2} Tr(\otimes_{i=1}^N \sigma^{p_i}[i] |\psi_n\rangle\langle\psi_n|)$ is a real coefficient and $\sigma^{p_i}[i]$ is a Pauli operator acting on qubit i. One easily verifies that we have

$$\mathbb{E}\left[Tr(\rho_{A,n}^2)\right] = 2^{N_B} \sum_{\{p\,:\,\forall i \notin A,\, p_i = 0\}} \mathbb{E}\left[\xi_n^2(p)\right] \qquad (1)$$

and our main purpose will be to analyze the evolution of the expected values of the squared coefficients, $\mathbb{E}\left[\xi_n^2(p)\right]$. Note that $\sum_p \xi_n^2(p) = Tr(|\psi_n\rangle\langle\psi_n|^2) = 1$ so that the $\mathbb{E}\left[\xi_n^2(p)\right]$ form a *probability distribution* on $\{0,x,y,z\}^N$ for all n.

Evolution of the coefficients— The key idea of the proof is the realization that there is a *Markov chain P* on $\{0,x,y,z\}^N$ which takes q distributed according to $(\mathbb{E}\left[\xi_n^2(q)\right])_q$ in one step of P to p distributed according to $(\mathbb{E}\left[\xi_{n+1}^2(p)\right])_p$. Then if the random unitary W_n at time n acts on qubits c, t in state $|\psi_n\rangle$,

$$\mathbb{E}\left[\xi_{n+1}^2(p)\,|\,\psi_n, c, t\right] = \frac{1}{16} \sum_{q,q' \in \{0,x,y,z\}^N \forall i \notin \{c,t\},\, q_i \neq q_i'} \xi_n(q)\xi_n(q') \times$$

$$\times \mathbb{E}\left[Tr[U\sigma^{q_c}[c]U^\dagger \sigma^{\hat{p}_c}[c]] Tr[U\sigma^{q_c'}[c]U^\dagger \sigma^{\hat{p}_c}[c]]\right] \times$$

$$\times \mathbb{E}\left[Tr[V\sigma^{q_t}[t]V^\dagger \sigma^{\hat{p}_t}[t]] Tr[V\sigma^{q_t'}[t]V^\dagger \sigma^{\hat{p}_t}[t]]\right],$$

where the $(\hat{p}_c, \hat{p}_t)$ are uniquely determined by $CNOT[c,t]\sigma^{p_c}[c]\sigma^{p_t}[t]CNOT[c,t]{=}\pm\sigma^{\hat{p}_c}[c]\sigma^{\hat{p}_t}[t]$. Direct calculation with the Haar measure on $U(2)$ shows that the products of expectations in the sum vanish unless $q = q'$. Then with the Kronecker symbol $\delta_{i,j}$ we find $\mathbb{E}\left[\xi^2_{n+1}(p) \mid \psi_n, c, t\right] = \sum_{q\in\{0,x,y,z\}^N} P^{(c,t)}(q,p) \prod_{i\notin\{c,t\}} \delta_{q_i,p_i}\xi^2_n(q)$

$$where\ P^{(c,t)}(q,p) = \begin{cases} 1, & \hat{p}_c = \hat{p}_t = q_c = q_t = 0; \\ 1/3, & \hat{p}_c = q_c = 0 \text{ and } \hat{p}_t, q_t \neq 0 \\ 1/3 & \hat{p}_t = q_t = 0 \text{ and } \hat{p}_c, q_c \neq 0 \\ 1/9, & \text{otherwise.} \end{cases}$$

Averaging the term $P^{(c,t)}(q,p)\prod_{i\notin\{c,t\}}\delta_{q_i,p_i}$ over the $N(N-1)$ choices of c, t produces the entry $P(q,p)$ of the transition matrix of the desired Markov chain P.

Convergence rate of the Markov chain.— The above shows that one can obtain $(\mathbb{E}\left[\xi^2_n(p)\right])_p$ from $(\xi^2_0(q))_q$ by performing n steps of P. One can "simplify" this picture by noticing that if $\{q(n) = (q(n)_1 q(n)_2 \ldots q(n)_N)\}_{n\geq 1}$ is such an n-step evolution of P, the sets $S(n) = \{i \in \{1,\ldots,N\} : q(n)_i \neq 0\}$ also form a Markov Chain. The quantity we are interested in only depends on this chain on those sets (cf. (1)): $i \notin A,\ p_i = 0\}\mathbb{E}\left[\xi^2_n(p)\right]$

$$\mathbb{E}\left[Tr(\rho^2_{A,n})\right] = 2^{N_B}\mathbb{P}\left(S(n) \subset A\right). \qquad (2)$$

Thus we need only to consider the chain $\{S(n)\}_n$.

As it turns out, our chain is *almost ergodic*: removing the isolated state $S(n) = \emptyset$, we obtain an ergodic chain on $\Omega = 2^{\{1,\ldots,N\}}\backslash\{\emptyset\}$. Since $\mathbb{P}\left(S(n) = \emptyset\right) = \mathbb{P}\left(S(0) = \emptyset\right) = 2^{-N}$, the convergence to equilibrium of $S(n)$ on Ω is enough for our purposes.

Some elementary calculations reveal that $\{S(n)\}$ is an ergodic reversible chain with equilibrium distribution $\mathcal{M}(S) = 3^{|S|}/(4^N - 1)$, $S \in \Omega$. Moreover, using standard *path coupling* and *comparison* techniques [22] one can deduce that all eigenvalues $\lambda \neq 1$ of $\{S(n)\}$ satisfy $\lambda \leq 1 - 4/9N(N-1)$; i.e. the *spectral gap* of $\{S(n)\}$ is $\geq 4/9N(N-1)$. Combined with the fact that $S(n+1) = S(n)$ with probability $\geq 1/2$ for any value of $S(n)$, we deduce [22]

$$\left|\mathbb{P}\left(S(n) \subset A\right) - \sum_{\emptyset\neq S\subset A}\mathcal{M}(S)\right| \leq \frac{(1 - \frac{4}{9}N(N-1))^n}{\min_{S\in\Omega}\mathcal{M}(S)}$$
$$\leq 4^N e^{-\frac{4n}{9N(N-1)}}.$$

Equation (2) and a few calculations finish the proof.

We now give numerical results indicating that for sufficiently large systems one can in fact associate a specific step with the achievement of the entanglement distribution compatible with the Haar measure.

Observe cut-off — Many Markov chains exhibit the so called "cut-off effect"[20]. The cut-off refers to an abrupt approach to the stationary distribution occurring at a certain number of steps taken in the chain. Say we have a Markov chain defined by its transition matrix P, and that it converges to a stationary distribution π. Initially the total variation distance $TV = \| P - \pi \| = sup \mid P(E) - \pi(E) \mid$ between the corresponding probability distributions is given by $TV = 1$. After k steps this distance is given by $TV(k) = \| P^k - \pi \|$. A cut-off occurs, basically, if $TV(k) \simeq 1$ for $k = 0, 1, 2, \ldots a$ and therafter falls quickly such that after a few steps $TV(k) \simeq 0$. As we increase the size of the state space, the ratio of the number of steps during which the abrupt approach takes place and a should vanish asymptotically. Then, for very large state spaces, we can say that the randomisation occurs at a steps, which is a function of the size of the state space. Rigorously, this may be stated as follows [20]. *Let P_n, π_n be Markov Chains on sets χ_n. Let a_n, b_n be functions tending to infinity, with b_n/a_n tending to zero. Say the chains satisfy an a_n, b_n cutoff if for some starting states x_n and all fixed real θ with $k_n = \lfloor a_n + \theta b_n \rfloor$, then $\| P^{k_n}_n - \pi_n \| \longrightarrow c(\theta)$ with $c(\theta)$ a function tending to zero for θ tending to infinity and to 1 for θ tending to minus infinity.* Here we observe this behaviour in the entanglement distribution, a functional of the Markov chain on unitaries given by the random circuit, and we accordingly term this a cut-off.

Numerical Observation — Numerical simulations indicate that a cut-off effect in the entanglement probability distribution under the random circuit on $|0\rangle^{\otimes N}$ may be observed both, for single qubit gates drawn from the Haar measure on U(2), see Figure 2, and for stabilizer gates, see Figure 3.

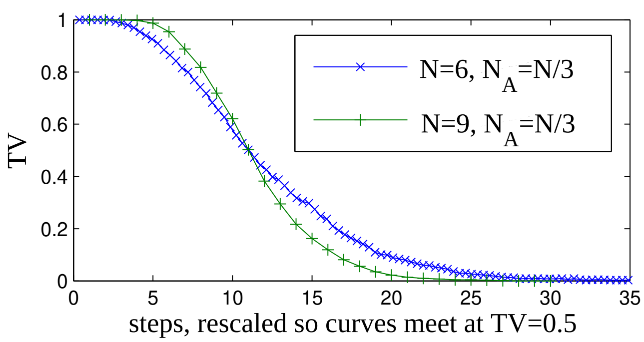

FIG. 2: Observe a variation Cut-Off of the entanglement probability distribution compared with that of the Haar measure as determined numerically. The state space has been discretised by rounding off entanglement values to the nearest integer. We observe that $TV \simeq 1$ for a while and then falls. Finally there is a stage where $TV \simeq 0$. We include the result for two setting to point out that the effect becomes more pronounced with increasing N.

These simulations using stabilizer gates allow us to consider far larger systems sizes. Here we choose the single qubit gates U and V from the set $\{\sigma^x, \sigma^y, \sigma^z, S, H\}$ [21] with equal probability. It should be noted that the proof of Lemma 1 still holds (see [23] for details) and the entanglement behaviour will remain similar. The restriction allows us to use the efficient stabilizer formalism [17] and the tools developed in [18] which in turn allows for an efficient evaluation of state properties. Figure 3 shows how the relative steepness of the curve in the "cut-off" region increases with the systems size N using this 'stabilizer' random circuit.

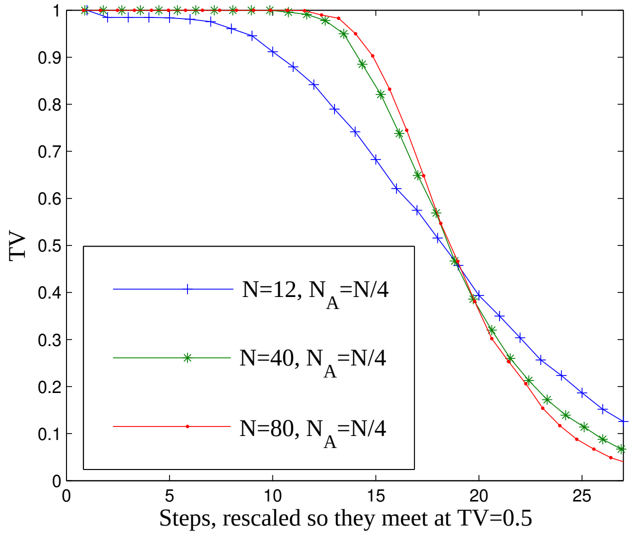

FIG. 3: cut-off effect in the 'stabilizer' random circuit. We used tools from [18] to efficiently evaluate the entanglement of the state. The total variation is evaluated relative to the final distribution derived in [19]. Asymptotically TV=0 for all the simulations.

Extensions of the present result – The above results may be extended in various directions that will be described briefly here.

Mixed States — To study these questions in a mixed state setting we do the same random circuit on a three-party pure state ρ_{ABC} and then trace out C to study the entanglement between A and B which now share a mixed state. In this setting there are classical and quantum correlations and one may study convergence rates and other properties employing e.g. the quantum mutual information, the entanglement cost and distillable entanglement.

Multi-particle entanglement measures – It would be interesting to extend the above results to properties of multi-partite entanglement. For entanglement measures based on average purities [1] this is possible with the results established here. Other measures such as the entanglement of formation may also be treated but require extensions of the approach presented here that go beyond the scope of this paper.

Markov Process Quantum Monte Carlo Methods – Our results possess another interpretation that is of interest for the numerical study of quantum-many-body systems. One numerical approach to classical spin systems is to evolve spin configurations randomly according to the Metropolis rule, ie always accepting moves that decrease energy and accepting moves that increase energy with a probability proportional to $exp\{-\Delta E/kT\}$. This reproduces the correct thermal average. One may of course consider a similar approach in the quantum setting applying random two-qubit gates to progress the state. Our present results fall into this category but apply for infinite temperatures as we draw our unitaries from the invariant Haar measure. However, we may adapt our analysis to the finite temperature regime employing stabilizer states at the expense of having to analyze a more complicated Markov process. Basic ideas of our approach carry over and open the possibility for rigorous statements concerning the convergence rate of such a Markov Process Quantum Monte Carlo approach.

The proof of Theorem 1 and Lemma 1 outlined in this work as well as the above extensions of our present result will be presented in detail in forthcoming publications.

Conclusion — In this work we have proved that the average entanglement over the unitarily invariant measure is reached in a time that is polynomial in the size of the system by a quantum random process that is restricted to random two-qubit interactions. We also provided numerical evidence that for large systems the Haar measure is achieved at a specific point in time, the variation cut-off. Our results demonstrate that the entanglement properties of generic entanglement are physical in the sense that they can be generated efficiently from random sequences of two-qubit gates. This also suggests that protocols like [2, 12, 13, 14] gain further significance based on our results. Possible extensions of our results with applications in various areas of physics have been discussed highlighting the physical significance of the present results.

Acknowledgements — We would like to acknowledge discussions with J. Oppenheim in early stages of this work and are grateful for discussions with T. Rudolph, G. Smith and J. Smolin. We acknowledge support by the EPSRC QIP-IRC, The Leverhulme Trust, EU Integrated Project QAP, the Royal Society, the NSA and the ARDA through ARO contract number W911NF-04-C-0098.

[1] M.B. Plenio and S. Virmani, arXiv:quant-ph/0504163.
[2] P. Hayden, D.W. Leung and A. Winter, arXiv:quant-ph/0407049.
[3] E.Lubkin, J. Math. Phys **19**, 1028 (1978).
[4] S.Lloyd and H.Pagels, Ann. of Phys. **188**, 186 (1988).
[5] D.N.Page, Phys. Rev. Lett. **71**, 1291 (1993).
[6] S.K Foong and S.Kanno, Phys. Rev. Lett. **72**, 1148 (1994)
[7] M.A. Nielsen and I. Chuang, *Quantum Information and Computation*, Cambridge Univ. Press, section 4.5.4.
[8] J. Emerson, E. Livine and S. Lloyd, arXiv:quant-ph/0503210
[9] J. Emerson, Y.S. Weinstein, M. Saraceno, S. Lloyd and D.G. Cory, Science 302, 2098 (2003).
[10] G.Smith and D.W.Leung, arXiv:quant-ph/0510232.
[11] J. Emerson, QCMC04, AIP Conf. Proc. 734, 139 (2004).
[12] A.Abeyesinghe, P.Hayden, G.Smith and A. Winter, arXiv:quant-ph/0407061.
[13] H. Buhrman, M. Christandl, P. Hayden, H.K. Lo, and S. Wehner. arXiv:quant-ph/0504078.

[14] A. Harrow, P. Hayden, and D. Leung, Phys. Rev. Lett., **92**, 187901 (2004).
[15] J. Emerson, R. Alicki and K. Zyczkowski, arXiv:quant-ph/0503243.
[16] D.P. DiVincenzo, D.W. Leung, and B.M. Terhal, IEEE Trans. Inf. Theory, 48(3), 580 (2002).
[17] D. Gottesman, arXiv:quant-ph/9807006.
[18] K.M.R. Audenaert and M.B. Plenio, New J. Phys. **7**, 170 (2005). Computer codes downloadable at www.imperial.ac.uk/quantuminformation.
[19] O.C.O.Dahlsten and M.B.Plenio, arXiv:quant-ph/0511119, to appear in QIC 2006.
[20] Cut-off effect in Markov Chains, P.Diaconis.
[21] In the computational basis we define $\sigma_x = [0,1;1,0], \sigma_x = [0,-i;i,0], \sigma_x = [1,0;0,-1], S = [1,0;0,i]$ and $H = [1,1;1,-1]/\sqrt{2}$ as well as $CNOT = [1,0,0,0;0,1,0,0;0,0,0,1;0,0,1,0]$.
[22] M. Jerrum, *Counting, Sampling and Integrating: a Markov Chain approach*, Birkhauser, (2003).
[23] Publication in preparation by the authors.