Math. Struct. in Comp. Science (2007), *vol.* 17, *pp.* 1221–1263.
doi:10.1017/S0960129507006366 Printed in the United Kingdom

Complexity of chaos and quantum computation

BERTRAND GEORGEOT

Laboratoire de Physique Théorique, Université Toulouse III, CNRS, 31062 Toulouse, France
Email: georgeot@irsamc.ups-tlse.fr

Received 4 October 2006

This paper reviews recent work related to the interplay between quantum information and computation on the one hand and classical and quantum chaos on the other.
First, we present several models of quantum chaos that can be simulated efficiently on a quantum computer. Then a discussion of information extraction shows that such models can give rise to complete algorithms including measurements that can achieve an increase in speed compared with classical computation. It is also shown that models of classical chaos can be simulated efficiently on a quantum computer, and again information can be extracted efficiently from the final wave function. The total gain can be exponential or polynomial, depending on the model chosen and the observable measured. The simulation of such systems is also economical in the number of qubits, allowing implementation on present-day quantum computers, some of these algorithms having been already experimentally implemented.
The second topic considered concerns the analysis of errors on quantum computers. It is shown that quantum chaos algorithms can be used to explore the effect of errors on quantum algorithms, such as random unitary errors or dissipative errors. Furthermore, the tools of quantum chaos allows a direct analysis of the effects of static errors on quantum computers. Finally, we consider the different resources used by quantum information, and show that quantum chaos has some precise consequences on entanglement generation, which becomes close to maximal. For another resource, interference, a proposal is presented for quantifying it, enabling a discussion on entanglement and interference generation in quantum algorithms.

Contents

1. Introduction

In classical computer science, the notion of complexity quantifies the asymptotic difficulty of solving a given problem. Many complexity classes have been defined, which try and evaluate this in term of space or time resources or both. The main divide separates polynomial problems, for which the resources needed grow polynomially with the number of bits of the input, and exponential problems, for which these resources grow exponentially with the number of bits. Polynomial problems are thought of as easy, while exponential ones are hard, in the sense that even a moderate increase of the input size becomes very quickly intractable. In many cases it is easy to quantify the complexity of an algorithm, but it is more difficult to do the same for a problem, since that requires us to find the best possible algorithm or at least its complexity. This explains why, while certain problems are known to be polynomial (arithmetic operations, and so on), and others to be exponential, many problems are 'probably' exponential: the fastest known algorithm is exponential, but there is no proof of the non-existence of a better algorithm (for example, the factorisation of integers or the travelling salesman problem).

Quantum computation (for good reviews see Steane (1998), Nielsen and Chuang (2000), Preskill (1998) and Benenti *et al.* (2004)) also gives rise to a well-defined notion of complexity, corresponding to the asymptotic number of elementary quantum operations (gates) needed for the resolution of a given problem. Unlike classical computation, great care has to be exercised in specifying the measurement process and the total number of operations needed, including the measurements. Indeed, on a quantum computer the information is hidden in a wave function, and the extraction of information requires quantum measurements. Several problems have been shown to admit an increase in speed for a quantum computer compared with classical computation. The most famous is Shor's algorithm (Shor 1994), which factorises an integer into prime factors in a polynomial number of operations, which is thus exponentially faster than any known classical algorithm. Grover's algorithm (Grover 1997) finds a given item in an unstructured list quadratically faster than any classical procedure.

On the other hand, in physics, complexity often refers to the dynamics of the system. The most complex systems in classical physics correspond to chaotic systems, for which a body of well-defined properties have been found and classified. Such systems often display ergodicity, mixing and exponential divergence of nearby trajectories. In the quantum realm, the domain of quantum chaos is less clearly delineated, but it is known that the corresponding wave functions show complex features that interconnect all parts of the system.

In recent years, these two notions of complexity have begun to interact within the quantum information field. In particular, the efficient simulation of chaotic classical and quantum systems on a quantum computer has been shown to be possible, and has even been implemented experimentally. Also, tools from the quantum chaos community have allowed us to understand certain types of errors that appear with quantum computers. This paper will review these different subjects, with an inevitable emphasis on my own work, which I know best. I will conclude with some remarks on the resources available for quantum information, exemplifying a link between quantum chaos and entanglement production, and also presenting a way to measure the interference used during a quantum process such as a quantum algorithm.

2. Complexity in classical and quantum chaos

The development of classical mechanics from Newton to Lagrange and Hamilton has enabled us to write down equations describing the dynamics. That these equations could be integrated fully in some cases led to the probably widespread belief that, in general, there existed certain sets of coordinates in which the motion will become simple and predictable. This corresponds to the notion of integrable systems. In such systems, the number of constants of motion equals the number of degrees of freedom N. In general, this leads to the existence of action-angle variables, in which the equations of motion become extremely simple. The classical trajectories lie on N-dimensional tori foliating the $2N$-dimensional phase space.

It was only at the end of the nineteenth century that Poincaré stumbled across some evidence of a very different behaviour while investigating the three-body problem. Yet this was a specific case, and only after the advent of computers did numerical integrations of equations of motion decisively show that integrable systems where the exception rather than the rule, and that many systems display a dynamics that is far from simple and predictable, and was termed chaotic.

2.1. *Classical chaos*

Such a dynamics also leads to a notion of complexity, corresponding to the difficulty of accurately predicting the behaviour of such systems. The study of this type of dynamics led to the definition of several degrees of chaos in Hamiltonian systems (for more detailed reviews see Lichtenberg and Lieberman (1992) and Ott (1993)). The lowest degree is ergodicity, for which one typical trajectory is dense in phase space (this is equivalent to the asymptotic equality of time and space averages). The next level is mixing: for any two subsets A and B of non-zero measure within the (finite) phase space Ω with a measure μ, if one applies the dynamics described by iterations of the function f, then $\mu(A)/\mu(\Omega) = \lim_{n\to\infty}\mu(B \bigcap f^n(A))/\mu(B)$. This means that for time long enough, any subset of Ω contains the same proportion of points originally in A. This property is already much stronger than ergodicity, but does not tell us how fast the mixing takes place. K-systems are mixing systems where the process is exponentially fast. In such systems, nearby trajectories diverge exponentially with time, and the correlation

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

functions decay exponentially. A certain function, called the Kolmogorov–Sinai entropy, is positive for such systems and quantifies the rate of mixing. This level of chaoticity corresponds to what is termed hard chaos, where the most extreme properties of chaos are seen.

Most physical systems actually lie between the integrable and chaotic extremes, being so-called mixed systems where integrable islands coexist with chaotic zones in phase space. A particular way of producing mixed systems is the (sufficiently smooth) perturbation of an integrable system. Indeed, according to the Kolmogorov–Arnold–Moser (KAM) theorem, rational tori where orbits are periodic disappear as soon as the perturbation is non-zero, and are replaced by chains of integrable islands (resonances) surrounded by chaotic layers. On the other hand, irrational tori where orbits are quasiperiodic and dense survive for non-zero perturbation; they are first deformed and then finally disappear for stronger perturbation.

Chaos can even be seen for Hamiltonian systems with one degree of freedom (phase space of dimension 2) provided energy is not conserved. The simplest such models are periodic in time with 'kicked potentials', giving a Hamiltonian such as $H(I,\theta,t) = TI^2/2 + kV(\theta)\sum_n \delta(t-n)$ (where θ is an angle, I is the conjugate action variable, k and T are parameters, and $V(\theta)$ is a potential). Integration over one period yields a map with discretised time

$$\bar{I} = I - kV'(\theta);\ \bar{\theta} = \theta + T\bar{I} \tag{1}$$

where bars denote values of (I,θ) after one iteration. These maps are area-preserving. Dynamics takes place on a cylinder (periodicity in θ), and is controlled by a single parameter $K = kT$. The map (1) is periodic in I of period $2\pi/T$, so the phase space structures repeat themselves on each cell of size $2\pi/T$. For $K = 0$, this dynamics is integrable (one-dimensional tori are lines I =constant). For many choices of the potential V, classical dynamics becomes chaotic when $K = kT$ increases. In particular, this is the case for $V(\theta) = \cos(\theta)$, which corresponds to the famous Chirikov standard map, which is also called the kicked rotator. For this map, a KAM transition takes place for $0 < K < K_g \approx 0.9716\ldots$ (see the picture of phase space in Figure 1). For $K \geqslant K_g$, the last invariant torus disappears and a single large connected chaotic zone enables chaotic diffusion through the system, with diffusion coefficient $D = \langle n^2\rangle/t \approx k^2/2$.

2.2. *Quantum chaos*

The translation of such properties to quantum mechanics has been the subject of the field of quantum chaos, which emerged in the 1960's and 70's. It seems obvious that quantum systems whose classical limit is chaotic should possess specific properties, since classical mechanics is a limit of quantum mechanics. Still, the limit is usually far from trivial, and, besides, quantum evolution is driven by the linear Schroedinger equation, which excludes any type of non-linear behaviour. Thus, the properties of classical chaos cannot be taken immediately to apply to some quantum systems. Instead, the work of many authors (see the reviews in, for example, Ott (1993) and Gutzwiller (1990)) has

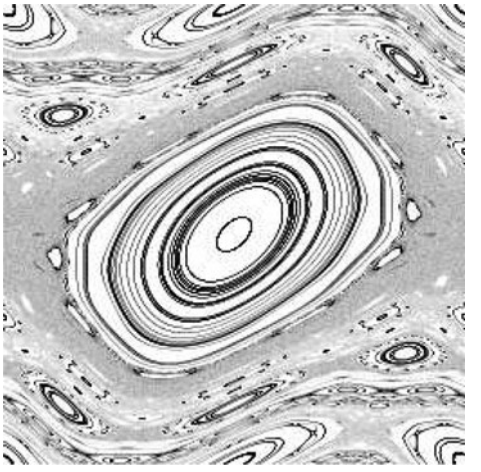

Fig. 1. The classical phase space of the Chirikov standard map at $K = K_g = 0.9716\ldots$ ($t = 10^4$ iterations of (1) with 200 points). The vertical axis is momentum and the horizontal axis is angle. The figure shows one phase space cell of size $2\pi/T$ in momentum. (Lévi *et al.* 2003)

enabled us to find certain properties that are present in quantum systems whose classical limit is chaotic, and can be understood as characterising the complexity of quantum chaos.

One such property concerns the construction of quantum wave functions semiclassically from classical quantities. While integrable systems enable the quantisation of individual tori (Einstein–Brillouin–Keller quantisation), chaotic systems require knowledge from classical orbits all over the system to approximate wave functions.

Another important property is connected to Random Matrix Theory. This approximates the statistical properties of spectra and wave functions by those of large matrices with random Gaussian entries. It gives predictions for several statistical quantities concerning eigenvalues or eigenstates of a Hamiltonian. As the average density of states depends on geometric features of the system and has no universality, spectra should be unfolded in order to get a mean level spacing equal to one before comparisons can be made with Random Matrix Theory predictions. A popular statistics is the nearest-neighbour distribution $P(s)$ of eigenvalues. This quantity is the density of probability for the distance between adjacent levels. It was conjectured in Berry and Tabor (1977) that the spectra of classically integrable systems should behave as uncorrelated random numbers, giving for $P(s)$ the Poisson law $P_P(s) = e^{-s}$. In contrast, it was conjectured in Bohigas *et al.* (1984) that classically chaotic systems should follow Random Matrix Theory predictions, which for $P(s)$ imply a level repulsion at short distance ($P(s) \to 0$ as $s \to 0$) and a faster than exponential decay for large s. The Wigner distribution $P_W(s)$, which approximates the Random Matrix results with good accuracy, is, for example, plotted on the left-hand side of Figure 10. This conjecture has been checked on many examples. It is remarkable that Random Matrix Theory can be quite predictive for many systems despite the fact that it

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

has no free parameter. In a sense, through Random Matrix Theory a kind of universality in quantum chaos emerges, where complex quantum systems share common features that can be modelled by random variables.

Finally, an important property of solid-state physics systems has a parallel in quantum chaos. Indeed, it was noted by Anderson in the 1950's that electrons in a disordered potential can be exponentially localised, although their classical motion would be diffusive. This is one way to create an insulator in solid state physics, which is called Anderson localisation. In some quantum chaos systems, a similar behaviour can be observed, termed dynamical localisation. Although the classical motion is diffusive, for these systems the quantum eigenstates are exponentially localised, albeit without any random potential.

The quantisation of chaotic maps described in the preceding section gives a variety of models displaying these properties. For the map (1), this yields an operator U such that $\bar{\psi} = U\psi$, where ψ is the wave function and $\bar{\psi}$ is its new value after one iteration, with

$$\hat{U} = e^{-ikV(\hat{\theta})} e^{-iT\hat{n}^2/2} \tag{2}$$

where $\hat{n} = -i\partial/\partial\theta$.

For $V(\theta) = \cos(\theta)$, the quantised kicked rotator has evolution operator corresponding to $\hat{U} = e^{-ik\cos\hat{\theta}} e^{-iT\hat{n}^2/2}$. The quantum dynamics depends on two parameters k and T (classically one single parameter $K = kT$ was enough), with T playing the role of an effective $\hbar$. The classical limit corresponds to $k \to \infty$, $T \to 0$ while keeping $K = kT = \text{constant}$. For $K < K_g \approx 0.9716..$, the quantum dynamics shows quantum diffusion limited by KAM tori, but for $K \gg K_g$, classical diffusion is replaced by quantum localisation. Eigenfunctions of $\hat{U}$ in momentum representation are $\sim \exp(-|n-m|/l)/\sqrt{l}$ with localisation length $l = D/2 \approx k^2/4$. Thus, dynamical localisation can be observed on the kicked rotator provided the system is larger than l. On the other hand, if the localisation length is greater than the system size, we recover results in accordance with Random Matrix Theory, with ergodic eigenfunctions. Therefore, many properties of quantum chaos can be seen in such a system despite its simplicity; this makes the kicked rotator a paradigmatic model of quantum chaos, which, additionally, has been shown to be a model for Rydberg atoms in microwave fields. Furthermore, it has been realised experimentally with cold atoms.

The quantum phase space distribution function is a very useful tool for the study of the features of complex wave functions. In classical mechanics, it is possible to describe the dynamics through (Liouville) probability distributions in phase space. In quantum mechanics, a wave function $|\psi\rangle$ embodies the state of the system, in momentum or position representation. Momentum and position do not commute, and a true probability distribution in phase space cannot really be defined. Instead, for a continuous system one can define the Wigner function through: $W(p,q) = \frac{1}{\sqrt{2\pi\hbar}} \int e^{-\frac{i}{\hbar}p.q'} \psi(q + \frac{q'}{2})^* \psi(q - \frac{q'}{2}) dq'$ (q is position and p momentum).

This function cannot be interpreted as a probability distribution, since it is real but can take negative values. Still, it satisfies the sum rules $\int_q W(p,q)dq = |\psi(p)|^2$ and $\int_p W(p,q)dp = |\psi(q)|^2$.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

On an N-dimensional Hilbert space (for example, for maps like (2)), one should use $2N \times 2N$ points of phase space and the formula becomes (with $\Theta = \frac{N\theta}{2\pi}$):

$$W(\Theta, n) = \frac{1}{2N} \sum_{m=0}^{N-1} e^{-\frac{2i\pi}{N} n(m-\Theta/2)} \psi(\Theta - m)^* \psi(m). \tag{3}$$

Smoothing the Wigner function over cells of area $\hbar$ gives a real non-negative function, which is therefore more like a classical probability distribution. Using a Gaussian smoothing gives the Husimi function $\rho_H(\theta_0, n_0) = |\langle \phi_{(\theta_0,n_0)} | \psi \rangle|^2$ where the smoothing function

$$\phi_{(\theta_0,n_0)}(\theta, n) = A \sum_n e^{-(n-n_0)^2/4a^2 - i\theta_0 n} |n\rangle$$

is a Gaussian wave packet centred on (θ_0, n_0) in phase space (A is a normalisation constant and a determines the width of the Gaussian).

Other smoothing functions can be used, such as, for example, the modified Husimi function (Frahm *et al.* 2004)

$$\rho_H^{(p)}(\theta_0, n_0) = |\langle \phi^{(p)}_{(\theta_0,n_0)} | \psi \rangle|^2 \tag{4}$$

where

$$\phi^{(p)}_{(\theta_0,n_0)}(\theta, n) = (1/N^{1/4}) \sum_{n=n_0}^{n_0+\sqrt{N}-1} e^{-i\theta_0 n} |n\rangle$$

(that is, the smoothing function is a box in momentum). This modified Husimi function is also real and non-negative. Figure 2 shows examples of Wigner and modified Husimi functions for the kicked rotator model. These quantum distributions show some correspondence with classical phase space plots such as in Figure 1, but in a much clearer way in the case of the Husimi function, the Wigner function presenting many interference patterns making it more complicated to interpret.

3. Coping with complexity: simulating chaos on quantum computers

Historically, the first application proposed for quantum computers (Feynman 1986) was the simulation of quantum systems. However, this first proposal was not very explicit but was refined later (Lloyd 1996), showing, for example, that certain many-body Hamiltonians could be simulated efficiently on quantum computers. Nevertheless, some questions remain unclear, such as the precise extent of systems that can be simulated efficiently through quantum algorithms, the precise observables that can be efficiently measured, and the total quantum complexity of such simulations. Models from quantum chaos are therefore good testgrounds to study and assess such problems, since despite being described by simple equations allowing efficient simulation even on small-scale quantum computers, they display many complex properties that can also be seen in more complicated systems. Historically, the first model of quantum chaos to be shown to be efficiently simulated by a quantum computer was the baker's transformation (Schack 1998), which shows quantum chaos but is not of the type (2).

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

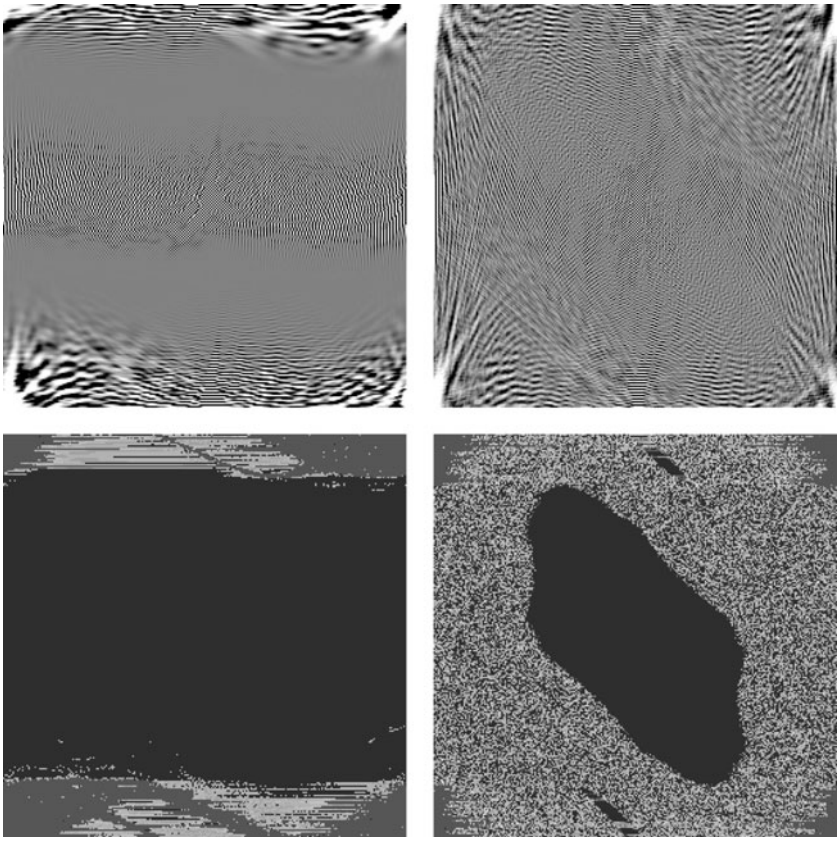

Fig. 2. The top pictures show the Wigner function for the quantum kicked rotator with $K = 0.9$ (left) and $K = 2$ (right). Here $T = 2\pi/N$, where $N = 2^{n_q}$, with $n_q = 7$. The vertical axis is momentum and the horizontal axis is angle. The whole Wigner function (on a $2N \times 2N$ lattice) is plotted. White represents the positive maximal values and black the negative values. The initial state is uniformly spread on the set $0 \leqslant n < N/8$, and the Wigner function is computed after 1000 iterations of (2). The bottom pictures show the modified Husimi function (4) for the quantum kicked rotator with $K = 0.9$ (left) and $K = 2$ (right). Here $T = 2\pi/N$, where $N = 2^{n_q}$, with $n_q = 16$. The function is plotted on a lattice of $\sqrt{N} \times \sqrt{N}$ and each point is the average of N points. The initial state is the same as for the top figures, and the function is computed after 1000 iterations of (2). Gray represents the maximal value, white the intermediate value and black the minimal value. (Terraneo *et al.* 2005)

3.1. *Simulation of chaotic quantum maps*

As explained in Section 2.2, quantum maps form a very congenial class of models displaying quantum chaos. In these systems, time is discretised and evolution corresponds to iterations of a one-step operator given by (2). Classical simulations of these systems take advantage of the factorised form (2) into an operator diagonal in momentum and an operator diagonal in position. Indeed, one starts from a wave function in momentum representation, then applies the first operator diagonal in momentum $e^{-iT\hat{n}^2/2}$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

by direct multiplication of the components of the wave function. Then one applies a fast Fourier transform to change representation from momentum to position. In this representation, the second operator $e^{-ikV(\theta)}$ is diagonal and can be readily implemented by direct multiplications. Then an inverse Fourier transform takes the wave function back to momentum representation. In this way, one iteration of (2) on a wave function in a Hilbert space of dimension N takes $O(N \log N)$ classical elementary operations, the slowest parts being the Fourier transforms.

It is possible to implement the evolution (2) on a quantum computer using many fewer elementary operations. Indeed, it was shown in Georgeot and Shepelyansky (2001a) that one iteration of (2) for $V(\theta) = \cos(\theta)$, corresponding to the kicked rotator, can be implemented on an N-dimensional Hilbert space ($N = 2^{n_q}$) with $O((\log N)^3)$ quantum gates. The quantum simulation follows the strategy of the classical one, with an increase in speed for each part.

Step I Preparation of initial state:

$$\psi(0) = \sum_{n=0}^{N-1} a_n |n\rangle.$$

For example, $\psi(0) = |N/2\rangle$.

Step II Action of $e^{-iT\hat{n}^2/2}$:

$$\sum_{n=0}^{N-1} a_n |n\rangle \Rightarrow \sum_{n=0}^{N-1} a_n e^{-iTn^2/2} |n\rangle$$

(by $\sim n_q^2$ applications of two-qubit gates).

Step III Quantum Fourier transform:

$$\sum_{p=0}^{N-1} a_n e^{-iTn^2/2} |n\rangle \Rightarrow \sum_{i=0}^{N-1} b_i |\theta_i\rangle$$

with $b_j = \frac{1}{N} \sum_{n=0}^{N-1} a_n e^{-iTn^2/2} e^{2i\pi jn/N}$. This changes from n to θ representation and costs $\sim n_q^2$ quantum gates.

Step IV Construction of the cosines:

$$\sum_{i=0}^{N-1} b_i |\theta_i\rangle |0\rangle \Rightarrow \sum_{i=0}^{N-1} b_i |\theta_i\rangle |\cos\theta_i\rangle.$$

This requires $\sim n_q^3$ gates and can be made using elementary arithmetical operations, which are known to be implementable efficiently on a quantum computer, at the cost of using several workspace registers (but these only amount to $O(n_q)$ qubits).

Step V Action of $e^{-ik\cos\hat{\theta}}$:

$$\sum b_i |\theta_i\rangle |\cos\theta_i\rangle \Rightarrow \sum b_i e^{-ik\cos\theta_i} |\theta_i\rangle |\cos\theta_i\rangle$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

(by n_q applications of one-qubit gates). Then we erase the cosines by running step IV backwards ($\sim n_q^3$ operations):

$$\sum_{i=0}^{N-1} b_i e^{-ik\cos\theta_i}|\theta_i\rangle|\cos\theta_i\rangle \Rightarrow \sum_{i=0}^{N-1} b_i e^{-ik\cos\theta_i}|\theta_i\rangle|0\rangle.$$

Step VI Quantum Fourier transform ($\sim n_q^2$ operations); this puts the wave function back in n representation.

The total number of elementary quantum gates is thus $O((\log N)^3)$; the whole process needs only $\sim \log N$ qubits. Thus simulation of the quantum kicked rotator needs exponentially less resources on a quantum computer than on a classical device.

Different regimes can be probed depending on how the parameters of the system scale with the number of qubits n_q. Keeping $K = kT$ constant in (2) keeps the classical dynamics unchanged. If, additionally, T is kept constant while n_q is increased, the size of phase space will increase exponentially (number of cells of size $2\pi/T$ in momentum). In this regime the localisation of eigenstates is seen as soon as the (constant) localisation length becomes smaller than the system size. In contrast, if $T = 2\pi/2^{n_q}$, the phase space keeps a constant size (one cell of size $2\pi/T$) while the effective $\hbar$ decreases exponentially. In this regime the localisation length rapidly becomes larger than the system size, and Random Matrix properties and semiclassical limits can be probed.

In this quantum simulation, the slowest part is the construction of the cosines, which is expensive both in number of qubits and gates. It is actually possible to find quantum algorithms that give a sufficiently good approximation of the wave function without computing the cosines explicitly, thus speeding up the process even further (see below). For other potentials $V(\theta)$, the exact quantum simulation can also be faster. Indeed, a related model called the sawtooth map corresponds to $\bar{\psi} = U\psi$ with the evolution operator $U = e^{-iT\hat{n}^2/2}e^{ik(\hat{\theta}-\pi)^2/2}$. It was shown in Benenti *et al.* (2001) that this model can be simulated on a quantum computer on an N-dimensional Hilbert space ($N = 2^{n_q}$), using only $3n_q^2 + n_q$ quantum gates per iteration and n_q qubits. This algorithm for simulation of the sawtooth map has actually very recently been experimentally implemented with three qubits using the NMR technique (Henry *et al.* 2005). Although the localisation is only algebraic in the sawtooth map, this phenomenon could be observed for the eight-dimensional Hilbert space in the experiment.

An even simpler map of the form (2) is given by the evolution operator

$$\hat{U} = e^{-2i\pi\hat{p}^2/N}e^{2i\pi\alpha\hat{q}}. \tag{5}$$

It was shown in Giraud and Georgeot (2005) that this map can be simulated on a quantum computer for a Hilbert space of dimension $N = 2^{n_q}$, with $2n_q^2 + 2n_q$ gates and n_q qubits, making it very economical. Depending on the value of α, this map can display a dynamics that can be chaotic, regular or intermediate between these two extremes.

The algorithms above are exact and efficient, but, for example, the kicked rotator algorithm needs many extra qubits for workspace; this may be a problem for the small quantum computers currently being built. It is therefore worthwile exploring the possibility of using approximate algorithms, which require less resource than the exact simulations.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

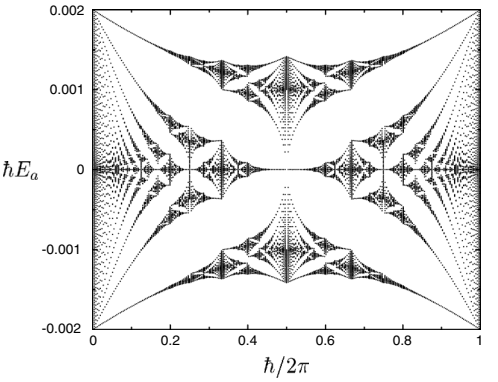

Fig. 3. Eigenphases of the Harper operator of (6) as a function of $\hbar$ for $K = L = 10^{-3}$ and Hilbert space dimension 2^8; one recovers the fractal spectrum of the Harper Hamiltonian. (Lévi and Georgeot 2004)

This has been done using another quantum map, the kicked Harper model (Lévi and Georgeot 2004), as the example.

The Harper model $H_0(p, q) = \cos(p) + \cos(q)$ is a famous model describing electrons in a magnetic field, which is well known for having a fractal spectrum, which is called the 'Hofstadter butterfly' (see Figure 3). Nevertheless, it is an integrable system. A more complex system is represented by the kicked Harper model: $H(I, \theta, t) = L\cos(I) + K\cos(\theta)\sum_n \delta(t - n)$, which once integrated over one period gives the map $\bar{I} = I + K\sin\theta$, $\bar{\theta} = \theta - L\sin\bar{I}$.

This map depends on two parameters K and L, and displays a transition to chaos as K and L increase. Quantisation leads to

$$\bar{\psi} = \hat{U}\psi = e^{-iL\cos(\hbar\hat{n})/\hbar} e^{-iK\cos(\hat{\theta})/\hbar}\psi \tag{6}$$

where $\hat{n} = -i\partial/\partial\theta$ and $\psi(\theta + 2\pi) = \psi(\theta)$. This model describes the motion of electrons in electromagnetic fields and the stochastic heating of a plasma. The limit $K = L \to 0$ gives the Harper model with its fractal spectrum (see Figure 3). There is dynamical localisation, similar to Anderson localisation of electrons in solids, as in the kicked rotator, but, in addition, for a certain range of values of K and L, there is a transition to a partially delocalised regime, with coexistence of localised and delocalised states.

On an N-dimensional Hilbert space with $N = 2^{n_q}$, an exact algorithm similar to the one described above for the kicked rotator requires $O(\log N^3)$ quantum gates for the evolution of the wave function and several workspace registers.

A first strategy for building more economical algorithms enables us to implement an approximation of operators of the form $e^{-ik\cos(p\hat{\theta})}$ by a succession of simpler operators. This follows an idea first presented in Pomeransky and Shepelyansky (2004). To this end, we introduce

$$M(\alpha, U) = HC_U H e^{i\frac{\alpha}{2}\sigma_z} HC_{U^{-2}} H e^{i\frac{\alpha}{2}\sigma_z} HC_U H$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

where C_U is U controlled by an ancilla qubit and H is a Hadamard gate. We have

$$M(\alpha, U) = 1 + i\alpha \frac{U + U^{-1}}{2} + O(\alpha^2).$$

If we now choose $U = e^{ip\theta}$, then

$$M(\alpha, U) = 1 + i\alpha \cos(p\,\theta)\sigma_z + O(\alpha^2) \approx e^{i\alpha \cos(p\,\hat{\theta})}.$$

Thus we can approximate $e^{-ik\cos(p\,\hat{\theta})}$ by $M(\alpha, U)^{n_s}$ with $\alpha = \frac{-k}{n_s}$ and error $O(\alpha^2)$. This can be improved further by symmetrisation, using $\widetilde{M}(\alpha, U) = M\left(\frac{\alpha}{2}, U\right) M\left(\frac{\alpha}{2}, U^{-1}\right)$. Then $e^{-ik\cos(p\,\hat{\theta})} \approx \widetilde{M}(\alpha, U)^{n_s}$ with error $O(\alpha^3)$.

This enables us to build a 'time-slice algorithm' for the kicked Harper model on $N = 2^{n_q}$-dimensional space. The implementation of both $e^{-iK\cos(\hat{\theta})/\hbar}$ and $e^{-iL\cos(\hbar\hat{n})/\hbar}$ by n_s iterations of the appropriate $\widetilde{M}(\alpha, U)$ needs $4 + 2(n_q - a) + (n_s - 1)(7 + 2(n_q - a))$ gates; the quantum Fourier transforms need $n_q(n_q + 1)$ gates. In total, only $n_q + 1$ qubits and $O(n_q^2)$ quantum gates are needed. Numerical simulations for increasing n_s show a good precision for relatively low n_s (Lévi and Georgeot 2004).

An alternative strategy, which was also explored in Lévi and Georgeot (2004), uses Chebychev polynomials to approximate the cosines. This method is used in classical computers to approximate functions. The Chebychev polynomials are defined by:

$$T_0(x) = 1, \quad T_1(x) = x, \quad T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x).$$

If $f(x)$ is a function on $[-1, 1]$, and

$$c_j = \frac{2}{M} \sum_{k=0}^{M-1} f\left[\cos\left(\frac{\pi\left(k + \frac{1}{2}\right)}{M}\right)\right] \cos\left(\frac{\pi j\left(k + \frac{1}{2}\right)}{M}\right),$$

then for large M we have that $\sum_{j=0}^{M-1} c_j T_j(x) - \frac{1}{2}c_0$ is a very good approximation of $f(x)$ on $[-1, 1]$. If we take such a polynomial $P(x)$ approximating $\cos(\pi(x + 1))$, then $e^{-ik\cos(p\,\hat{\theta})}$ can be approximated by $e^{-ikP\left(\frac{p\hat{\theta}}{\pi} - 1\right)}$, which is much easier to implement on a quantum computer. To simulate the kicked Harper model, a Chebychev polynomial approximation of degree d leads to a complexity of $O({n_q}^d)$ ($N = 2^{n_q}$). Numerics (Lévi and Georgeot 2004) show that $d = 6$ is enough to get a very good approximation of the wave function. The simulation of one time step of the kicked Harper model on an $N = 2^{n_q}$-dimensional space needs only n_q qubits and $O((n_q)^d)$ quantum gates.

The numerical results given in Lévi and Georgeot (2004) showed that both approximate methods give good results for a moderate number of qubits. The most economical in number of qubits is the Chebychev method, where no workspace qubit is used. However, in the numerical simulations the time-slice method, despite needing one more qubit, was actually the most efficient in terms of the number of gates used, and therefore in terms of the computing time.

Thus, we see that even in cases where the exact algorithm for simulating (2) requires many workspace qubits, it is possible to use efficient approximate quantum algorithms that use very few extra qubits and still simulate the dynamics with good accuracy. This implies that quantum chaos maps of the form (2) can in many cases be implemented

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

on small-size quantum computers, such as the ones currently being built throughout the world.

3.2. *Information extraction*

We have seen that complex quantum evolution, manifested by quantum chaos properties, can be simulated with exponential efficiency on a quantum computer. Still, at the end of the simulation one is left with an N-dimensional wave function that, in general, requires $O(N)$ measurements for an accurate description. Thus, to assess the quantum algorithmic complexity of such simulations, one should describe the measurement procedure, and compare the efficiency of obtaining a given observable from quantum and classical algorithms. This problem is present in general for any quantum simulation of quantum systems, and corresponds to the even more general question of efficient extraction of information from a general quantum wave function.

The simplest idea is to use coarse-grained measurements. For a wave function on n_q qubits (Hilbert space of dimension $N = 2^{n_q}$), this can be achieved by measuring the first n_f qubits only, thus yielding a wave function that is coarse grained over 2^{n_f} cells (this can be realised equivalently by measuring all qubits and binning the data in a histogram of 2^{n_f} boxes). If n_f is kept constant while the total number of qubits increases, a given precision can be achieved for the probability of each cell at a constant cost. Coupled with a procedure as above to simulate a system exponentially fast, this can, in principle, yield an exponential gain. Nevertheless, the wave function obtained is only an approximation, and this should be compared with classical approximate methods, which are often faster than exact simulations. Also, the time evolution of the system should be long enough to enable the desired result to be obtained, which can mitigate the quantum gain. As an example, these two factors lead to a polynomial gain when the coarse-grained method is applied to the measure of the localisation length of quantum chaotic maps.

Indeed, we have seen in Section 2.2 that the kicked rotator presents localised states. The localisation length l can be measured directly by fitting an exponential function around maximal values of $|\psi\rangle$ obtained by coarse-grained measurements. This is effective and costs only a constant number of measurements to get a given precision in units of l (Benenti *et al.* 2003).

However, the usual way to obtain this length l numerically is to start from an initial state that is localised on one value of momentum and evolve the wave function through (2). The wave packet initially spreads but after a certain number of iterations its size reaches the localisation length and the spreading stops. Thus iterations should be performed until size $\approx l \approx D$ (D is the classical diffusion constant). For a short time initially in the kicked rotator one expects diffusive spreading $\langle n(t)^2 \rangle \approx Dt$; thus the wave packet needs to be evolved until the time $t^* \approx l^2/D \approx l$. Thus the total number of gates needed is $\sim l$, dropping logarithmic factors.

On the other hand, classically it is possible to get a good approximation of the evolution by restricting it to a Hilbert space of dimension $\sim l$. The classical simulation of a vector of dimension $\sim l$ for time t^* costs $\sim l^2$ operations. Thus the comparison leads to only a quadratic improvement for the quantum algorithm.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

Other transport properties such as the diffusion constants can be obtained by similar procedures. A coarse-grained measurement enables us to get these diffusion constants once the wave function has spread enough. But, for example, in the kicked Harper model the quantum dynamics for short times is diffusive on the $K = L$ line, and this gives $\sim (t^*)^{3/2}$ operations classically, and $\sim t^*$ quantum mechanically for evolving the system up to time t^*. The time t^* corresponds to a time long enough for the diffusion to be seen for a wave packet initially localised on one momentum value. Outside the $K = L$ line, the motion is ballistic ($\langle n(t)^2 \rangle \approx Dt^2$). The same arguments as above give $\sim (t^*)^{3/2}$ operations classically and $\sim t^*$ quantum mechanically for evolving the system up to time t^*. Thus, the gain is again polynomial in both cases, albeit with different powers (Lévi and Georgeot 2004).

A recent efficient algorithm to simulate the evolution of a wave packet on disordered quantum small-world networks was presented in Giraud *et al.* (2005). These networks have been investigated in statistical physics since they are widespread in nature and have the interesting feature of linking distant sites through a small number of links. The quantised version of this system shows a spreading of the wave packet, which can get faster and faster when more and more random links are added to the network (Giraud *et al.* 2005). Thus, in this case it is possible that an exponential gain could be obtained for the computation of diffusion constants since the factor limiting the efficiency for quantum computation of such quantities is the spreading rate of the wave packet.

Another quantity that can be extracted from a complex wave function is the fidelity decay (Emerson *et al.* 2002). We suppose we have a quantum map with evolution operator U that is efficiently implementable on a quantum computer and a perturbed evolution operator U_p that is efficiently implementable also. The function $f(t) = |\langle U^t \psi_0 | U_p^t \psi_0 \rangle|^2$ measures the fidelity decay between the exact and perturbed wave function, and has been the subject of many studies since it reflects the dynamics of the system. If the initial state is $|\psi_0\rangle = U_0|0\rangle$, then $\langle U^t \psi_0 | U_p^t \psi_0 \rangle = \langle 0 | U_0^+ (U^+)^t U_p^t U_0 | 0 \rangle$, so simulating $U_0^+ (U^+)^t U_p^t U_0$ and sampling the population of the state $|0\rangle$ gives the fidelity decay (with polynomial precision). This may give rise to a possible exponential gain compared with classical simulations, since there is no known classical algorithm giving this result efficiently. This procedure was actually recently experimentally implemented using the NMR technique (Ryan *et al.* 2005).

It is also possible to measure the spectral statistics discussed in Section 2.2 on a quantum computer after evolving a map with evolution operator U such as in (2). It was shown in Poulin *et al.* (2003) that one can transfer the value of the traces of iterates of U on an ancilla qubit with $\mathrm{Tr} U^p / N = \langle \sigma_z \rangle$ for the probe qubit. The value of traces for small p are known to characterise the dynamics of the quantum map: regular, integrable, or intermediate. Measuring the traces on a quantum computer can be shown to give a quadratic improvement over classical computation.

Several recent works have also studied the extraction of information using quantum phase space distribution functions such as the Wigner and Husimi functions presented in Section 2.2. These functions are important since they are widely used, represent all information about the wave function, and allow especially easy comparison with classical evolution. It was shown in Miquel *et al.* (2002) that one can measure Wigner functions (3)

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

at one given phase space location using an ancilla qubit. The goal is to obtain the Wigner function of a wave function $|\psi\rangle$. To do this, we apply one Hadamard gate to the ancilla qubit, then the operator $A(\Theta, n) = S^{\Theta} R V^{-n} \exp(2i\pi\Theta n/2N)$ to the system, the application being conditioned by the value of the ancilla qubit (S = shift in Θ basis, $S(|\Theta\rangle) = |\Theta+1\rangle$; V = shift in the n basis; R = the reflection operator, $R(|n\rangle) = |N-n\rangle$). Then we apply one Hadamard gate to the ancilla qubit. The expectation value of the ancilla can be shown to be

$$\langle \sigma^z \rangle = Re[Tr(A(\Theta, n)\rho)] = 2NW(\Theta, n)$$

where $\rho = |\psi\rangle\langle\psi|$ is the density matrix and $N = 2^{n_q}$ is the dimension of the Hilbert space. In principle this allows us to extract the value of the Wigner function from the evolution of any efficiently implementable map of the form (2). Nevertheless, the values of W are usually very small, and this may require exponentially many iterations.

Another algorithm was proposed in Terraneo *et al.* (2005), which uses a different strategy: we build a state of the quantum computer whose amplitudes in a chosen basis gives the Wigner function. The wave function we want to study is supposed to be produced by t iterations of a map like (2) on an initial state $|\psi_0\rangle$.

The procedure is as follows:

Step I Transform $|\psi_0\rangle|\psi_0\rangle$ into

$$|U^t\psi_0\rangle|U^t\psi_0\rangle = \sum_{\theta,\theta'} \psi(\theta)\psi^*(\theta')|\theta\rangle|\theta'\rangle.$$

Then add an extra qubit and transform into

$$\sum_{\theta,\theta'} \psi(\theta)\psi^*(\theta')|\theta+\theta'\rangle|\theta'\rangle$$

(addition).

Step II Take the Fourier transform of the second register, to give

$$\sum_{\Theta}\sum_{n}\left(\sum_{\theta'} e^{-\frac{2i\pi}{N}n\theta'}\psi(\Theta-\theta')\psi^*(\theta')\right)|\Theta\rangle|n\rangle$$
$$= 2\sqrt{N}\sum_{\Theta}\sum_{n} W(\Theta, n)e^{-\frac{2i\pi}{N}n\Theta/2}|\Theta\rangle|n\rangle$$

where $\Theta = \theta + \theta'$ and Θ varies from 0 to $2N-1$ and n from 0 to $N-1$.

Step III Add an extra qubit in the state $|0\rangle$ and apply a Hadamard gate to give

$$\sqrt{2N}\left(\sum_{\Theta}\sum_{n=0}^{N-1} W(\Theta, n)e^{-\frac{2i\pi}{N}n\Theta/2}|\Theta\rangle|n\rangle + \sum_{\Theta}\sum_{n=N}^{2N-1} W(\Theta, n)e^{-\frac{2i\pi}{N}(n-N)\Theta/2}|\Theta\rangle|n\rangle\right).$$

Then multiply by the phases $e^{-\frac{2i\pi}{N}n\Theta/2}$ and $e^{-\frac{2i\pi}{N}(n-N)\Theta/2}$ to give the final wave function

$$|\psi_f\rangle = \sqrt{2N}\sum_{\Theta=0}^{2N-1}\sum_{n=0}^{2N-1} W(\Theta, n)|\Theta\rangle|n\rangle.$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

This procedure allows further quantum data treatment, such as amplitude amplification, or the quantum wavelet transform.

Amplitude amplification (Brassard *et al.* 2002) is a generalisation of Grover's algorithm. It increases the amplitude of a whole subspace H, instead of a single marked state. Let P be a projector on this subspace H, and $\hat{V}$ be an operator taking $|0\rangle$ to a state having some projection on H. Repeated iterations of $\hat{V}(I-2|0\rangle\langle 0|)\hat{V}^{-1}(I-2P)$ on $\hat{V}|0\rangle$ will increase the projection. Indeed, if one write $\hat{V}|0\rangle = P\hat{V}|0\rangle + (I-P)\hat{V}|0\rangle$, the result of one iteration is to rotate the state toward $P\hat{V}|0\rangle$ staying in the subspace spanned by $P\hat{V}|0\rangle$ and $(I-P)\hat{V}|0\rangle$. One can check that after one iteration the state has a component along $(I-P)\hat{V}|0\rangle$ decreased by an amount that depends on $|P\hat{V}|0\rangle|^2$. If N is the dimension of the total Hilbert space and M the dimension of H, then $\sqrt{N/M}$ iterations are needed to bring the probability to be in H close to 1. One sees from the procedure that the probability to be in H is increased by changing the norm of the projection, keeping its direction in H constant. Thus for a wave function, using amplitude amplification to increase the projection on some subset of the computational basis will keep the initial relative amplitudes on each basis vector of the subset.

Wavelet transforms are generalisations of Fourier transforms. For the wavelet bases, each basis vector is localised in position as well as momentum, with different scales (note the difference compared with the Fourier basis, which is composed of plane waves). Wavelet basis vectors are obtained by translations and dilations of an original function and their properties enable us to probe the different scales of the data as well as localised features, both in space and frequency. The wavelet transforms are used in a large number of applications involving classical data treatment, in particular, they allow us to reach large compression rates for classical images in standards like MPEG. Indeed, in many cases the same information can be spread on many fewer wavelet coefficients than Fourier coefficients. Efficient quantum algorithms for implementing such transforms have been built, requiring polynomial resources to treat an exponentially large vector.

These different strategies have been tested by numerical simulations for the kicked rotator model on an N-dimensional space in Terraneo *et al.* (2005). The cost of measuring the final wave function after t iterations was assessed through computation of a participation ratio of the Wigner function $\xi = 1/(\sum N^2 W(\Theta, n)^4)$, which computes how amplitudes are dispatched on the different basis vectors of the computational basis. If N peaks of approximately equal weights $1/N$ are present, then $\xi = N$, whereas N^2 components of equal weights (in absolute value) $1/N^{3/2}$ give $\xi = N^2$. This quantity ξ therefore enables us to estimate the number of main components of the Wigner function, and as a consequence the number of measurements needed to get the largest peaks with a given accuracy. For direct measurements, numerical results (see the examples on the left-hand side of Figure 4) show that the quantum algorithm needs $O(tN^{\alpha})$ operations with $\alpha \approx 1.8-2$; classically one needs $O(tN^2 \log N)$ operations, meaning a small polynomial gain is obtained. This is the only gain attainable through the measurement of the probe qubit as in Miquel *et al.* (2002). Other possibilities arise if we use the direct construction of the Wigner function allowed by the algorithm described above. Coarse-grained measurement could give a possible exponential gain. Comparing amplitude amplification on an $N_D \times N_D$ square, we get $O(tN + N_D N)$ operations classically and $O(tN_D^{\alpha} N)$ quantum mechanically, which means

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

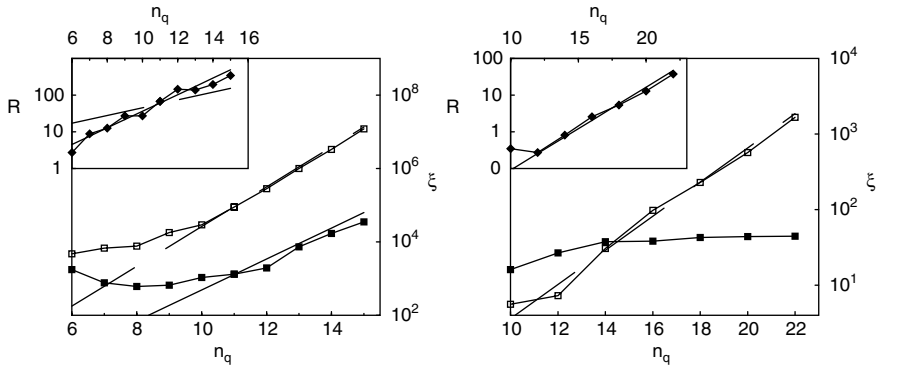

Fig. 4. The plot on the left-hand side shows $\xi = 1/(\sum N^2 W(\Theta, n)^4)$ for the Wigner function (open squares) and its wavelet transform (full squares) for $K = 2$. The straight lines are $\alpha = 1.8$ and $\beta = 1.4$, respectively; $N = 2^{n_q}$. In the inset, the ratio R between ξ of the Wigner function and the wavelet transformed Wigner function is plotted. The full line represents the scaling $N^{0.75}$, while the dashed line represents $N^{0.35}$. Here $T = 2\pi/N$, where $N = 2^{n_q}$. The initial state is uniformly spread on the set $0 \leqslant n < N/8$, and the Wigner function is computed after 1000 iterations of (2). The plot on the right-hand side shows the scaling for ξ versus n_q for the function $H(\theta, n)$ where $|H(\theta, n)|^2$ is the modified Husimi function in (4), with parameters $K = 2$ and $T = 2\pi/N$, $N = 2^{n_q}$. In the main plot, empty squares represent ξ of $H(\theta, n)$ the full squares represent ξ of the wavelet transform of the modulus of $H(\theta, n)$, and the dashed line is $N^{0.7}$. In the inset, the ratio R between ξ of $H(\theta, n)$ and wavelet transform of $|H(\theta, n)|$ is plotted for different n_q, the full line is $N^{0.7}$. The number of iterations and the initial state are the same as for the picture on the left-hand side. (Terraneo *et al.* 2005)

we again get a small polynomial gain. Finally, wavelet transforming the Wigner function leads to $O(tN^{\beta})$ with $1.4 \leqslant \beta \leqslant 2$ quantum mechanically, compared with $O(tN^2 \log N)$ classically, giving a larger polynomial gain. The gain is larger in the chaotic regime

For Husimi functions, the same strategy of computing a ξ that counts the number of main components can be used. Paz *et al.* (2004) showed how to use an ancilla qubit to transfer the value of the Husimi function and obtain its value at a specific phase space location. The method is complicated: it constructs a Gaussian using the ground state of the Harper Hamiltonian, and suffers from similar drawbacks to the same method for the Wigner function.

It is actually much simpler to use the modified Husimi function (4). Indeed, Frahm *et al.* (2004) showed that if we use a quantum Fourier transform of the first half of the qubits, we can transform an N-dimensional wave function $|\psi\rangle$ ($N = 2^{n_q}$) into $|\psi_H\rangle = \sum_{\theta,n} H(\theta, n)|\theta\rangle|n\rangle$, where θ and n take only $\sqrt{N}$ values each and $|H(\theta, n)|^2$ is the modified Husimi function, using only $(n_q/4)(n_q/2 + 1)$ quantum gates. It is therefore quite economical to construct the modified Husimi function on a quantum register from a given wave function.

Numerical results for the kicked rotator on an N-dimensional space after t iterations (Terraneo *et al.* 2005) (see the example on the right-hand side of Figure 4) show that direct measurements lead to $O(tN^{\gamma})$ operations with $0.5 \leqslant \gamma \leqslant 0.7$ for the quantum algorithm,

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

compared with $O(tN)$ classically, leading to a polynomial gain. As before, coarse-grained measurements can give rise to a possibly exponential gain. Amplitude amplification on an $N_D \times N_D$ square requires $O(t\sqrt{N}N_D^{\gamma-1/2})$ operations quantum mechanically, against $O(tN)$ classically. This means that a quadratic gain is obtained, independent of the system simulated. The wavelet transform also gives a polynomial gain.

Thus, the quantum phase space distribution can be obtained from a simulation on a quantum computer faster than on a classical computer. It is also possible to obtain the spectrum of an operator with some speeding up. A general procedure has been presented in Kitaev (1995) and Abrams and Lloyd (1999). Given a unitary operator U and an eigenvector $|u\rangle$, the goal is to find the associated eigenvalue $e^{2i\pi\omega_u}$ efficiently. The procedure starts from $1/\sqrt{N}\sum_{t=0}^{N-1}|t\rangle|u\rangle$, and we transform it into $1/\sqrt{N}\sum_{t=0}^{N-1}|t\rangle|U^t u\rangle = 1/\sqrt{N}\sum_{t=0}^{N-1}e^{2i\pi\omega_u t}|t\rangle|u\rangle$. Then a quantum Fourier transform of the first register yields $|\omega_u\rangle|u\rangle$. To be exponentially efficient, this requires:

(i) an operator U whose exponentially large iterates are efficiently implementable, and
(ii) a good approximation of one eigenvector.

This is the case for Shor's algorithm, which can be reinterpreted as phase estimation on the operator $U|y\rangle = |ay \bmod(N)\rangle$.

If (i) and (ii) are not fulfilled, as is the case for maps such as (2) in general, a modification of the procedure enables us to get a polynomial gain (Lévi and Georgeot 2004). The evolution operator on an N-dimensional Hilbert space ($N = 2^{n_q}$) should be efficiently implementable, as is the case in several models like (2). We start with $\sum_{t=0}^{N-1}|t\rangle|\psi_0\rangle$, for example, $|\psi_0\rangle = 2^{-n_q/2}\sum_n |n\rangle$. Then we transform it into $2^{-n_q/2}\sum_{t=0}^{N-1}|t\rangle|U^t\psi_0\rangle$ in $O(N)$ operations (since iterates of U should be computed sequentially). Then a quantum Fourier transform of the first register yields peaks centred at eigenvalues of U. A measurement of the first register gives one random eigenvalue of U with good probability in $O(N)$ operations. If we combine this procedure with amplitude amplification, all eigenvalues in a given interval can be obtained in $O(N\sqrt{N})$ operations.

For the kicked Harper model, this should be compared with the $O(N^2)$ operations needed classically to get the spectrum, and gives a polynomial gain for exploring the complexity of fractal spectra such as the one in Figure 3.

Thus, we see that extracting information from a complex wave function requires some care. The exponential efficiency of simulating maps of the form (2) on a quantum computer does not translate straightforwardly into an exponential gain for a full quantum algorithm including measurements. Yet the discussion presented here shows that methods do exist for extracting information efficiently, and, depending on the observable considered, the gain can be polynomial or possibly exponential compared with classical algorithms. Thus the quantum simulation of maps such as (2) has a practical interest, which is reinforced by the remarkable economy of resources used.

3.3. *Simulation of classical chaos*

It may seem natural that quantum computers can simulate complex quantum mechanical systems with some efficiency. However, although quantum mechanics rules the world

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

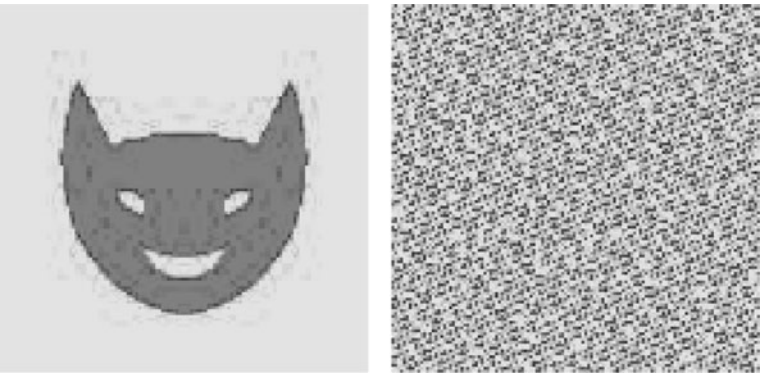

Fig. 5. Dynamics of the cat map (7) on a 128×128 lattice. Left: initial distribution; right: distributions after 10 iterations; the probability is represented by the shade of gray from light gray (low probability) to black (high probability); due to the exponential instability, the initial structures disappear very quickly. (Georgeot and Shepelyansky 2001b)

around us, many applications and problems require the use of classical mechanics. It is therefore important to determine whether quantum computers can help in understanding classical dynamical systems. While regular systems are usually quite predictable, chaotic properties lead to an exponential divergence of nearby trajectories and instability, which makes chaotic systems hard to simulate over long times on a classical computer.

Chaotic maps with one degree of freedom (phase space of dimension 2) are described by simple equations but can display most of the features of hard chaos. They are therefore good test grounds for studying the feasibility of quantum simulations of classical chaos. A well-known example is the Arnold cat map:

$$\bar{y} = y + x \ (\mathrm{mod}\ 1);\ \bar{x} = y + 2x \ (\mathrm{mod}\ 1). \tag{7}$$

This is a textbook example of hard chaos, with positive Kolmogorov–Sinai entropy, exponential divergence of trajectories, and so on.

To simulate such an evolution numerically for a classical phase space probability distribution, one should discretise the phase space into small cells and iterate the cells as trajectories (an example of such an evolution is given in Figure 5). It was shown in Georgeot and Shepelyansky (2001b) that a phase-space density on a $2^{n_q} \times 2^{n_q}$ lattice (that is, 2^{2n_q} different trajectories) can be simulated on a quantum computer with only $16n_q - 22$ quantum gates per iteration and $3n_q - 1$ qubits. This should be contrasted with the simulation on a classical computer, which costs 2^{2n_q+1} additions.

The algorithm for one iteration of (7) is very simple; it uses repeated applications of modular addition (addition modulo $N = 2^{n_q}$), which is known to be efficiently implementable on a quantum computer:

Step I Preparation of the initial wave function: $\psi(0) = \sum_{i,j} a_{i,j}|x_i\rangle|y_j\rangle$. This wave function encodes the initial phase space distribution, (x_i, y_j) labelling the phase space cells of the $2^{n_q} \times 2^{n_q}$ lattice and $|a_{i,j}|^2$ specifying the probability in this cell.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

Step II (Modular addition)

$$\sum_{i,j} a_{i,j}|x_i\rangle|y_j\rangle \Rightarrow \sum_{i,j} a_{i,j}|x_i\rangle|y_j + x_i(\mathrm{mod}(1))\rangle = \sum_{i,j} b_{i,j}|x_i\rangle|y_j\rangle.$$

Step III (Modular addition)

$$\sum_{i,j} b_{i,j}|x_i\rangle|y_j\rangle \Rightarrow \sum_{i,j} b_{i,j}|x_i + y_j(\mathrm{mod}(1))\rangle|y_j\rangle = \sum_{i,j} c_{i,j}|x_i\rangle|y_j\rangle.$$

The cat map is area-preserving and reversible. As quantum computers are inherently reversible due to the unitarity of quantum evolution, it may seem that such quantum simulations of classical chaos are limited to reversible processes. This would be a big limitation, since dissipative dynamical systems arise quite commonly in physics. In particular, chaotic dissipative dynamics often converges to a strange attractor with fractal dimension: this has been observed in turbulence and weather forecasting, molecular dynamics, chaotic chemical reactions, multimode solid state lasers, ecology and physiology, and so on. In fact, it was shown in Terraneo *et al.* (2003) that the dissipative deterministic map $\bar{y} = \frac{y}{2} + x \pmod 2$, $\bar{x} = \frac{y}{2} + 2x \pmod 1$, which converges to a strange attractor of fractal dimension ≈ 1.543, can be simulated efficiently on a quantum computer. Indeed, quantum computation of a density on a $2^{n_q} \times 2^{n_q+1}$ lattice can perform one iteration of the map with $17n_q - 10$ quantum gates. Four registers are needed, $|x\rangle, |y\rangle, |\mathrm{workspace}\rangle, |\mathrm{garbage}\rangle$. The additional garbage register is needed because of the irreversibility of the map, and keeps track of the information loss during the evolution. The size of this garbage register grows like t (simplest algorithm), but can be made to grow like $\ln t$ if the 'pebble game' algorithm described in Preskill (1998) is used.

As in the case of simulation of quantum systems, the results above imply that one can simulate the evolution of classical chaotic maps with exponential efficiency compared with classical simulation. However, this gain can be illusory since one has to take into account the measurement procedure to extract information from the final wave function.

Obviously, to extract the full phase-space density directly requires an exponential number of measurements. It was suggested in Georgeot and Shepelyansky (2002) that Fourier coefficients of the discretised phase-space density can be obtained by applying a quantum Fourier transform after iterating the map and performing coarse-grained measurements of the wave function. This gives the possibility of an exponential gain, since, unlike quantum dynamics, the classical dynamics is exponentially fast in Fourier space: large harmonics corresponding to exponentially small scales being very quickly populated due to chaos.

In the case of dissipative dynamics, it was shown in Terraneo *et al.* (2003) that going to Fourier space can also give the possibility of an exponential gain. Indeed, the spectrum of phase space correlation functions, defined by

$$C(t, k_{x,y}) = \sum_{x_0,y_0} \exp(2i\pi(x(t, x_0, y_0) + y(t, x_0, y_0))) \exp(2i\pi(k_x x_0 + k_y y_0))$$

can be obtained on a quantum computer by coarse-grained measurements (here the sum runs over points (x_0, y_0) of the initial distribution, and $(x(t, x_0, y_0), y(t, x_0, y_0))$ is the position of (x_0, y_0) after t iterations). Such correlation functions have been studied for

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

chaotic systems, where they determine various kinetic coefficients, such as the diffusion rate (Lichtenberg and Lieberman 1992). This requires $O(n_q^2)$ gates (t iterations of the map + $(2n_q + 1)$ one-qubit rotations + t reverse iterations + a quantum Fourier transform) on a quantum computer to obtain the state $A \sum_{k_x,k_y} C(t, k_{x,y})|k_x\rangle|k_y\rangle$ (with an additional normalisation constant) as the wave function. Measuring just the first n_f qubits, a polynomial number of measurements gives a coarse-grained image of $|C(t, k_{x,y})|^2$. The possibility of exponential gain is further substantiated by a numerical simulation showing that this whole procedure is exponentially faster than classical Monte-Carlo (Terraneo *et al.* 2003).

A different way to extract information from the quantum simulation of classical complex dynamics was presented in Georgeot (2004), by looking at long times instead of large system size. A theorem of Poincaré states that for classical bounded conservative systems, some points from an arbitrary small phase space domain A will eventually return to A. The time needed for the first return is called the recurrence time; it is usually a very long time, and hard to find numerically.

For more general systems, periodic orbits form a related concept: these are orbits that return exactly to their starting position in phase space. They can be considered to be the 'backbone' of classical dynamics, since they enable us to compute diffusion coefficients and the properties of strange attractors, and to enter classical and semiclassical trace formulas.

We have seen above that the cat map (7) can be efficiently simulated on a quantum computer. It can be described as the action of the 2×2 matrix

$$L = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \text{ on } \begin{pmatrix} x \\ y \end{pmatrix}.$$

It is known that for this map the periodic points are the rational points; they all belong to some $g \times g$ lattice of $\{(p_1/g, p_2/g)\}$, $p_1, p_2 = 0, 1 \ldots g$. With such a lattice, the map acts on numerators only as $\bar{y} = y + x \pmod g$, $\bar{x} = y + 2x \pmod g$, or

$$\begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} = L \begin{pmatrix} x \\ y \end{pmatrix} \pmod g,$$

with $x, y, \bar{x}, \bar{y}$ integers.

The lattice period function $\alpha(g)$ is the smallest integer such that after $\alpha(g)$ iterations all points in the lattice have returned to the initial position. Alternatively, $\alpha(g)$ is the smallest integer t such that $L^t = I \pmod g$. It is a very erratic function of g, of order g, which can be considered as the equivalent of the recurrence times for the cat map (see Figure 6 for an example of its distribution).

It was shown in Georgeot (2004) that this quantity can be obtained efficiently on a quantum computer. The algorithm corresponds to the following steps:

Step I Start with $N^{-1/2} \sum_{t=0}^{N-1} |t\rangle|1\rangle|0\rangle|0\rangle|1\rangle$ where $N = 2^{n_q}$ with $n_q \sim \log_2 g$.

Step II Transform it into $N^{-1/2} \sum_{t=0}^{N-1} |t\rangle|A_t\rangle|B_t\rangle|C_t\rangle|D_t\rangle$, where (A_t, B_t, C_t, D_t) are entries of the matrix L^t mod g, periodic function of t.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

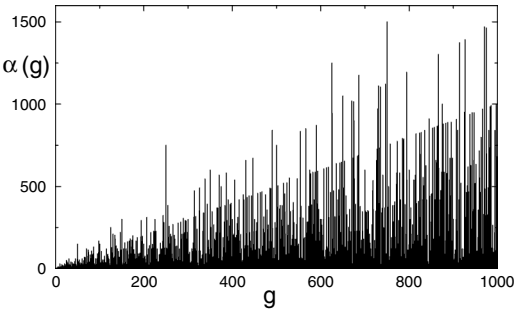

Fig. 6. The lattice period function $\alpha(g)$ for the Arnold cat map.

Step III Measure the last registers. The result is $|A\rangle|B\rangle|C\rangle|D\rangle$ corresponding to a given (randomly chosen) matrix K. The total state is $M^{-1/2}\Sigma_{j=0}^{M-1}|t_j\rangle|A\rangle|B\rangle|C\rangle|D\rangle$ where t_j are all t such that $L^{t_j} = K$, and $M \approx 2^{n_q}/\alpha(g)$.

Step IV Perform a quantum Fourier transform of the first register to yield peaks at multiples of $M \approx 2^{n_q}/\alpha(g)$. From the measurement of such a value, a continued fraction algorithm yields the period in $\sim n_q^3$ classical operations.

The reader familiar with Shor's algorithm for the factorisation of integers will recognise the steps, since this is very similar to the factorisation algorithm, the main difference being that the period of matrices, rather than numbers, is found. In total, $O((\log g)^3)$ operations and $\sim 9 \log g$ qubits are needed to find $\alpha(g)$. This is a probable exponential improvement in speed compared with a classical computation, since all methods known for computing $\alpha(g)$ classically are exponential in g.

More generally, a similar algorithm can be applied to other systems besides the cat map. We start from an initial point and look for periodicities of its iterates. We use a discretised (unitary) map on a lattice $x_i = i/N$, $i = 0, \ldots, N-1$ and $y_j = j/N$, $j = 0, \ldots, N-1$, with $N = 2^{n_q}$. The initial state is $2^{-p/2}\sum_{t=0}^{2^p-1}|t\rangle|x_0\rangle|y_0\rangle$ with $p \approx n_q$. This is transformed efficiently into $2^{-p/2}\sum_{t=0}^{2^p-1}|t\rangle|L^t(x_0)\rangle|L^t(y_0)\rangle$. Then we perform a quantum Fourier transform of the first register. This can only be efficient if a fast (polynomial in k) classical computation of (L^{2^k}) is possible.

In general, however, iterates of L cannot be computed efficiently for most classical maps, but L is efficiently computable over exponentially many points. In this case the algorithm above does not give an increase in speed, but a quantum computer can still obtain recurrence times faster than classical computers using the Grover algorithm as a subroutine. One chooses a time t fixed and a subdomain A. A simple case is a square of size $P \times P$ with $P = 2^p$ in a phase space of size $N \times N$ where $N = 2^{n_q}$. The initial state is $|\psi_0\rangle = 2^{-p}\sum_{i=0}^{2^p-1}\sum_{j=0}^{2^p-1}|x_i\rangle|y_j\rangle$. Then we perform $|\psi_0\rangle \rightarrow 2^{-p}\sum_{i=0}^{2^p-1}\sum_{j=0}^{2^p-1}|L^t(x_i)\rangle|L^t(y_j)\rangle$. After that, we give a (-1) phase to the values of $|L^t(x_i)\rangle|L^t(y_j)\rangle$ ending a trajectory returning to A, then invert everything. This yields $2^{-p}\sum_{i=0}^{2^p-1}\sum_{j=0}^{2^p-1}\epsilon|x_i\rangle|y_j\rangle$, where $\epsilon = \pm 1$, and $\epsilon = -1$ marks a point that has returned to A after t iterations. We are now in a position to use this as an oracle in Grover iterations to increase the probability of these particular points; one return among M is found in $O(tP/\sqrt{M})$ operations, as opposed to $O(tP^2/M)$ classically.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

We can also obtain periodic orbits of period t with a similar procedure. We start from all the $N \times N$ points of the lattice with $N = 2^{n_q}$. Then $|\psi_0\rangle$ is transformed into $2^{-n_q} \sum_{i=0}^{2^{n_q}-1} \sum_{j=0}^{2^{n_q}-1} |x_i\rangle|y_j\rangle|L^t(x_i)\rangle|L^t(y_j)\rangle$. After t iterations the value of the iterate is compared to the initial value; a minus sign is given if it is the same; then we invert the process and get $2^{-n_q} \sum_{i=0}^{2^{n_q}-1} \sum_{j=0}^{2^{n_q}-1} \epsilon|x_i\rangle|y_j\rangle$. As before, this is used as an oracle in Grover iterations; one periodic orbit among M is found in $O(tN/\sqrt{M})$ operations, as opposed to $O(tN^2/M)$ classically.

For example, let us look at classical maps of the form (1). If $V(\theta) = \cos\theta$ (the Chirikov standard map), the discretised map on a $2^{n_q} \times 2^{n_q}$ lattice can be performed in $O(n_q^3)$ gates, while its iterates cannot be implemented exponentially fast with respect to the number of iterates. This implies that a quadratic gain is achievable for the computation of recurrence times and periodic orbits.

For $V(\theta) = -\theta^2/2$ (sawtooth map), the discretised mapping is

$$\bar{Y} = Y + [NK(2\pi X/N - \pi)/(2\pi)](\mathrm{mod}N); \quad \bar{X} = X + \bar{Y}(\mathrm{mod}N).$$

For integer K, one can get an exponential gain, but only a quadratic gain is possible for non-integer K. The case $K = \pm 1/2$ for return times needs only 3 registers; a domain 4×4 in a 8×8 lattice requires only 8 qubits and a few tens of quantum gates.

Therefore, as with the simulation of quantum chaotic maps, we see that it is possible to extract information efficiently from the simulation of classical dynamical systems on quantum computers. Again, the gain can be polynomial or exponential depending on the quantity considered and the system simulated. Some of these algorithms can be implemented with a remarkable economy of resources, meaning they could be implemented on present day quantum computers. However, unlike the case with quantum chaotic maps, no experimental implementation of this type of algorithm has been realised so far.

4. Complexity against computation: errors in the quantum computer

The preceding section was concerned with various algorithms that can be implemented on a quantum computer once such a system is built. Yet, despite years of experimental progress, we are still far from being able to built such a device of any reasonable size. The reason lies in the difficulties associated with keeping a set of qubits coherent and in manipulating them while unwanted processes make the system evolve in uncontrollable ways. These error processes can be identified as belonging to one of three main types, their relative importance depending on the precise implementation. The first type is random unitary errors, such as imperfections in the implementation of the quantum gates. This can be modelled as noise in the quantum gates applied. The second type is external non-unitary errors, which correspond to coupling to the external world and are usually described as 'decoherence'. Finally, the third type of errors correspond to internal imperfections in the device, and are manifested even when a quantum computer is at rest without coupling to the external world. Quantum algorithms such as those developed in Section 3.1, since they use a small amount of resources to produce complex quantum wave functions on which different observables can be measured, are ideal test grounds for exploring the effects of such errors on quantum algorithms, especially numerically. In the following we will

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

study these three types of errors, assessing how they affect the quantum computer while simulating a complex wave function. It will turn out that tools from quantum chaos can help to model the effect of internal errors. Also, different types of errors will be shown to have vastly different effects depending on the observable considered.

4.1. *Random unitary errors*

The first type of error corresponds to random unitary errors; it can be modelled as, for example, unitary noise in the gates. Numerical simulations and analytical estimates for the kicked rotator model on a quantum computer with such types of errors have been performed in Song and Shepelyansky (2001) and Lévi *et al.* (2003). The system is therefore described by (2) with $V(\theta) = \cos\theta$. The Hilbert space dimension is $N = 2^{n_q}$, and T and k are constant. In this case, the size of phase space grows exponentially with n_q, keeping the effective $\hbar$ constant. This is the regime where quantum localisation can be seen for large K values.

The errors were implemented by rotating each quantum gate by a small angle drawn randomly in $[0, \varepsilon]$. For such a process of random errors, one expects physically that each gate transfers probability of order ε^2 from the exact wave function. The results of the simulations showed that this can lead to vastly different time scales, depending on the observable.

The first quantity we can look at is the fidelity: $f(t) = | < \psi_\varepsilon(t) | \psi_0(t) > |^2$ (the projection of the perturbed state onto the exact state). As each gate transfers probability of order ε^2, this leads to an estimate for the fidelity time scale (the unit of time is the number of iterations of (2)):

$$t_f \approx C_f/(\varepsilon^2 n_g) \tag{8}$$

where n_g is the number of gates for one iteration of (2), which depends polynomially on n_q (see Section 3.1). The time scale (8) is therefore polynomial in ε and n_q (C_f is a constant). This time scale is confirmed numerically by the plot on the left-hand side of Figure 7.

If we now turn to the second moment $< n^2 > = < (n - n_0)^2 >$, where the initial wave function is $|\psi_0\rangle = |n_0\rangle$, the results are quite different. Indeed, similar arguments to those given for the fidelity time scale now lead to a very different estimate for the second moment time scale:

$$t_q \approx C_q k^4/(\varepsilon^2 n_q 2^{2n_q}). \tag{9}$$

This is polynomial in ε, but exponential in n_q (C_q is a constant). This is confirmed by the plot on the right-hand side of Figure 7. The reason for such behaviour lies in the fact that even a small transfer of probability from the exact localised state can increase the second moment enormously, provided the transfer is to regions far away in phase space. Indeed, the random errors are strongly non-local in phase space: a change in the most significant qubit being enough to change location over half of phase space.

This shows that the same physical process of errors can give vastly different outcomes for the same computation, depending on the observable we are interested in.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

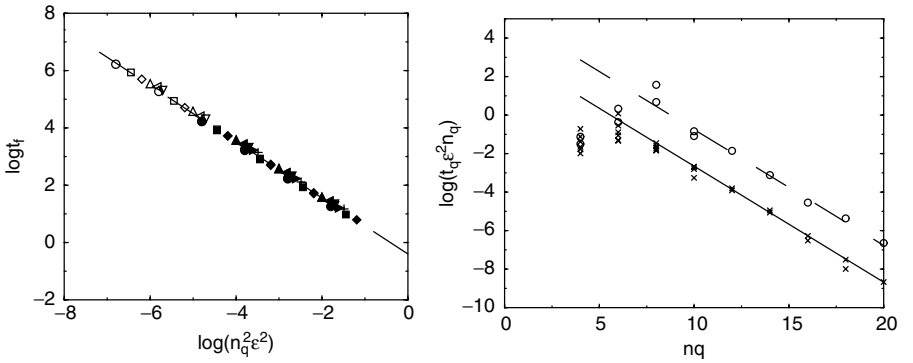

Fig. 7. The plot on the left-hand side shows the dependence of the time scale t_f on system parameters for $n_q = 4$ (○), 6 (squares), 8 (◇),10 (△), 12 (◁), 14 (▽), 16 (▷), 18 (+). Here $K = 1.3$, $T = 2\pi/N$ ($N = 2^{n_q}$) (open symbols) or $K = 5$, $T = 0.5$ (full symbols). The dashed line is the theoretical formula (8) with $C_f = 0.35$. The initial state is $|\Psi_0 >= |n_0 >$, with $n_0 = 1$ ($K = 1.3$) or $n_0 = N/2$ ($K = 5$). The plot on the right-hand side shows the dependence of the rescaled time scale t_q on the number of qubits n_q for $10^{-6} < \epsilon < 0.03$, $T = 0.5$, $K = 5$ (×) and $K = 15$ (○). The initial state is $|\Psi_0 >= |n_0 >$ with $n_0 = N/2$. Full and dashed lines correspond to the theoretical formula (9) with $C_q = 0.23$. (Lévi *et al.* 2003)

In view of these results, it is important to explore how phase space distribution functions such as the Wigner function are affected by the errors, since such distributions are among the important observables to be extracted from a wave function.

This was investigated in Lévi *et al.* (2003) (an example of the effects of such errors on phase space distributions is given in Figure 8). It was shown that the relative error in the Wigner function $\delta W = \langle |W - W_\epsilon| \rangle / \langle |W| \rangle$ varies only polynomially with the parameters of the system (W and W_ϵ are the exact and perturbed Wigner functions, respectively). Numerical simulations (see Figure 9) showed that it obeys the time scale

$$t_W \approx C_W / (n_q^\alpha \epsilon^2) \tag{10}$$

where α depends on the regime (localised, chaotic, integrable) the system is in. This shows that the Wigner function is only polynomially affected by these errors, thus confirming the fact that it can be effectively measured on a quantum computer even in the presence of random errors.

4.2. *Dissipative decoherence*

The effect of errors on quantum chaos algorithms has also been recently explored for dissipative decoherence (Lee and Shepelyansky 2005). The dissipation was numerically computed using the method of quantum trajectories, which enables us to study a quantum computer undergoing decoherence for relatively long times. The algorithm tested was the one for the quantum sawtooth map discussed above in Section 3.1, which has actually been experimentally implemented with the NMR technique. It was shown that in the presence of these errors the fidelity decays exponentially with time and that the decay rate

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

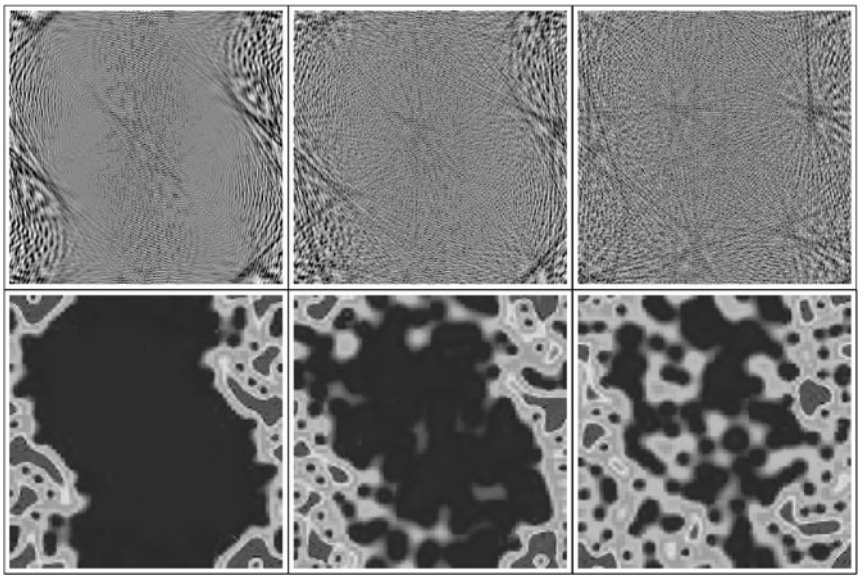

Fig. 8. Plot of Wigner (top) and Husimi (bottom) distributions for the kicked rotator model at $t = 10^3$ for $K = 1.3 > K_g$, $T = 2\pi/N$, $N = 2^{n_q}$ and $n_q = 7$. The initial state is $|\Psi_0> = |n_0>$, with $n_0 = 1$. The horizontal axis is momentum and the vertical axis is angle. The quantum noise (random unitary errors) is $\epsilon = 0$ (left), $\epsilon = 0.002$ (centre), $\epsilon = 0.004$ (right). For the top plots, grayness represents the amplitude of the Wigner function, from white (minimal negative value) to black (maximal positive value). For the bottom plots black represents the minimal intensity level, white an intermediate intensity level and gray the maximal intensity level. (Lévi *et al.* 2003)

is proportional to the number of qubits n_q, the number of quantum gates per iteration of the map n_g and the dissipation rate per gate induced by external decoherence Γ. This gives the following time scale for fidelity decay in the presence of dissipative errors:

$$t_d \approx 1/(n_q n_g \Gamma). \tag{11}$$

For localisation properties, a moderate dissipation destroys the dynamical localisation of the exact models, but in the limit of strong dissipation there is again localisation but on a quantum attractor, which may have a complex or simple structure depending on the parameters. It is interesting to note that the fidelity decay law obtained for quantum chaos algorithms also holds for the Grover algorithm in the presence of dissipative errors (Zhirov and Shepelyansky 2006).

4.3. *Static imperfections: many-body quantum chaos*

Before turning to internal errors, we will give brief consideration to quantum chaos in many-particle systems. Quantum chaos phenomena have been seen to manifest themselves quite commonly in quantum many-body systems, especially when some disorder is present. In such systems, the classical limit is often harder to grasp in practice than in the one-body case. Nevertheless, many models follow the predictions of Random Matrix Theory,

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

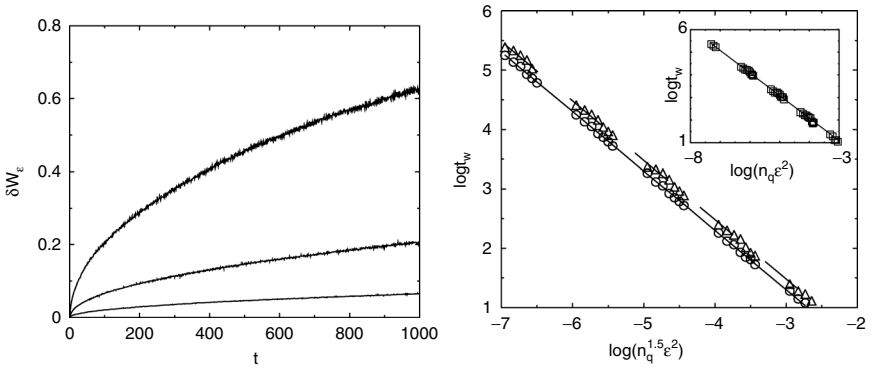

Fig. 9. The plot on the left-hand side shows the relative error in the Wigner function $\delta W_\epsilon = \langle |W - W_\epsilon| \rangle / \langle |W| \rangle$ as a function of time for $K = K_g$, $T = 2\pi/N$, $N = 2^{n_q}$ and $n_q = 10$. The initial state is $|\Psi_0 >= |n_0 >$, with $n_0 = N/2$. From bottom to top, the quantum noise is $\epsilon = 10^{-4}$, $\epsilon = 10^{-3.5}$, $\epsilon = 10^{-3}$. The Wigner function is averaged over $2N$ values in the chaotic zone. The plot on the right-hand side shows the dependence of time scale t_W on system parameters for $5 \leqslant n_q \leqslant 11$. Here $K = K_g$, $T = 2\pi/N$ ($N = 2^{n_q}$). The Wigner function is averaged over $2N$ values in the chaotic zone (◯) or in the integrable zone (△). The straight lines are the theoretical formula (10) with $\alpha = 1.5$ and $C_W = 0.02$ (full line) or $C_W = 0.03$ (dashed line). The initial state is $|\Psi_0 >= |n_0 >$, with $n_0 = N/2$. The inset shows the dependence of time scale t_W on system parameters for $5 \leqslant n_q \leqslant 14$. Here $T = 0.5$ and $K = 5$. The Wigner function is averaged over $2N$ values in the localised zone (squares). The full line is the theoretical formula (10) with $\alpha = 1$ and $C_W = 0.012$. The initial state is $|\Psi_0 >= |n_0 >$, with $n_0 = N/2$. (Lévi *et al.* 2003)

although possibly only in a certain energy range, and have wave functions ergodic in Hilbert space.

Usually, the presence of a random interaction drives an initially integrable or localised system to such a quantum chaos regime. This has been shown in many different systems such as nuclei, atoms, quantum dots, interacting fermions, quantum spin glasses, and so on. Remarkably enough, this happens despite the fact that the two-body interactions usually found in nature couple only very few of the many-body states of the unperturbed system.

Such a quantum chaos regime may appear in a quantum computer. Indeed, the energy between the two states of the qubits may fluctuate from one qubit to another. Also, an interaction between qubits is necessary to use two-qubit gates. Usually, in many quantum computer models this interaction is switched on and off to use the gates, but this cannot be done with perfect accuracy, and there will be residual random couplings that act permanently on the system. Such static (time-independent) imperfections make a quantum computer similar to a disordered interacting system of the type discussed above. A quantum computer with static imperfections can be modelled by the following Hamiltonian:

$$H = \sum_i \Gamma_i \sigma_i^z + \sum_{i<j} J_{ij} \sigma_i^x \sigma_j^x. \tag{12}$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

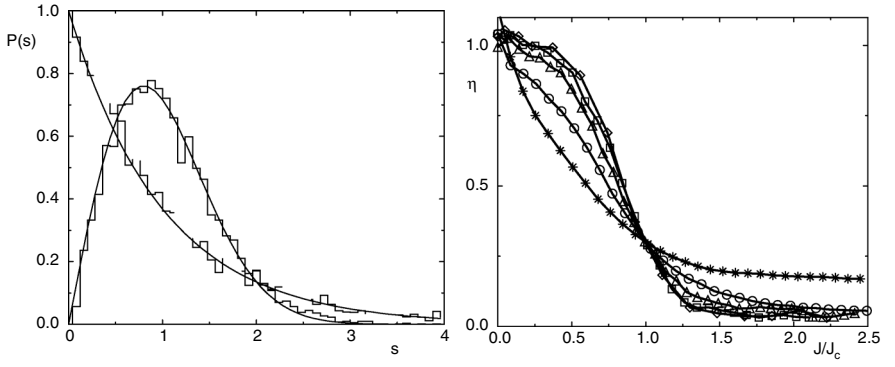

Fig. 10. The plot on the left-hand side shows the transition from Poisson to Wigner statistics for the Hamiltonian (12) in the central band for n_q=16: $J/\delta = 0.05, \eta = 0.99$ (dashed line histogram); $J/\delta = 0.32, \eta = 0.047$ (full line histogram). The full curves show the Poisson distribution $P_P(s)$ and the Wigner distribution $P_W(s)$. The plot on the right-hand side shows the dependence of η on the rescaled coupling strength J/J_c (J_c is the quantum chaos border, see text) for the states in the middle of the energy band for $n_q = 6(*), 9(o), 12(\text{triangles}), 15(\text{squares}), 16(\text{diamonds})$. (Georgeot and Shepelyansky 2000b)

This Hamiltonian was introduced in this context and analysed in Georgeot and Shepelyansky (2000a; 2000b). The qubits labelled by i, j are in a two-dimensional lattice; J_{ij} are nearest-neighbour couplings random uniform in $[-J, J]$; Γ_i is random in $[\Delta - \delta/2, \Delta + \delta/2]$; σ_i are Pauli matrices.

In the absence of the couplings ($J = 0$), the model (12) for n_q qubits and $\delta \ll \Delta$ presents a density of states composed of $n + 1$ bands, the central band being the most important in a number of many-body states. For $\delta = \Delta$, the different bands merge into one band of Gaussian shape. In both cases the spectral statistics are Poisson, which is typical of integrable systems as long as $J = 0$. Note that n_q qubits imply $N = 2^{n_q}$ multi-qubit states ('quantum register states'). To investigate the transition to quantum chaos when J increases, it is useful to study the spectral statistics. Numerical results show a transition from the Poisson distribution (typical of integrable systems) to the Wigner distribution (from Random Matrix Theory) of eigenvalues of (12) as J/δ increases, as seen in the plot on the left-hand side of Figure 10. To monitor the transition in a more precise way, it is customary to use a parameter η defined by

$$\eta = \frac{\int_0^{s_0} (P(s) - P_W(s)) ds}{\int_0^{s_0} (P_P(s) - P_W(s)) ds}$$

where $s_0 = 0.4729\ldots$ is the intersection point of $P_P(s)$ (Poisson distribution) and $P_W(s)$ (Wigner distribution). This parameter η varies continuously from $\eta = 1$ (Poisson) to $\eta = 0$ (Wigner). The results shown in the plot on the right-hand side of Figure 10 show a sharp transition (it can be smooth in other systems).

Where in parameter space does the transition take place? The Hamiltonian (12) has three energy scales. The largest is Δ, the one-particle level spacing. The smallest is Δ_n, the level spacing between multi-particle states, which decreases exponentially with n_q. There

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

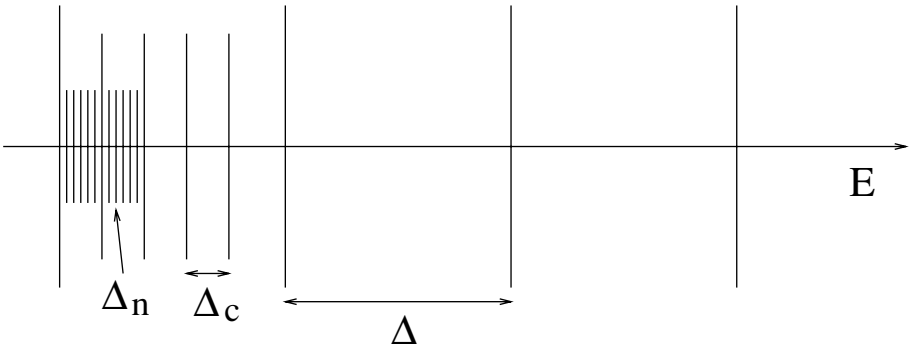

Fig. 11. The three different energy scales in (12): Δ is the one-particle level spacing; Δ_n the level spacing between multi-particle states; and Δ_c the level spacing between directly coupled multi-particle states. Note that $\Delta_n \ll \Delta_c < \Delta$.

is, however, a third energy scale. Indeed, the Hamiltonian corresponds to a very sparse matrix. Due to the two-body interaction, (12) can couple multi-qubit states only if they differ by only two qubits. Thus very few states are actually coupled by matrix elements of (12). This introduces a third energy scale, which is Δ_c, the level spacing between directly coupled multi-particle states, which varies polynomially with n_q. Thus one obviously has $\Delta_n \ll \Delta_c$. The three energy scales are shown in Figure 11.

The numerical results show that at a certain value of interaction J_c, the system undergoes a transition to quantum chaos. The dependence of this 'quantum chaos border' on system parameters is obviously of great interest. Recent work has dealt with this problem in similar systems: in particular, a general prediction was made in Åberg (1990) and Jacquod and Shepelyansky (1997). It was realised that chaos corresponds to mixing of many-particle states, and as higher orders of perturbation theory can be written in terms of two-particle terms, mixing of many-particle states should happen when two-particle states are mixed. We can therefore expect the critical interaction strength to be $J_c \approx \Delta_c$. This was confirmed by numerical simulations in many systems with two-body interactions.

For the Hamiltonian (12), we have seen that the spectrum for $J = 0$ (in the case $\delta \ll \Delta$) is composed of $n + 1$ bands with interband distance 2Δ and width $\sqrt{n_q}\delta$. Thus, in the central band, where $\sim 2^{n_q}/n_q$ states are present, this gives the estimate $\Delta_n \sim n_q^{3/2} 2^{-n_q}\delta$, which is exponentially small. In the same central band, one multi-qubit state is coupled to around n_q states in an energy interval 2δ, thus $\Delta_c \sim \delta/n_q$. The general estimate for J_c therefore implies that $J_c \approx \Delta_c \sim \delta/n_q \gg \Delta_n \sim n_q^{3/2} 2^{-n_q}\delta$. The numerical results presented in the plot on the left-hand side of Figure 12 show that this estimate is correct in the case of (12).

In the regime of quantum chaos, the true eigenstates of (12) are no longer quantum register states, but have components in many of them. To quantify this spreading of eigenstates, two related quantities are generally used, which depend on W_{im}, the quantum probability to find the quantum register state $|\psi_i\rangle$ in a true eigenstate $|\phi_m\rangle$ of the Hamiltonian ($W_{im} = |\langle\psi_i|\phi_m\rangle|^2$). The first quantity is the inverse participation ratio (IPR)

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

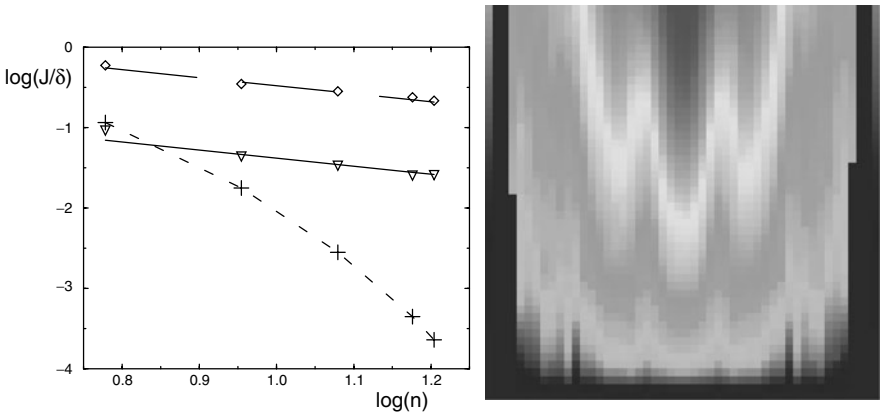

Fig. 12. The plot on the left-hand side shows the dependence of $\log(J_c/\delta)$ (diamonds) and $\log(J_{cs}/\delta)$ (triangles) on $\log(n_q)$; the variation of the scaled multi-qubit spacing ($\log(\Delta_n/\delta)$) with $\log(n_q)$ is shown for comparison (+). J_c is the quantum chaos border determined by level statistics, J_{cs} is the quantum chaos border determined by the beginning of the mixing of quantum register states. The dashed line gives the theoretical formula $J_c = C\delta/n_q$ with $C = 3.3$ and the solid line is $J_{cs} = 0.41\delta/n_q$. The results show that both definitions give the same parametric dependence. The dashed curve is drawn to guide the eye for (+). (Georgeot and Shepelyansky 2000b) The picture on the right-hand side shows the the quantum computer melting induced by the coupling between qubits. The shade of gray is used to represent the level of quantum eigenstate entropy S_q, which measure the mixing of quantum register states in eigenstates of 12, with gray close to maximal ($S_q \approx 11$), black close to minimal ($S_q \approx 0$) and white for intermediate values. The horizontal axis is the energy of the computer eigenstates counted from the ground state to the maximal energy ($\approx 2n_q\Delta$). The vertical axis is the value of J/δ, varying from 0 to 0.5. Here $n_q = 12$, $\delta = \Delta$, $J_c/\delta = 0.273$, and one random realisation of (12) is chosen. (Georgeot and Shepelyansky 2000a)

$\xi = 1/\sum_i |W_{im}|^4$. The second is the quantum eigenstate entropy $S_q = -\sum_i W_{im} \log_2 W_{im}$. One can check that:

— $S_q = 0$ and $\xi = 1$ if $|\phi_m\rangle$ is one quantum register state ($J = 0$)
— $S_q = 1$ and $\xi = 2$ if $|\phi_m\rangle$ is equally composed of two $|\psi_i\rangle$
— in an N-dimensional Hilbert space with $N = 2^{n_q}$, the maximal value are $S_q = n_q$ and $\xi = 2^{n_q}$ if all 2^{n_q} states contribute equally to $|\phi_m\rangle$.

Chaos implies mixing of exponentially many multi-qubit states – ergodicity. This can be understood as a kind of 'melting' of the quantum computer. This leads to the destruction of the computer without coupling to the environment, since its source lies in internal disorder in (12). This process can be quantified through the IPR and entropy: for example, the plot on the right-hand side of Figure 12 shows the entropy of the quantum computer as the interaction strength increases. The melting starts in the band centre where the density of states is largest, and then spreads to most of the Hilbert space. To show in more detail what happens for an individual state, the plot on the left-hand side of Figure 13 shows the projections of a true quantum computer eigenstate of (12) in the basis of quantum

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

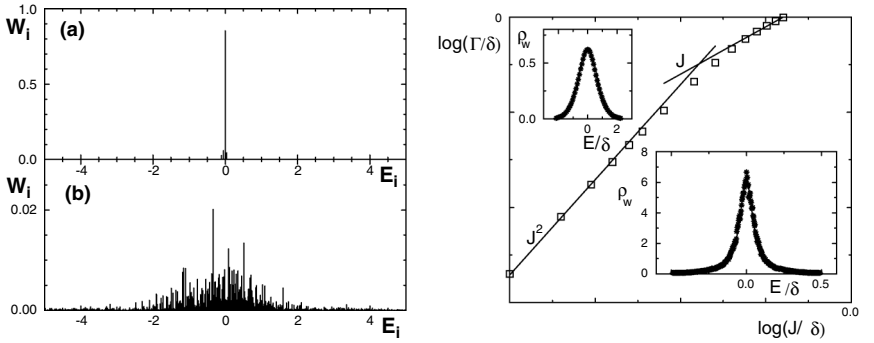

Fig. 13. The plot on the left-hand side shows two quantum computer eigenstates of model (12) in the basis of non-interacting multi-qubit states, that is, $W_i = |<\psi_i|\phi>|^2$ as a function of non-interacting multi-qubit energy E_i for $n_q = 12$ and $\delta = \Delta$ with $J_c/\delta = 0.273$ (see text). For (a) $J/\delta = 0.02$ (below the quantum chaos border) and for (b) $J/\delta = 0.48$ (above the quantum chaos border). (Georgeot and Shepelyansky 2000a) The plot on the right-hand side shows ρ_W for the quantum computer model (12) for $n_q = 15$ and $\delta \ll \Delta$. The inserts show examples of the LDOS for, on the right-hand side, $J/\delta = 0.08$ (Breit–Wigner form) and, on the left-hand side, $J/\delta = 0.4$ (Gaussian form). The main plot shows the dependence of the width Γ on J/δ. The straight lines are $\Gamma = 1.3J^2 n_q/\delta$ (Breit–Wigner theoretical formula) and $\Gamma \propto J$ (Gaussian regime). (Georgeot and Shepelyansky 2000b)

register states. Below the quantum chaos border, such an eigenstate is very close to one quantum register state, while above this border it is composed of a huge number of them.

Another useful related quantity is called the local density of states (LDOS), which is defined by $\rho_W(E-E_i) = \sum_m W_{im}\delta(E-E_m)$, and characterises how quantum register states are spread over the true eigenstates of the perturbed system. In general it has two forms. The first is the Breit–Wigner form

$$\rho_{BW}(E - E_i) = \frac{\Gamma}{2\pi((E-E_i)^2 + \Gamma^2/4)},$$

which is valid when Γ is smaller than the bandwidth ($\Gamma < \sqrt{n_q}\delta$) and many levels are contained inside this width. In this regime, the Breit–Wigner width Γ is given by the Fermi golden rule: $\Gamma = 2\pi U_s^2/\Delta_c$, where U_s is the root mean square of the transition matrix element and $1/\Delta_c$ is the density of directly coupled states. In our case $U_s \sim J$ and $\Delta_c \sim \delta/n_q$, so that $\Gamma \sim \frac{J^2 n_q}{\delta}$. The second form arises for large J, when $\Gamma > \sqrt{n_q}\delta$, and ρ_W becomes close to a Gaussian, whose width grows like $\Gamma \sim J$. The change from one dependence to the other takes place for $J > \delta/n_q^{1/4}$. These two regimes can be seen in the plot on the right-hand side of Figure 13, which shows the LDOS for the model (12). The general theory asserts that for $J > J_c$, all states inside the width Γ are mixed. Thus, for (12) this translates into an estimate of $\xi \approx \Gamma/\Delta_n \sim J^2/(\Delta_c\Delta_n)$ for the IPR.

The theory described above enables us to understand the time scale of the destruction of quantum register states in the different regimes of (12). For $J > J_c$, as these states are far from being eigenstates of (12), they decay with time. If one starts with a quantum register state $|\psi(0)\rangle = |\psi_{i_0}(0)\rangle$, this process can be measured by the fidelity $f(t) = |\langle\psi(t)|\psi_{i_0}(t)\rangle|^2$.

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

It is easy to see that the fidelity decay is the Fourier transform of the local density of states. Thus, for $J > J_c$, the Breit–Wigner form of the LDOS with width Γ implies an exponential decay $\sim e^{-\Gamma t}$, while a Gaussian shape of the LDOS with width Γ implies a Gaussian decay $\sim e^{-\Gamma^2 t^2}$. In both cases the time scale is $\tau \sim 1/\Gamma$ (Georgeot and Shepelyansky 2000b; Flambaum 2000). There will also be phase errors, which are not taken into account in this picture. Therefore, even in the regime of quantum chaos, the computer can be used reliably for some time, although it is eventually destroyed. It has been proposed (Berman *et al.* 2001; Lages and Shepelyansky 2006) that by imposing a gradient in the values of Γ_i in (12), the quantum computer might be more stable against static errors since this can push the quantum chaos border higher in interaction strength. However, this requires some fine-tuning in the parameters of the quantum computer, and its applicability depends on the experimental implementation.

The analysis we have presented so far has been purely static, the quantum computer being at rest with no gate applied. In reality we are interested in a quantum computer doing a calculation, and it is therefore important to assess the effect of static imperfections while the computer is performing some algorithm, such as a simulation of a quantum map of the form (2).

This analysis was performed on a quantum computer simulating the kicked Harper model (6) on an N-dimensional Hilbert space ($N = 2^{n_q}$) through the time-slice algorithm presented in Section 3.1 (Lévi and Georgeot 2004). To investigate such effects, the approximation was made that the Hamiltonian (12) acts during a time τ_g between each gate, which is taken to be instantaneous. A single rescaled parameter ε describes the amplitude of these static errors, with $\varepsilon = \delta\tau_g = J\tau_g$.

For K, L very small, it is known that in the classical kicked Harper model a small chaotic layer appears in phase space surrounding large integrable islands; this is called a 'stochastic web', and has been much studied since quantum transport in this regime is a complicated interplay between classical diffusion through the layer and quantum tunnelling.

In this regime, the effects of static errors were tested on the Husimi distribution (see Figure 14 for an example). The numerical results showed that the relative error is $1/2$ for a time scale $t_h \approx C_h/(\varepsilon n_q^{1.23})$, where C_h is a numerical constant. Thus the phase-space distributions vary polynomially with these static errors as well as in the case of random noise in the gates discussed in Section 4.1.

For larger values of K and L, classical chaos sets in and the quantum dynamics shows dynamical localisation, until a partial delocalisation takes place for increasing K and L. In the localised regime, it is possible to estimate theoretically the effect of static imperfections. It is similar to the analysis given above for the quantum computer at rest, but we should now consider the eigenstates of the evolution operator $\hat{U}$ of the unperturbed system (kicked Harper (6)) instead of the quantum register states.

In the regime where all states are localised with localisation length l, an eigenstate is coupled to only $\sim l$ neighbouring states with typical matrix element $V_{typ} \sim \varepsilon n_g \sqrt{n_q}/\sqrt{l}$, where n_g is the number of gates needed for one iteration of (6) and n_q is the number of qubits. This implies that the quantum chaos border is

$$\varepsilon_c \approx C_1/(n_g \sqrt{n_q}\sqrt{l}) \tag{13}$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

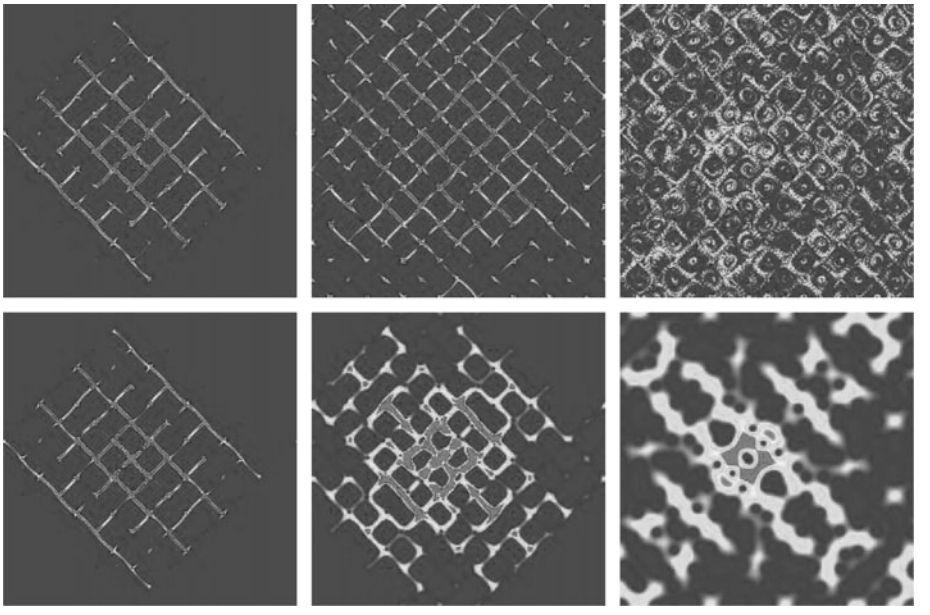

Fig. 14. Example of the Husimi distribution of a wave packet spreading on the stochastic web of (6) in the presence of static errors: here $K = L = 0.5$, $\hbar = 2\pi \times 64/2^{n_q}$ (this is the only figure where there are 8×8 cells, both in momentum and angle directions); the initial state is a Gaussian wave packet of area $\hbar$ started half a cell above the centre of the figure; and 100 iterations have been performed using 2×40 slices per iteration. For the top pictures, $n_q = 14$ and from left to right $\varepsilon = 10^{-6}$, $\varepsilon = 10^{-5}$, $\varepsilon = 10^{-4}$. For the bottom pictures, $\varepsilon = 0$ and from left to right $n_q = 14$, $n_q = 11$, $n_q = 8$. The amplitude of the Husimi function is represented by shades of gray with black representing zero, gray representing maximal values and white representing intermediate values. (Lévi and Georgeot 2004)

where C_1 is a numerical constant. This formula was checked numerically (see Figure 15). For $\varepsilon \ll \varepsilon_c$, the localisation length l can be measured for very long times (no quantum chaos regime), while for $\varepsilon \gg \varepsilon_c$, we get that l can be measured up to $t \sim 1/(\varepsilon n_g \sqrt{n_q})$.

If K and L increase, a certain fraction of the eigenstates of $\hat{U}$ in (6) become delocalised. In this case, the typical matrix element between states with at least one delocalised is $V_{typ} \sim \varepsilon n_g \sqrt{n_q}/\sqrt{N}$, where $N = 2^{n_q}$. This implies that the quantum chaos border should vary as

$$\varepsilon_c \approx C_2/(n_g \sqrt{n_q} \sqrt{N}) \tag{14}$$

where C_2 is a numerical constant. This formula agrees with numerical simulations (see Figure 16). Unlike the localised case, the threshold is now exponentially small since $N = 2^{n_q}$ (see also Benenti *et al.* (2002) where a similar phenomenon was seen on a different system). However, even if, realistically, the quantum chaos regime is unavoidable, $\varepsilon \gg \varepsilon_c$ means that observables are measurable up to time $t \sim 1/(\varepsilon n_g \sqrt{n_q})$.

For other maps of the form (2) displaying quantum chaos, provided one is in a regime where localisation is not visible and eigenfunctions of the simulation evolution operator U are ergodic, one can use Random Matrix Theory to compute the threshold and the

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

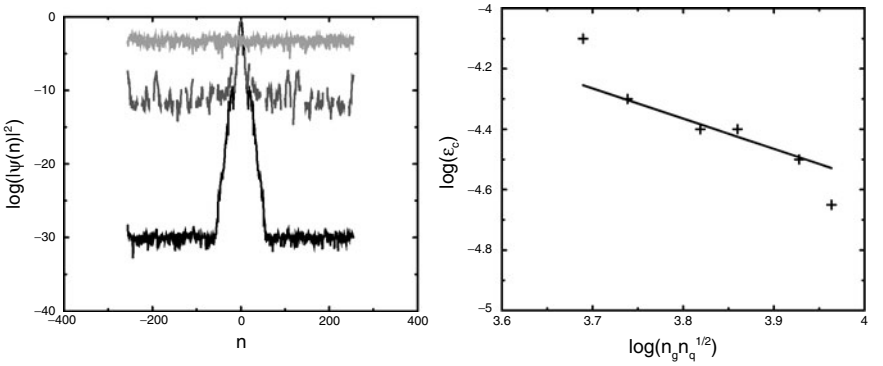

Fig. 15. The plot on the left-hand side shows an example of the wave function after iterations of (6) in the localised regime in the presence of static imperfections: here $K = 1$, $L = 5$, $\hbar/(2\pi) = (13 - \sqrt{5})/82$, the initial state is $|\psi_0\rangle = |0\rangle$, 1000 iterations have been performed using 2×40 slices per iteration, $n_q = 8$, and, from bottom to top, $\varepsilon = 0$ (black, solid line), $\varepsilon = 10^{-7}$ (dark gray, dashed line), $\varepsilon = 10^{-3}$ (light gray, solid line). In the centre, the first two curves are superposed and indistinguishable. The plot on the right-hand side shows the critical value of ε (error strength) as a function of parameters for $K = 2, L = 27$, with other parameter values the same as for the plots on the left-hand side. The solid line is the formula (13). (Lévi and Georgeot 2004)

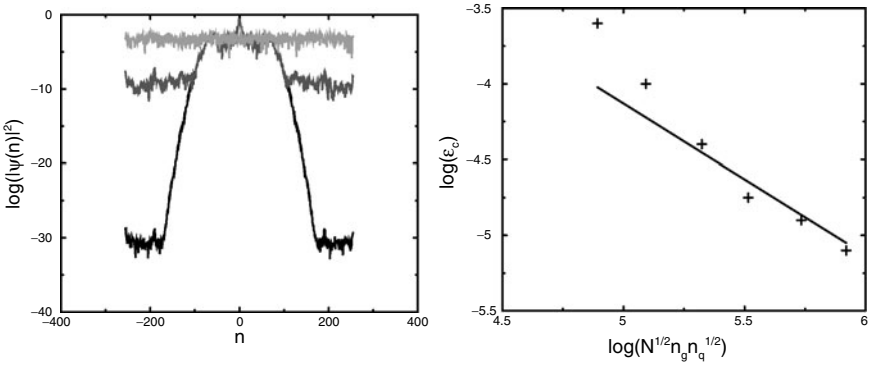

Fig. 16. The plot on the left-hand side shows an example of the wave function after iterations of (6) in the partially delocalised regime in the presence of static imperfections. Here $K = 2$, $L = 5$, $\hbar/(2\pi) = (13 - \sqrt{5})/82$, the initial state is $|\psi_0\rangle = |0\rangle$, 100 iterations have been performed using 2×40 slices per iteration, $n_q = 8$ ($N = 2^{n_q}$), and, from bottom to top, $\varepsilon = 0$ (black, solid line), $\varepsilon = 10^{-7}$ (dark gray, dashed line), $\varepsilon = 10^{-3}$ (light gray, solid line). In the centre, the first two curves are superposed and indistinguishable. The plot on the right-hand side shows the critical value of ε (error strength) as a function of parameters for $K = 10$, $L = 27$ with other parameter values the same as for the plot on the left-hand side. The solid line is the formula (14). (Lévi and Georgeot 2004)

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

time scales. This was done in Frahm *et al.* (2004). It was shown that for fidelities $f(t)$ close to one, we have

$$\ln f(t) \approx -\frac{t}{t_c} - \frac{2t^2}{t_c t_H} \tag{15}$$

where $t_c = \frac{1}{\varepsilon^2 n_q n_g^2}$ and $t_H = 2^{n_q}$ is the Heisenberg time (the inverse of the mean level spacing), and $N = 2^{n_q}$ is the dimension of the Hilbert space, n_g is the number of gates needed for one iteration of the map, and ε is the amplitude of static imperfections. Two regimes are therefore possible:

(i) $t_c < t_H$ or, equivalently, $\varepsilon > \varepsilon_c = 2^{-n_q/2}/(n_g\sqrt{n_q})$: the system is above the quantum chaos threshold ε_c, the first term in (15) dominates, and makes the fidelity decay exponential, as in the case of random errors, though the decay is parametrically faster.

(ii) $t_c > t_H$ or, equivalently, $\varepsilon < \varepsilon_c = 2^{-n_q/2}/(n_g\sqrt{n_q})$: the system is below the quantum chaos threshold ε_c, the second term in (15) dominates, and makes the fidelity decay as a Gaussian, which is very different from the exponential decay of random errors.

As in the case of the partially delocalised regime of the kicked Harper, the quantum chaos border also decreases exponentially with n_q in this result.

The effect of static errors has also been explored for a quantum computer performing the Grover algorithm (Braun 2002; Pomeransky *et al.* 2005), showing that in this case the quantum chaos border decreases polynomially with the number of qubits n_q.

In the above discussion, the static imperfections have generally been found to have parametrically bigger effects than both the random unitary and dissipative errors discussed previously. However, it is interesting to note that it is actually possible to devise quantum error-correcting codes tailored for such types of static imperfections. This method of correction, which was introduced in Kern *et al.* (2005) and called the Pauli Random Error Correction (PAREC) method, is based on repeated application of Pauli operators, which change the computational basis. Interestingly, there is no need to increase the number of qubits, unlike most other quantum error correcting codes. This randomisation procedure eliminates the time-coherence of static errors and the time scales after correction are now similar parametrically to the ones for incoherent errors such as random unitary noise.

5. Complexity, entanglement and interference

In this section we address the question of how to measure the complexity of quantum states. Quantum chaos gives one answer to such questions. Quantum computation can also give a parallel answer: any quantum state can be built from a simple initial state through the action of quantum operations. So the complexity of a quantum process, or of a quantum algorithm, can be used to define the complexity of a state. To understand the construction of complex quantum states from simple initial states, it is important to understand the resources used in quantum manipulation of information, which are not the same as in classical computing. One of them is the superposition principle, which enables us to manipulate as a single state arbitrary superpositions of classical registers. Another resource is entanglement: the non-factorisability of most quantum states into individual

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

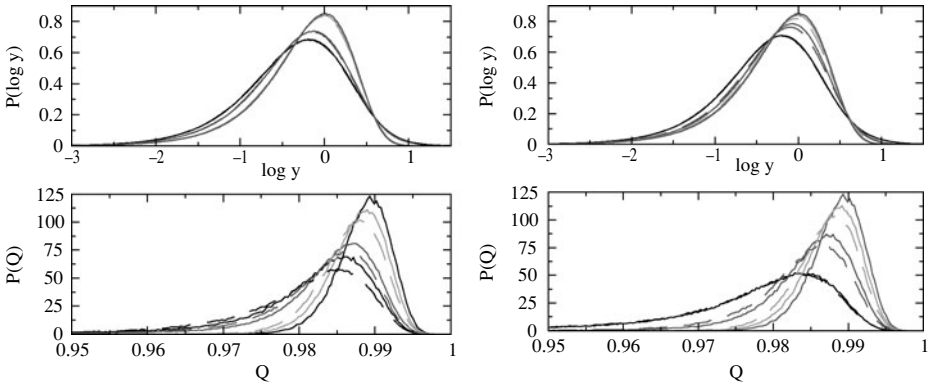

Fig. 17. The plots on the left-hand side show the distributions of matrix elements (top) and Q of column vectors (bottom) for iterates $\hat{U}^n$ of $\hat{U}$ in (5) for $N = 2^9$, in momentum representation. Matrix elements x are rescaled by $y = N|x|^2$. From lowest to topmost curve: black is $\alpha = 1/3$, dark gray is $\alpha = 1/5$, light gray is $\alpha = (1 + \sqrt{5})/2$, intermediate gray is the random matrix result. The plots on the right-hand side are the same as those on the left for iterates of a random phase model where in (5) the first operator is replaced by random phases, for $N = 2^8$. (Giraud and Georgeot 2005)

qubit states. Finally, quantum computing uses interferences between different registers as a resource. In this section we will look more closely at the production of entanglement and interference in quantum processes, pointing out the links, where they exist, with the quantum chaos concepts.

5.1. *Entanglement and quantum chaos*

It is well known that entanglement is an important resource that is specifically quantum and is produced in large quantities in efficient quantum algorithms. It has even been suggested that the amount of entanglement measures the difficulty of simulating a quantum state classically. Remarkably, entanglement and quantum chaos have been shown to be linked. Indeed, several studies have shown that quantum chaotic maps of the form (2) are good producers of entanglement. Indeed, the entanglement of Random Matrix column vectors or eigenvectors gets closer and closer to the maximal value as the size of matrices increases. Parallel to this, it has been shown that several quantum chaotic maps exhibit distributions of entanglement among column vectors (after many iterates) or eigenvectors which are close to the values for Random Matrices (Bandyopadhyay and Lakshminarayan 2002; Scott and Caves 2003; Weinstein and Hellberg 2005). To illustrate this point, Figure 17 shows the matrix element and entanglement distributions for the map (5) and a random phase version of it, for different values of α. The classical map corresponding to (5) is ergodic and mixing for α irrational, and in this case the quantum evolution operator has eigenvalues following Random Matrix predictions. The entanglement in Figure 17 is measured by the average bipartite entanglement between

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

one qubit and the rest of the system

$$Q = 2 - 2/n_q \sum_{k=1}^{n_q} \mathrm{Tr}\rho_k^2,$$

where ρ_k is the density operator corresponding to the k-th qubit after having traced out the rest, and n_q is the number of qubits. This Q is a popular measure of entanglement called the Meyer–Wallach measure. For irrational α, the distribution of Q for column vectors is very close to the Random Matrix prediction, which, in turn, for large matrices is close to the maximal value. For rational α, the map (5) is not chaotic and not integrable, and the evolution operator eigenvalues are intermediate between Random Matrices and Poisson. Figure 17 shows that in this case the entanglement distribution as well as the matrix element distribution departs from Random Matrix results, in a parallel way. The distribution of Q gets further from the maximal value as the matrix elements are far from Random Matrix predictions. In this system, as one get further from quantum chaos, the less entangled one becomes.

A further confirmation of this link between entanglement and quantum chaos has been observed in many-body systems. Indeed, it was shown in Mejia-Monasterio *et al.* (2005) that the Hamiltonian (12) of Section 4.3 displays a large increase in bipartite entanglement once the interaction becomes larger than the quantum chaos border. Actually, the existence of this link inspired the construction of pseudo-random operators based on quantum chaotic maps, which efficiently mimic random operators with Random Matrix statistics of entanglement (Emerson *et al.* 2003).

5.2. *Entanglement and interference in quantum algorithms*

Although entanglement has been much studied and many competing measures are available for it, this is not the case for interference, which is, in a sense, more mysterious. Indeed, interference cannot be easily associated with a state in isolation, but only with a process, and it obviously depends on the basis chosen. Nevertheless, a measure of interference was proposed in Braun and Georgeot (2006). This allows us to compare interference and entanglement production in quantum algorithms, including the quantum chaos algorithms of Section 3.1.

To explain this measure of interference, consider a process mapping density matrices ρ to density matrices ρ' in an N-dimensional Hilbert space through $\rho'_{ij} = \sum_{k,l} P_{ij,kl}\rho_{kl}$, and let us start with a pure initial state, $\rho = |\psi\rangle\langle\psi|$, with $|\psi\rangle = \sum_{j=1}^{N} a_j|j\rangle$, with phases φ_j such that $a_j = |a_j|\exp(i\varphi_j)$. One can define a real phase sensitivity matrix S, which measure how probabilities $|\rho'_{ii}|$ are affected by the phases φ_j, with matrix elements $S_{il} = \partial p'_i/\partial\varphi_l$. The interference measure is obtained by taking the trace of SS^T, averaging it over all initial phases, and applying it to an equipartitioned state with $|a_i| = 1/\sqrt{N}$ for all $i = 1, \ldots, N$.

This procedure defines the interference measure by

$$\mathscr{I}(P) = \sum_{i,k,l} |P_{ii,kl}|^2 - \sum_{i,k} |P_{ii,kk}|^2. \tag{16}$$

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

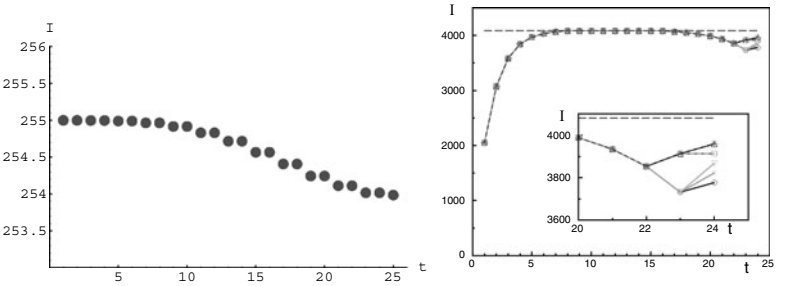

Fig. 18. Potentially available interference. The plot on the left shows the accumulated interference up to and including step number t in Grover's algorithm for $n_q = 8$ qubits. One Grover iteration corresponds to four steps in the plot. The plot on the right shows the accumulated interference up to and including step number t generated during Shor's algorithm for factorisation of $R = 15$ (finding the period of $f(x) = a^x \pmod R$ on $n_q = 12$ qubits, where the first four qubits hold the values of x and the next eight the values of $f(x)$). Values of a are $a = 13$ (circles, full line), $a = 7$ (squares, dashed line), $a = 11$ (diamonds, full line), $a = 8$ (triangles, full line), $a = 14$ (inverted triangles, full line), $a = 4$ (crosses, full line), $a = 2$ (stars, dashed line). Data for different values of a differ only for the last two time steps. The horizontal dashed red line is the maximum possible value of interference for an untouched second register, $\mathscr{I} = 2^{n_q} - 2^L = 4080$. The inset shows the same curves for the last steps on a different scale. Lines are there to guide the eye only. Massive interference $\mathscr{I} = 2^n - 2^L$ (or almost n i-bits) is generated during the application of the Walsh–Hadamard gate (part 1, first eight points). Interference is unchanged in part 2 (next eight points), and decreases during the final part (quantum Fourier transform) (final eight points). (Braun and Georgeot 2006)

For unitary processes described by an $N \times N$ unitary matrix U, it becomes

$$\mathscr{I}(P(U)) = \left(N - \sum_{i,k} |U_{ik}|^4 \right). \tag{17}$$

The measure (16) allows us to define a unit of interference, the 'i-bit'; the number of 'i-bits' in a process is $n_I = \log_2(\mathscr{I}(P) + 1)$. In the case of unitary processes, the measure (17) verifies $0 \leqslant \mathscr{I}(P(U)) \leqslant N - 1$. Note that it can be related to the inverse participation ratio (IPR) is defined in Section 4.3, applied to all column vectors of the matrix. One can easily verify that (17) gives the expected results for some specific cases. Indeed, for a process described by a permutation matrix, we have $\mathscr{I}(P(U)) = 0$, that is, no interference is produced by swapping states. On the other hand, for Fourier and Walsh–Hadamard transforms, $\mathscr{I}(P(U)) = N - 1$, so the maximal value is reached.

It is instructive to use the interference measure to quantify interference production in the most famous quantum algorithms: those of Grover and Shor. The results are shown in Figure 18. It turns out that both algorithms generate an exponential amount of interference right at the beginning, as they start out with the Walsh–Hadamard transform on many qubits. At the end, the information extraction, which concentrates probability on a small subspace, reduces the total interference produced from the beginning. An alternative approach is to calculate, instead of this 'potentially available interference',

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

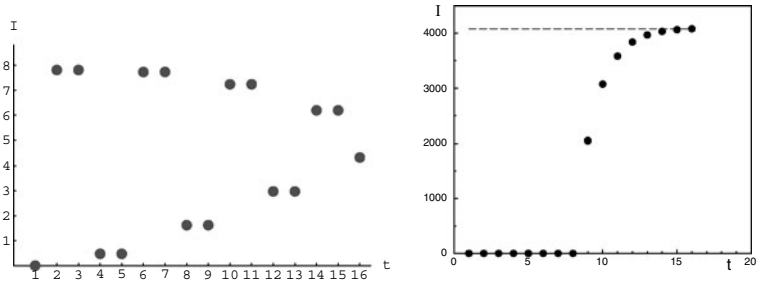

Fig. 19. Actually used interference. The plot on the left-hand side shows the accumulated interference up to and including step number t generated during Grover's algorithm, excluding the initial Walsh–Hadamard transform, for $n_q = 7$ qubits. The step number on the t-axis is shifted by one compared to Figure 18 (left), that is, step 1 is now the first application of the oracle, which does not lead to interference. The accumulated interference is changed only during the following steps. The maximum value $\mathscr{I} \simeq 8$ is asymptotically independent of the number of qubits. The plot on the right-hand side shows the accumulated interference up to and including step number t generated during Shor's algorithm, excluding the initial Walsh–Hadamard transform for factorisation of $R = 15$ ($n_q = 12$ qubits). The step number on the t-axis is the same as in Figure 18 (right) but shifted by 8. The horizontal dashed red line is the maximum possible value of interference for transformations of the first register alone $\mathscr{I} = 4080$. The accumulated interference is changed only during the final quantum Fourier transform, and does not depend on the value of a. (Braun and Georgeot 2006)

the accumulated interference for the algorithm without the initial Walsh–Hadamard transform, which amounts to a change in the initial state. The results for this 'actually used interference' are given in Figure 19 and show that in this case the production of interference is small in Grover's algorithm, while it remains exponential in the case of Shor's algorithm. This result may be related to the fact that the former only has polynomial efficiency, while the latter has exponential efficiency. The high level of interference produced in Shor's algorithm may also be related to the fact that the operator performing this algorithm has quantum chaotic properties, such as spectral statistics in agreement with Random Matrix Theory (Maity and Lakshminarayan 2006).

Interestingly enough, if one now looks at entanglement production for both algorithms, there is a sort of symmetry. Indeed, each Grover iteration can be divided into four operators, two of them (Walsh–Hadamard transforms) producing interference but no entanglement (products of one-qubit gates), and two of them (changes in the phase of amplitudes) creating entanglement but no interference. In the same way, the three parts of Shor's algorithm consist of two phases producing interference but little entanglement (an initial Walsh–Hadamard transform and a final Fourier transform), and one producing massive entanglement but no interference (the computation of the modular exponentiation function $f(x)$). This is also true for quantum chaos algorithms such as, for example, the simulation of the kicked rotator presented in Section 3.1. Indeed, one iteration of the map requires, essentially, four phases in the computation: two of them are quantum Fourier transforms creating little entanglement but vast amounts of interference; and two

https://doi.org/10.1017/S0960129507006366 Published online by Cambridge University Press

of them are diagonal multiplications (which correspond to multiplication by diagonal matrices) and the computation of a function on another register (which corresponds to multiplication by permutation matrices), yielding no interference but a large amount of entanglement.

6. Conclusion

In this paper I have reviewed a recent body of work, including my own, which connects the fields of classical and quantum chaos with quantum information and computation. Three main connections can be discerned. As chaos is, in a sense, a science of complex systems, it is a source of problems that are difficult to tackle with classical computation and are good candidates for a quantum speed-up. It turns out that the simulation of such systems can be faster on a quantum computer than classically: the gain can be exponential or polynomial, depending on the system considered and the observable we are interested in. As many physical systems display chaotic properties, this gives new practical applications for quantum computing. Another very important feature of these algorithms is that they can sometimes be very economical in the number of gates and qubits required. This makes them a good choice for testing the small-scale quantum computers currently being built, and explains why some of them have already been implemented experimentally.

A second connection between chaos and quantum computing is in error analysis. Quantum algorithms for chaotic physical systems are very versatile and varied, and permit a thorough analysis of the effect of different types of errors on the outcome of a quantum computation. Furthermore, the tools of quantum chaos can be applied to the quantum computer as a physical system in order to investigate the effects of certain types of errors such as static errors.

A final connection is related to the resources of quantum computation: the complexity of quantum chaotic systems reflects itself in high degrees of entanglement. We have also made a proposal to quantify interference, and this resource may also be produced in large amounts for chaotic systems.

The results presented in this paper show that the concepts of complexity due to chaos and complexity in the sense of information theory are not totally disconnected. This recent interplay between two exciting fields of science should go on to give some new insights to both of them in the future.

Acknowledgements

I would like to thank Benjamin Lévi, Marcelo Terraneo, Olivier Giraud, Daniel Braun and especially Dima Shepelyansky for many discussions and collaborations in this field. Thanks are also due to Calmip in Toulouse and Idris in Orsay for access to their supercomputers. This work was supported in part by the EC IST-FET project EuroSQIP and by the French Agence Nationale de la Recherche (ANR) project INFOSYSQQ.

References

Åberg, S. (1990) Onset of chaos in rapidly rotating nuclei. *Phys. Rev. Lett.* **64** 3119–3122.

Abrams, D. S. and Lloyd, S. (1999) Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors. *Phys. Rev. Lett.* **83** 5162–5165.

Bandyopadhyay, J. N and Lakshminarayan, A. (2002) Testing Statistical Bounds on Entanglement Using Quantum Chaos. *Phys. Rev. Lett.* **89** 060402.

Benenti, G., Casati, G., Montangero, S. and Shepelyansky, D. L. (2001) Efficient quantum computing of complex dynamics. *Phys. Rev. Lett.* **87** 227901.

Benenti, G., Casati, G., Montangero, S. and Shepelyansky, D. L. (2002) Eigenstates of operating quantum computer: hypersensitivity to static imperfections. *Eur. Phys. J. D* **20** 293–296.

Benenti, G., Casati, G., Montangero, S. and Shepelyansky, D. L. (2003) Dynamical localization simulated on a few qubits quantum computer. *Phys. Rev. A* **67** 052312.

Benenti, G., Casati, G. and Strini, G. (2004) *Principles of quantum computation and information*, World Scientific.

Berman, G. P., Borgonovi, F., Izrailev, F. M. and Tsifrinovich, V. I. (2001) Avoiding quantum chaos in quantum computation. *Phys. Rev. E* **65** 015204.

Berry, M. V. and Tabor, M. (1977) Level clustering in the regular spectrum. *Proc. R. Soc. London Ser. A* **356** 375–394.

Bohigas, O., Giannoni, M.-J. and Schmit, C. (1984) Characterization of Chaotic Quantum Spectra and Universality of Level Fluctuation Laws. *Phys. Rev. Lett.* **52** 1–4.

Brassard, G., Høyer, P., Mosca, M. and Tapp, A. (2002) Quantum Amplitude Amplification and Estimation. In: Lomonaco, S. J., Jr. and Brandt, H. E. (eds.) *Quantum Computation and Quantum Information: A Millenium Volume*, Contemporary Mathematics Series **305**, AMS.

Braun, D. (2002) Quantum chaos and quantum algorithms. *Phys. Rev. A* **65** 042317.

Braun, D. and Georgeot, B. (2006) Quantitative measure of interference. *Phys. Rev. A* **73** 022314.

Emerson, J., Weinstein, Y. S., Lloyd, S. and Cory, D. G. (2002) Fidelity Decay as an Efficient Indicator of Quantum Chaos. *Phys. Rev. Lett.* **89** 284102.

Emerson, J., Weinstein, Y. S., Saraceno, M., Lloyd, S. and Cory, D. G. (2003) Pseudo-Random Unitary Operators for Quantum Information Processing. *Science* **302** 2098.

Feynman, R. P. (1986) Quantum mechanical computers. *Found. Phys.* **16** 507.

Flambaum, V. V. (2000) Time dynamics in chaotic many-body systems: can chaos destroy a quantum computer? *Aust. J. Phys.* **53** 489.

Frahm, K. M., Fleckinger, R. and Shepelyansky, D. L. (2004) Quantum chaos and random matrix theory for fidelity decay in quantum computations with static imperfections. *Eur. Phys. J. D* **29** 139–155.

Georgeot, B. (2004) Quantum computing of Poincaré recurrences and periodic orbits. *Phys. Rev. A* **69** 032301.

Georgeot, B. and Shepelyansky, D. L. (2000a) Quantum chaos border for quantum computing. *Phys. Rev. E* **62** 3504.

Georgeot, B. and Shepelyansky, D. L. (2000b) Emergence of quantum chaos in the quantum computer core and how to manage it. *Phys. Rev. E* **62** 6366.

Georgeot, B. and Shepelyansky, D. L. (2001a) Exponential gain in quantum computing of quantum chaos and localization *Phys. Rev. Lett.* **86** 2890–2893.

Georgeot, B. and Shepelyansky, D. L. (2001b) Stable quantum computation of unstable classical chaos. *Phys. Rev. Lett.* **86** 5393–5396.

Georgeot, B. and Shepelyansky, D. L. (2002) Georgeot and Shepelyansky reply. *Phys. Rev. Lett.* **88** 219802.

Giraud, O. and Georgeot, B. (2005) Intermediate quantum maps for quantum computation. *Phys. Rev. A* **72** 042312.

Giraud, O., Georgeot, B. and Shepelyansky, D. L. (2005) Quantum computing of delocalization in small-world networks. *Phys. Rev. E* **72** 036203.

Grover, L. K. (1997) Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **79** 325–328.

Gutzwiller, M. C. (1990) *Chaos in Classical and Quantum Mechanics*, Springer.

Henry, M. K., Emerson, J., Martinez, R. and Cory, D. G. (2006) Localization in the quantum sawtooth map emulated on a quantum information processor. *Phys. Rev. A* **74** 062317.

Jacquod, P. and Shepelyansky, D. L. (1997) Emergence of Quantum Chaos in Finite Interacting Fermi Systems. *Phys. Rev. Lett.* **79** 1837–1840.

Kern, O., Alber, G. and Shepelyansky, D. L. (2005) Quantum error correction of coherent errors by randomization. *Eur. Phys. J. D* **32** 153–156.

Kitaev, A. (1995) Quantum measurements and the Abelian Stabilizer Problem. Preprint quant-ph/9511026.

Lages, J. and Shepelyansky, D. L. (2006) Suppression of quantum chaos in a quantum computer hardware. *Phys. Rev. E* **74** 026208.

Lee, J. W. and Shepelyansky, D. L. (2005) Quantum chaos algorithms and dissipative decoherence with quantum trajectories. *Phys. Rev. E* **71** 056202.

Lévi, B. and Georgeot, B. (2004) Quantum Computation of a Complex System: the Kicked Harper Model. *Phys. Rev. E* **70** 056218.

Lévi, B., Georgeot, B. and Shepelyansky, D. L. (2003) Quantum computing of quantum chaos in the kicked rotator model. *Phys. Rev. E* **67** 046220.

Lichtenberg, A. and Lieberman, M. (1992) *Regular and Chaotic Dynamics*, Springer.

Lloyd, S. (1996) Universal quantum simulators. *Science* **273** 1073–1078.

Maity, K. and Lakshminarayan, A. (2006) Quantum chaos in the spectrum of operators used in Shor's algorithm. *Phys. Rev. E* **74** 035203.

Mejia-Monasterio, C., Benenti, G., Carlo, G. G. and Casati, G. (2005) Entanglement across a transition to quantum chaos. *Phys. Rev. A* **71** 062324.

Miquel, C., Paz, J. P., Saraceno, M., Knill, E., Laflamme, R. and Negrevergne, C. (2002) Tomography and spectroscopy as quantum computations. *Nature* **418** 59.

Nielsen, M. A. and Chuang, I. L. (2000) *Quantum computation and quantum information*, Cambridge University Press.

Ott, E. (1993) *Chaos in Dynamical Systems*, Cambridge University Press.

Paz, J. P., Roncaglia, A. J. and Saraceno, M. (2004) Quantum algorithms for phase space tomography. *Phys. Rev. A* **69** 032312.

Pomeransky, A. A. and Shepelyansky, D. L. (2004) Quantum computation of the Anderson transition in the presence of imperfections. *Phys. Rev. A* **69** 014302.

Pomeransky, A. A., Zhirov, O. V. and Shepelyansky, D. L. (2004) Phase diagram for the Grover algorithm with static imperfections. *Eur. Phys. J. D* **31** 131–135.

Poulin, D., Laflamme, R., Milburn, G. and Paz, J. P. (2003) Testing integrability with a single bit of quantum information. *Phys. Rev. A* **68** 022302.

Preskill, J. (1998) Quantum information and computation. Webcourse available at `http://www.theory.caltech.edu/people/preskill/ph229/`.

Ryan, A. C., Emerson, J., Poulin, D., Negrevergne, C. and Laflamme, R. (2005) Characterization of Complex Quantum Dynamics with a Scalable NMR Information Processor. *Phys. Rev. Lett.* **95** 250502.

Schack, R. (1998) Using a quantum computer to investigate quantum chaos. *Phys. Rev. A* **57** 1634.

Scott, A. and Caves, C. (2003) Entangling power of the quantum baker's map. *J. Phys. A* **36** 9553.

Shor, P. W. (1994) Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: Goldwasser, S. (ed.) *Proc. 35th Annu. Symp. Foundations of Computer Science*, IEEE Computer Society.

Song, P. H. and Shepelyansky, D. L. (2001) Quantum computing of quantum chaos and imperfection effects. *Phys. Rev. Lett.* **86** 2162–2165.

Steane, A. (1998) Quantum Computing. *Rep. Progr. Phys.* **61** 117.

Terraneo, M., Georgeot, B. and Shepelyansky, D. L. (2003) Strange attractor simulated on a quantum computer. *Eur. Phys. J. D* **22** 127–130.

Terraneo, M., Georgeot, B. and Shepelyansky, D. L. (2005) Quantum computation and analysis of Wigner and Husimi functions: toward a quantum image treatment. *Phys. Rev. E* **71** 066215.

Weinstein, Y. S. and Hellberg, C. S. (2005) Entanglement Generation of Nearly Random Operators. *Phys. Rev. Lett.* **95** 030501.

Zhirov, O. V. and Shepelyansky, D. L. (2006) Dissipative decoherence in the Grover algorithm. *Eur. Phys. J. D* **38** 405–408.