SCIENTIFIC REPORTS

OPEN

Exponential Sensitivity and its Cost in Quantum Physics

András Gilyén[1,2], Tamás Kiss[1] & Igor Jex[3]

State selective protocols, like entanglement purification, lead to an essentially non-linear quantum evolution, unusual in naturally occurring quantum processes. Sensitivity to initial states in quantum systems, stemming from such non-linear dynamics, is a promising perspective for applications. Here we demonstrate that chaotic behaviour is a rather generic feature in state selective protocols: exponential sensitivity can exist for all initial states in an experimentally realisable optical scheme. Moreover, any complex rational polynomial map, including the example of the Mandelbrot set, can be directly realised. In state selective protocols, one needs an ensemble of initial states, the size of which decreases with each iteration. We prove that exponential sensitivity to initial states in any quantum system has to be related to downsizing the initial ensemble also exponentially. Our results show that magnifying initial differences of quantum states (a Schrödinger microscope) is possible; however, there is a strict bound on the number of copies needed.

Quantum technology progresses at a fast pace. Preparation, control and measurement of coherent quantum systems[1] became possible on an unprecedented level leading to a wealth of proposals of applications ranging from quantum information processing to high precision measurements and sensors. In these protocols, increasingly sophisticated sequences of coherent evolution, measurement and post-selection are applied in order to control the state of quantum systems. Dynamics achieved by state selective protocols was proven essential for a large number of quantum information protocols[2,3] and quantum communication[4]. Prominent examples of probabilistic protocols are the KLM scheme[2] for linear optical quantum gates or the entanglement purification protocols[5–7] employing measurement and selection in order to increase the entanglement between subsystems.

Manipulation by measurement and selection breaks the linearity of quantum mechanics, thereby broadening the possibilities for quantum evolution[8–11]. In contrast, in the well established field of quantum chaos[12] one studies the signatures of chaos in closed quantum systems with linear evolution. In such systems the linearity of time evolution prevents distance growing between two initial quantum states. However, the essential non-linearity of an iterated, state selective protocol can result in truly chaotic behaviour[13–15], meaning that initially close quantum states can get separated rapidly. The existence of such sensitive quantum protocols has been shown in[13], but sensitivity was proved only for a tiny fractal subset of initial states having zero measure. In this article we demonstrate that exponential sensitivity can exist for all initial states in an experimentally realisable optical scheme. Moreover, we show that any complex rational polynomial map, including the example of the Mandelbrot maps[16], can be directly realised using state selective protocols, bringing a whole new class of quantum protocols to life.

From a fundamental point of view, one can search for the most general evolution for a quantum system. A very general dynamics is sometimes imagined as the action of both unitary evolution and non-selective measurements on a system together with one or more ancillas. The evolution reduced for the system only is called a quantum channel. When talking about quantum states in practice, it is unavoidable to be able to repeat experiments on an ensemble of identically prepared initial states in order to uncover the underlying probabilistic laws. This ensemble view of quantum states allows for the following trick when designing the most general dynamics for a given initial state. Let us, for example, consider systems from the ensemble pairwise and let them interact with each other. After the interaction one can perform a measurement on one of the pairs and then discard the measured member of the pair. In case of selective measurement, one may also discard the unmeasured member of the pair, depending on the measurement result. The resulting ensemble will be reduced in size, but some of its properties may be changed in a beneficial way, e.g. entanglement between subsystems. The above procedure goes beyond the usual

[1]Institute for Solid State Physics and Optics, Wigner Research Centre for Physics, Hungarian Academy of Sciences, Budapest, H-1121, Hungary. [2]Department of Theoretical Physics, Budapest University of Technology and Economics, Budapest, H-1111, Hungary. [3]Faculty of Nuclear Sciences and Physical Engineering, Czech Technical University in Prague, Prague, 115 19 Praha 1, Czech Republic. Correspondence and requests for materials should be addressed to A.G. (email: gilyen.andras@wigner.mta.hu)

notion of quantum channels in the following sense. The initial step of the procedure, namely taking the systems pairwise, can be viewed as splitting the original ensemble into two parts and employing one part as an ancilla. In other words, the state of the ancilla will be dependent on the state of the system. The state dependent ancilla lies at the heart of the non-linearity of the process.

Results

A linear optical experimental scheme implementing a family of non-linear maps.

We propose here a simple experimental setup that implements a non-linear process exhibiting exponential sensitivity to the initial state. Our scheme is inspired by an experimentally tractable entanglement purification protocol[17,18] and uses only linear optical elements. At the beginning of each iterative step we form pairs of photonic qubits from the ensemble of identically prepared photons and apply a post-selective transformation on the pairs. After measuring the polarization of one photon we either keep or discard the other photon depending on the measurement result. The post-selection induces a non-linear, deterministic transformation on the remaining photons; therefore, the kept photons remain identically prepared.

The key element of our scheme is the polarizing beam splitter (PBS). When two photons arrive at the same time but from different spatial input modes, this linear optical element introduces entanglement between the spatial modes and the polarization degrees of freedom, see Fig. 1. We apply post-selection and accept the output of the PBS only if there is a photon in both spatial output modes.

Let $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states for our photonic qubits. Consider the effect of the PBS acting on a product state of two incoming photons:

$$
\begin{aligned}
&(\alpha|H\rangle + \beta|V\rangle)_1 \otimes (\alpha|H\rangle + \beta|V\rangle)_2 \\
&\quad \rightarrow \alpha^2|H\rangle_3|H\rangle_4 + \beta^2|V\rangle_3|V\rangle_4 + \alpha\beta\left(|H,V\rangle_3 + |H,V\rangle_4\right)
\end{aligned}
\tag{1}
$$

After post-selection the remaining quantum state is

$$
\begin{aligned}
&N\left(\alpha^2|H\rangle_3|H\rangle_4 + \beta^2|V\rangle_3|V\rangle_4\right) \\
&\quad = \frac{N}{\sqrt{2}}\left((\alpha^2|H\rangle + \beta^2|V\rangle)_3|+\rangle_4 + (\alpha^2|H\rangle - \beta^2|V\rangle)_3|-\rangle_4\right)
\end{aligned}
\tag{2}
$$

where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ and $N = 1/\sqrt{|\alpha|^4 + |\beta|^4}$ is a norming factor. The success probability of the protocol is $1/N^2 \geq 1/2$. If we measure the photon at output mode 4 in the basis $\{|+\rangle, |-\rangle\}$, then the other photon collapses to $N \cdot (\alpha^2|H\rangle \pm \beta^2|V\rangle)$ corresponding to the measurement result. To get a definite outcome $\alpha^2|H\rangle + \beta^2|V\rangle$ we may apply a Pauli-Z gate whenever we measure $|-\rangle$ (Fig. 1(f)) or simply neglect such cases, introducing another level of post-selection (Fig. 1(g)). Either way the protocol implements a non-linear transformation $S: \alpha|H\rangle + \beta|V\rangle \mapsto N \cdot (\alpha^2|H\rangle + \beta^2|V\rangle)$ which maps the identical qubit states of an ensemble to another qubit state of a smaller identical ensemble. If we iterate this process S amended with an additional unitary step U, the iterates $(US)^n$ exhibit increasingly rich dynamics.

It has been shown[13] that by iteratively applying US on an ensemble of identically prepared qubits, the one qubit state of the ensemble after n iterations $|\psi_n\rangle = \alpha_n|H\rangle + \beta_n|V\rangle$ may evolve sensitively. By sensitivity we mean that for some initially similar quantum states $|\psi_0\rangle$, $|\psi_0'\rangle$ the evolving states $|\psi_n\rangle$, $|\psi_n'\rangle$ can get very different during iteration, i.e. using some quantum information distance d (e.g. the Bures distance) we can get $d(|\psi_n\rangle, |\psi_n'\rangle) \gg d(|\psi_0\rangle, |\psi_0'\rangle)$. More precisely we call the process sensitive at some initial state $|\psi_0\rangle$ if arbitrarily close quantum states can get separated from it to a constant distance C, i.e. $\forall \varepsilon > 0, \exists |\psi_0'\rangle: d(|\psi_0\rangle, |\psi_0'\rangle) < \varepsilon, d(|\psi_n\rangle, |\psi_n'\rangle) > C$. We call this exponential sensitivity if it also holds requiring $n \sim \log(1/\varepsilon)$.

Sensitivity has been shown for initial states lying on a fractal subset of the Bloch sphere called the Julia set[16,19], see Fig. 2. The specific fractals that were examined regarding the protocol US[13] all had zero measure. However certain choices of unitaries from the family $U_{\theta,\varphi} = \begin{bmatrix} \cos(\theta) & \sin(\theta)e^{i\varphi} \\ -\sin(\theta)e^{-i\varphi} & \cos(\theta) \end{bmatrix}$ seem to produce increasingly saturated Julia set images (see Fig. 2) suggesting that it may reach a point where the whole Bloch sphere is covered by sensitive initial states. A candidate for such a transformation is $\Phi = U_{\pi/4,\pi/2}S$, where $U_{\pi/4,\pi/2} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$.

Exponential sensitivity for all initial states.

In order to handle the arising non-linear maps better we project the surface of the Bloch sphere to the complex plane using stereographic projection. Thus a (photonic) qubit $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ may be described using a single complex parameter including infinity: $z = \frac{\alpha}{\beta} \in \hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. This representation yields ($\rightsquigarrow$) a new description of our protocol in terms of rational functions[16,19]:

$$
\psi \rightsquigarrow z = \frac{\alpha}{\beta}; \quad S \rightsquigarrow s: z \rightarrow z^2; \quad \Phi \rightsquigarrow f: z \rightarrow \frac{z^2 + i}{iz^2 + 1}
\tag{3}
$$

Using this formalism, it turns out that f is one of a few special so-called Lattès maps[20] and as such has gained a lot of attention in the theory of complex dynamical systems[19]. We can better understand the special properties of our Lattès map by analysing its relationship to the corresponding linear transformation of the 2 dimensional torus. We will represent the torus $\mathbb{C}/\mathbb{Z}[i]$ as the complex plane modulo the Gaussian integers
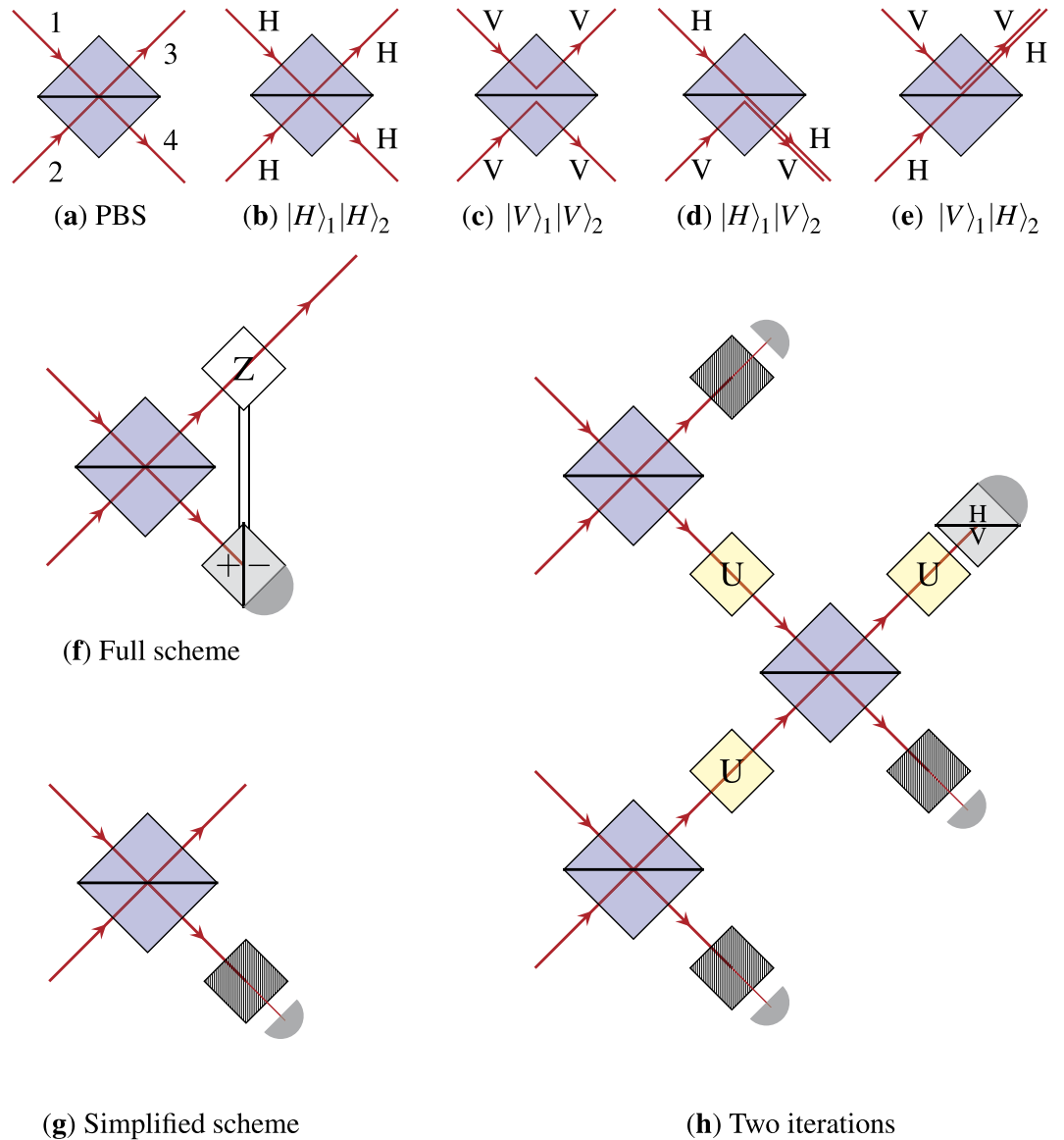
Figure 1. The proposed experimental setup. (**a**) A Polarizing beam splitter (PBS) with two spatial input/output modes. (**b–e**) The effect of the PBS acting on the four possible two photon input states regarding polarizations. (**f**) A post-selective linear optical scheme inducing a non-linear transformation (**g**) and its simplified version utilising a polarizer reducing the success probability by 1/2. (**h**) A two level scheme amended by a unitary transformation U acting on the polarization state of the photons. We consider a run of this experimental setup successful if all the detectors click. This condition introduces the post-selection to the system.

$\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$. Its transformation is represented by multiplication with $\cdot(1 - i)$: $\tilde{z} \to (1 - i) \cdot \tilde{z} \mod (1, i)$, which rotates and folds the torus 2 times over itself. The correspondence between the torus and the sphere is established via the so called Weierstrass elliptic function[21] $\wp: \mathbb{C}/\mathbb{Z}[i] \mapsto \hat{\mathbb{C}}$. Relating the two surfaces gives rise to the identity $f^{\circ n}(z) = \wp((1 - i)^n \cdot \wp^{-1}(z))$ showing that iterating f on $\hat{\mathbb{C}}$ has essentially the same effect as repeatedly applying multiplication $\cdot(1 - i)$ on $\mathbb{C}/\mathbb{Z}[i]$, see Fig. 3 and Methods.

Viewing Φ through these glasses it becomes clear that it shows chaotic behaviour on the whole Bloch sphere. The map representing Φ on the torus uniformly stretches the surface of the torus by a factor of $\sqrt{2}$ and folds over itself two times. It is intuitively clear that the iterative application of such a transformation shows exponential sensitivity to the initial position on the torus and has a positive Lyapunov exponent. Even more strikingly, it exhibits exponential mixing, yielding that during the iteration of Φ even a tiny uncertainty about the initial state evolves exponentially fast to a complete uncertainty, meaning that the iterated state may be any point of the Bloch sphere, as depicted on Fig. 3. For a rigorous derivation of the exponential mixing see Methods.
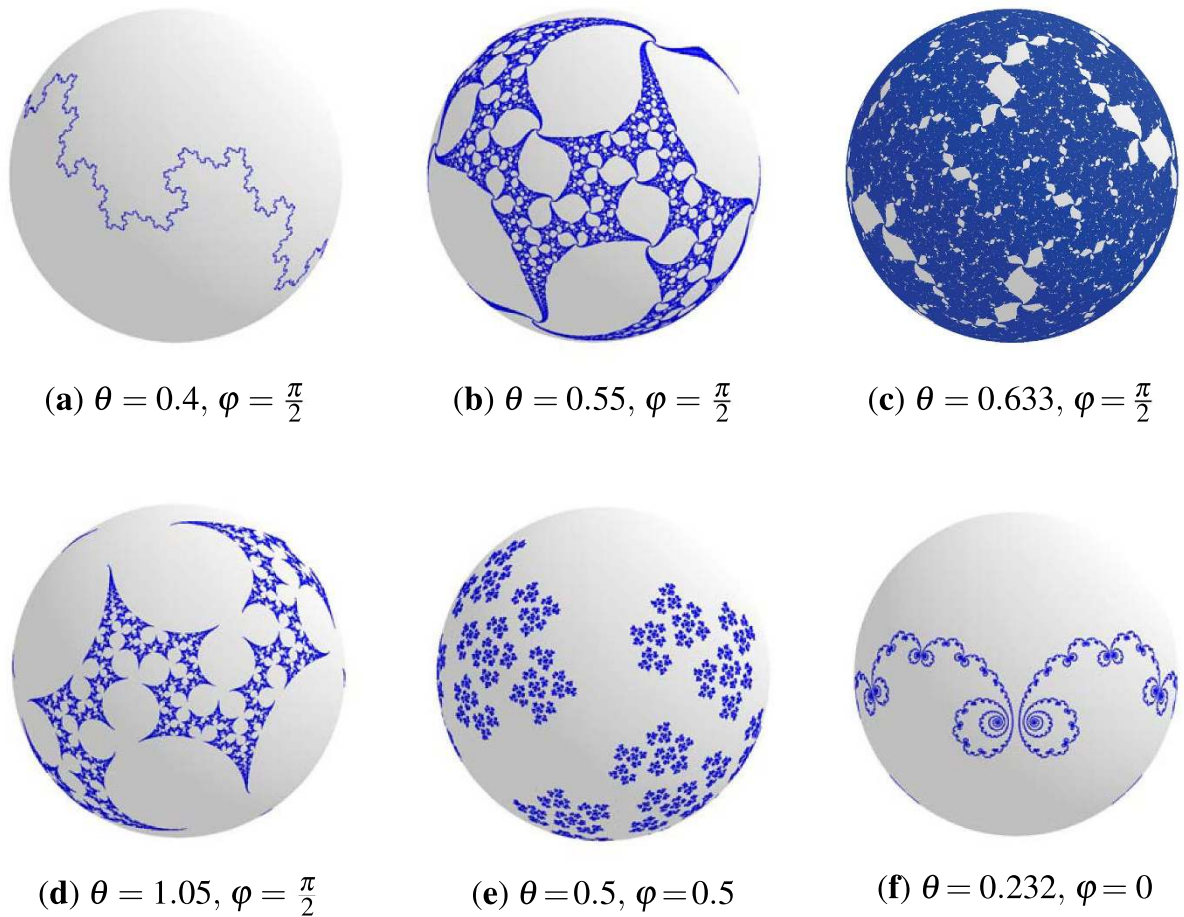
(a) $\theta = 0.4$, $\varphi = \frac{\pi}{2}$ **(b)** $\theta = 0.55$, $\varphi = \frac{\pi}{2}$ **(c)** $\theta = 0.633$, $\varphi = \frac{\pi}{2}$

(d) $\theta = 1.05$, $\varphi = \frac{\pi}{2}$ **(e)** $\theta = 0.5$, $\varphi = 0.5$ **(f)** $\theta = 0.232$, $\varphi = 0$

Figure 2. Julia sets consisting of the sensitive initial states lying on the Bloch sphere. Julia sets (blue) are plotted for various choices of $U_{\theta,\varphi}$. (**a–c**) Shows how the Julia set starts covering the whole Bloch sphere while increasing the value of θ. (**d**) Transition from a web to a simple closed curve. (**e**) The sensitive initial states form a completely disconnected set. (**f**) The result of a parabolic explosion (implosion)[30] where a stable fixpoint has become unstable - breaking a circle like connected Julia set into infinitely many parts.
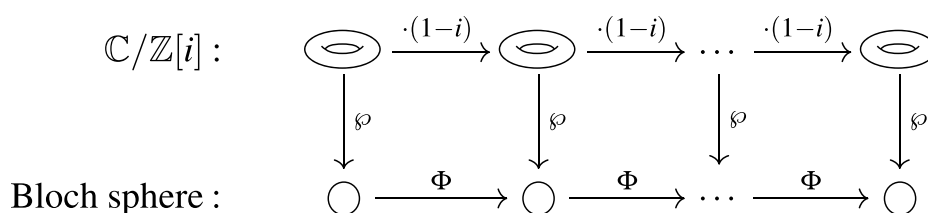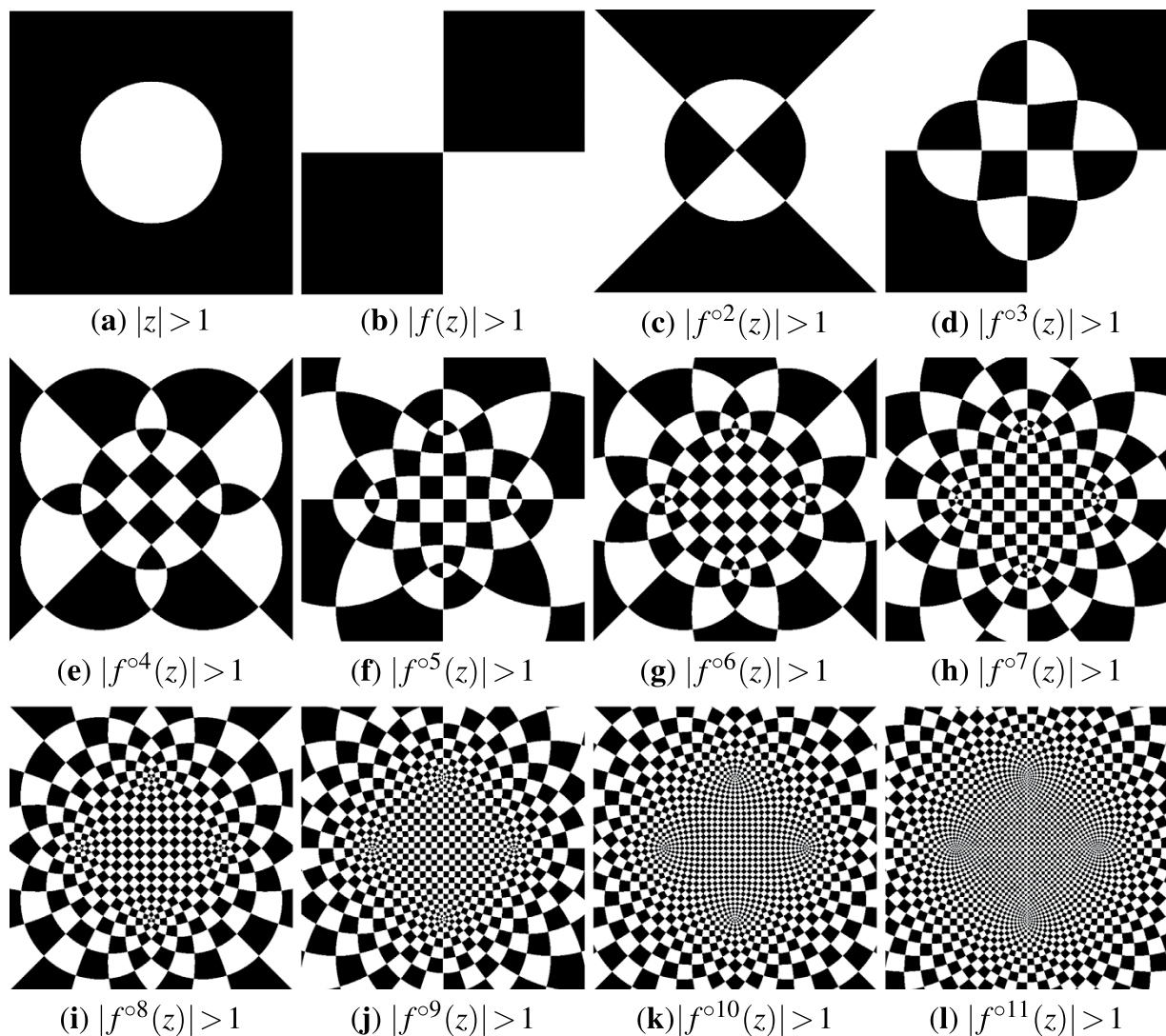
Emergence of general complex rational dyanmics and the Mandelbrot set. We may find even more exotic transformations by generalising the protocol to allow the physical realisation of any rational map $z \rightarrow \frac{\sum_{k=0}^{n} c_k z^k}{\sum_{k=0}^{n} d_k z^k}$ of degree $n \geq 2$. Our generalised scheme proceeds by forming n-tuples of identical pure qubits $\otimes_{j=1}^{n} (\alpha|0\rangle + \beta|1\rangle)_j$ and applying an appropriate n-qubit unitary V. The final step of one iteration is measuring all the qubits except the last one and keeping it only if all measurements resulted 0; this post-selective step can be shortly described by the projection $[|0\rangle \langle 0 \ldots 00| + |1\rangle \langle 0 \ldots 01|]$. Implementing a specific rational map reduces to finding a V unitary satisfying:

$$[|0\rangle \langle 0 \ldots 00| + |1\rangle \langle 0 \ldots 01|] V \left(\overset{n}{\underset{j=1}{\otimes}} (\alpha|0\rangle + \beta|1\rangle)_j \right)$$

$$= \gamma \left(\sum_{k=0}^{n} c_k \alpha^k \beta^{n-k} |0\rangle + \sum_{k=0}^{n} d_k \alpha^k \beta^{n-k} |1\rangle \right) \tag{4}$$

with arbitrary $\gamma \neq 0$, providing the desired post-selected state. The existence of such V follows from a simple linear algebraic argument explicated in Methods.

A notable consequence is that we found a direct quantum physical realisation of the Mandelbrot maps $z \rightarrow z^2 + c$ and can devise a quantum circuit for it. Figure 4 shows a possible quantum circuit implementation for this family of maps. The scheme demonstrates how the corresponding family of 2-qubit unitaries may be constructed using only controlled 1-qubit gates, which are considered experimentally more feasible in general.

For the sake of completeness we note that recently another strong connection between rational functions and quantum computing with post-selection was discovered[22] from an algorithmic perspective.

(a) $|z| > 1$ **(b)** $|f(z)| > 1$ **(c)** $|f^{\circ 2}(z)| > 1$ **(d)** $|f^{\circ 3}(z)| > 1$

(e) $|f^{\circ 4}(z)| > 1$ **(f)** $|f^{\circ 5}(z)| > 1$ **(g)** $|f^{\circ 6}(z)| > 1$ **(h)** $|f^{\circ 7}(z)| > 1$

(i) $|f^{\circ 8}(z)| > 1$ **(j)** $|f^{\circ 9}(z)| > 1$ **(k)** $|f^{\circ 10}(z)| > 1$ **(l)** $|f^{\circ 11}(z)| > 1$

(m) A commutative diagram explaining the action of Φ.

Figure 3. Iterations of an exponentially mixing map. (a–l) Visualisation of the iteratives of f. Each subfigure shows $z \in [-2,2] \times [-2i,2i]$; the domains are coloured according to whether $|f^{\circ n}| > 1$(black) or ≤ 1 (white) distinguishing the northern and southern half of the Bloch sphere. After a few iterations even very close states get mapped to different halves of the Bloch sphere as indicated by the rapid alternation of black and white domains. (**m**) The iterative map $\Phi^{\circ n}$ acts on the Bloch sphere correspondingly to the action of multiplication by $(1 - i)^n$ on the torus, explaining the regular pattern.

The cost of non-linearity and the Schrödinger microscope. We have just shown that using post-selection one can implement a wide range of non-linear maps, which may be useful for various tasks. A highly non-linear map, like Φ, provides a sort of "Schrödinger microscope"[23] enabling one to exponentially magnify tiny differences between quantum states. Consider for example the behavior of Φ around the fixed state $|+\rangle = \Phi|+\rangle$. Using our representation in terms of rational functions this fixed point becomes $1 = f(1)$. Then $\frac{df(z)}{dz}\big|_{z=1} = -2i$ translates to that Φ doubles infinitesimal distances around $|+\rangle$, analogously to a microscope.
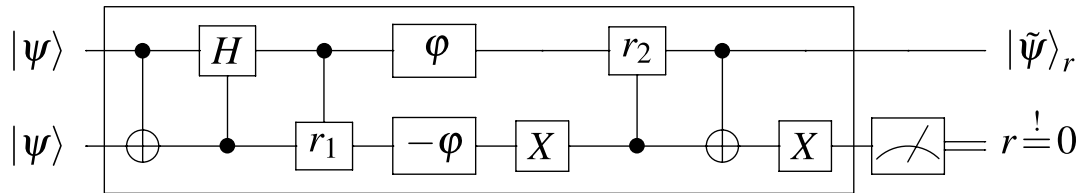
Figure 4. A quantum circuit implementing Mandelbrot maps. The controlled gate labelled by the real number r_j is essentially a rotation composed with a Pauli-Z-gate $\frac{1}{\sqrt{1+r_j^2}}\begin{bmatrix} 1 & r_j \\ r_j & -1 \end{bmatrix}$ and the gate labelled by $\pm\varphi$ is a phase gate $\begin{bmatrix} 1 & 0 \\ 0 & e^{\pm i\phi} \end{bmatrix}$, while H and X stand for the Hadamard and Pauli-X gates correspondingly. If we set $r_1 = 1/r_2$, $r_2 = |c| \cdot \sqrt{(1 + \sqrt{1 + 4/|c|^2})/2}$ and $e^{i\varphi} = \frac{c}{|c|}$, then the resulting map is $z^2 + c$, provided that we accept only the 0 measurement outcome on the second qubit.

Having such a tool we are tempted to develop powerful quantum algorithms utilising it. It is well known that introducing post-selection to Quantum Computing makes it extremely powerful - the corresponding complexity class PostBQP[24] includes NP and even PP. The question of efficiency and resource needs naturally arises. We address it using a black box argument considering results about state discrimination[25–27].

Suppose we have a quantum device implementing n iterations of Φ processing a qubit ensemble of size N. The size M of the successfully processed output ensemble may be probabilistic. We would like to determine its success rate, i.e. the average ratio M/N. To derive a bound on the success rate consider applying this quantum device to the qubit ensemble having state either $|\psi_0\rangle$ or $|\psi_1\rangle \neq |\psi_0\rangle$ with equal probability 1/2. If their distance $d(|\psi_0\rangle, |\psi_1\rangle) = \sqrt{1 - |\langle\psi_0|\psi_1\rangle|^2} \ll 1/N$, then the distance of the full ensemble states is $d(\otimes^N|\psi_0\rangle, \otimes^N|\psi_1\rangle) \approx \sqrt{N} \cdot d(|\psi_0\rangle, |\psi_1\rangle)$. Thus we cannot distinguish the possible ensemble states with error probability less than $\approx (1 - \sqrt{N} \cdot d(|\psi_0\rangle, |\psi_1\rangle))/2$, see [26, Chapter IV §2]. Suppose $d(\psi_j, |+\rangle) \ll 1/2^n$ for $j = 0, 1$ then, after n iterations of our process Φ, the distance of the two states increases by a factor of roughly 2^n since Φ doubles infinitesimal distances around the fixed point $|+\rangle$. If the device outputs M copies of the transformed states then we can distinguish the ensembles with error probability $\approx (1 - \sqrt{M} \cdot 2^n \cdot d(|\psi_0\rangle, |\psi_1\rangle))/2$. For large N the success rate is roughly constant because of the law of large numbers; thus we can treat the value M/N fixed. But $\sqrt{M} \cdot 2^n/\sqrt{N}$ cannot exceed 1 as the error probability of discrimination cannot decrease and so the success rate is upper bounded by 4^{-n}. This holds for states lying close to $|+\rangle$, in better cases the rate may be higher. For our implementation scheme each iteration has a success rate at least 1/4 (up to a negligible term $-1/N$ due to parity) implying that this scheme provides the best possible worst case success rate.

In this way we have shown that exponentially many copies are needed for n iterations of the process. Similar upper bound can be devised to any non-linear map that have a region where the separation of close states can be described by a multiplicative factor $\lambda > 1$. If we follow the above argument it turns out that the worst case success rate of such protocol is bounded by $1/\lambda^2$. Note that the particular choice of metric by which we measured separation does not limit the scope of the argument too much – we could use any other metric that agrees infinitesimally, e.g. the Bures metric. Thus it turns out that the implementation of any kind of Schrödinger microscope needs exponentially many copies of the states in terms of magnification steps (more precisely, quadratically many in terms of the total magnification).

Discussion

While exploring the possible dynamical properties of state selective protocols, we found that any complex rational map can be implemented using state selection. Such a general and natural correspondence between a physical system and the theory of complex dynamical systems is unique to our knowledge. We could also devise a realistic optical experimental scheme, which implements particularly interesting quadratic rational dynamics.

We showed that a specific setting of the proposed optical scheme implements an exponentially mixing map. At several regions of the Bloch sphere this protocol magnifies initial differences between quantum states almost uniformly, thus we may call it a Schrödinger microscope. The term Schrödinger microscope was introduced by Lloyd and Slotine[23] in connection with a non-linear quantum protocol emerging from collective weak measurements and coherent feedback. Even though[23] introduces Schrödinger microscope at a conceptual level, there was no explicit example shown unlike in this article. Although the collective weak measurement approach seems very different from our post-selective scheme, they are connected at a deep level: the effective non-linearity comes from the underlying ensemble of identical quantum states in both cases.

During our study of the emergence of exponential sensitivity, we were led to the analysis of implementation cost, which turned out to be exponential. We found a general bound on the number of copies needed for the successful implementation of any expanding non-linear map. We proved that a protocol capable of magnifying differences between close quantum states by a factor $\lambda > 1$ necessarily has a worst case rate of loss at least $1 - 1/\lambda^2$ in the number of copies of the unknown input quantum states. This "Quantum magnification bound" is basically another reformulation of the fact that one cannot bootstrap quantum information without an external source, somewhat resembling the quantum no-cloning theorem.

We used the "Quantum magnification bound" principle to show the optimality of our implementation of a Schrödinger microscope. In general, this principle helps to understand the advantages and limitations of any kind of Schrödinger microscope, regardless of the actual implementation method. Thus it also overcomes the difficulties coming from approximative arguments required to describe complex systems, like the protocol[23] involving collective weak measurements and coherent feedback. This fundamental bound may be applied to other quantum information protocols, providing a general tool for bounding the success rate of particular probabilistic protocols.

Looking at general processes, with inspiration coming from this principle, may also provide a new insight to the relation of classical and quantum chaos[28], suggesting that classical deterministic chaos may be just an approximation with a characteristic time scale. Classical deterministic chaotic systems explode quickly, and observing the deterministic evolution of the system, even at a macroscopic level, enables the determination of the initial conditions increasingly precisely[29]. But there is a level of precision that is prohibited by quantum uncertainty relations. This is an apparent philosophical contradiction, provided we believe classical physics is based on quantum mechanics; a possible dissolution is saying that on long time scales one cannot treat a classical process deterministically chaotic, just chaotic in some statistical sense.

Methods

Connection to Lattès maps.

The map $f = \frac{z^2 + i}{iz^2 + 1}$ can be written as $\frac{z+1}{z-1} \circ \frac{z^2+1}{-2iz} \circ \frac{z+1}{z-1}$, where $\widetilde{f} = \frac{z^2+1}{-2iz}$ is a well-known Lattès map[20], and $\frac{z+1}{z-1}$ is a self inverse Möbius transformation[19]. Since conjugation by Möbius transformation does not change the iterative features, it implies that f exhibits the same dynamics as $\widetilde{f}$. To give a physical meaning to this Möbius transformation, we mention that it corresponds to a rotation of the Bloch sphere, i.e. f and $\widetilde{f}$ essentially describe the same process, just written in a different qubits basis.

As we already indicated in this article, f is conjugate to the map $(1 - i) \cdot \mathrm{id}_{\mathbb{C}/\mathbb{Z}[i]}$ via the Weierstrass-$\wp$ function. In fact, we need a slightly transformed version of the Weierstrass-$\wp$ that is amended by our Möbius transformation. Our transformed version can be written as $\widetilde{\wp}(z) := \frac{z+1}{z-1} \circ \frac{2\wp(z; L = i)}{i\sqrt{g_2(L = i)}}$ (for the definitions of L, g_2 and $\wp$ $(z; L)$ see[21]). Using this function we get the key identity $f^{\circ n} \circ \widetilde{\wp} = \widetilde{\wp} \circ (1 - i)^n \cdot \mathrm{id}_{\mathbb{C}/\mathbb{Z}[i]}$.

$\widetilde{\wp}$ induces a two sheet branched covering with 4 exceptional points that are covered only once. (These points can be easily spotted on Fig. 3). With the exception of these 4 points, $\widetilde{\wp}$ is a two-to-one map so it does not have a well defined inverse. A general point $\hat{z} \in \hat{\mathbb{C}}$ has pre-images $z, -z \in \mathbb{C}/\mathbb{Z}[i]$, but the linear map on $\mathbb{C}/\mathbb{Z}[i]$ carries opposite numbers to opposite ones so fortunately the identity $f(\hat{z}) = \wp((1 - i) \cdot \widetilde{\wp}^{-1}(\hat{z})) \; \forall \hat{z} \in \hat{\mathbb{C}}$ holds regardless which branch of $\widetilde{\wp}^{-1}$ is considered. In this sense we can say, that the stronger identity $f^{\circ n}(\hat{z}) = \wp((1 - i)^n \cdot \widetilde{\wp}^{-1}(\hat{z})) \; \forall \hat{z} \in \hat{\mathbb{C}}$ also holds.

Metric on the Bloch sphere $\hat{\mathbb{C}}$ and the torus $\mathbb{C}/\mathbb{Z}[i]$.

We would like to show exponential mixing of our Lattès map, thus we need to understand how distances are distorted by $\widetilde{\wp}$. In order to trace the problem, we need to introduce some proper distance concepts.

A possible metric on pure quantum states is given by using the distance defined by the quantum angle $d_A\left(\left|\psi_{z_0}\right\rangle, \left|\psi_z\right\rangle\right) := \arccos |\langle \psi_0 | \psi_z \rangle|$. Note that this distance coincides with the natural spherical metric of the Bloch sphere, up to a multiplicative factor of 2. This metric is similar to the Bures metric defined by the distance $d_B = \sqrt{2\left(1 - F\left(\left|\psi_{z_0}\right\rangle\left\langle\psi_{z_0}\right|, \left|\psi_z\right\rangle\left\langle\psi_z\right|\right)\right)}$, where $F(.,.)$ is the Fidelity of two density matrices. A third possible distance definition is given by $d\left(\left|\psi_{z_0}\right\rangle, \left|\psi_z\right\rangle\right) = \sqrt{1 - \left|\left\langle \psi_{z_0} | \psi_z \right\rangle\right|^2}$. Since all three distance definitions coincide for infinitesimal distances, we are free to chose the most appropriate one for our calculations. For now we stick with the natural metric of $\hat{\mathbb{C}}$, which is 2 times the quantum angle $d_R(z_0, z) = 2 \cdot d_A(|\psi_{z_0}\rangle, |\psi_z\rangle)$ (the index R refers to the fact that d_R is a Riemannian metric). For the torus $\mathbb{C}/\mathbb{Z}[i]$ we use the natural Riemannian metric inherited from $\mathbb{C}$.

First, we show that the Möbius transformation $\frac{z+1}{z-1}$ leaves the metric on $\hat{\mathbb{C}}$ invariant. Putting it differently, we would like to show that the conformal metric $\rho := \frac{|ds'|}{|ds|}$ is trivial, where ds and ds' are tangent vectors of $\hat{\mathbb{C}}$ at points s and $s' = \frac{s+1}{s-1}$ such that ds is mapped to ds' by the tangent map. We proceed using the identity $\frac{|ds'|}{|ds|} = \frac{|dz|}{|ds|}\frac{|dz'|}{|dz|}\frac{|ds'|}{|dz'|}$, where dz and dz' are tangent vectors of $\mathbb{C}$. The conformal metric transformation introduced by the stereographic projection is well known to be $\frac{|ds'|}{|dz'|} = \frac{4}{|z'|^2 + 1}$, similarly $\frac{|dz|}{|ds|} = \frac{|z|^2 + 1}{4}$. Finally $\frac{|dz'|}{|dz|} = \left|d\left(\frac{z+1}{z-1}\right)/dz\right| = \left|\frac{(z-1) - (z+1)}{(z-1)^2}\right| = \frac{2}{|z-1|^2}$. Putting everything together $\frac{|ds'|}{|ds|} = \frac{|z|^2 + 1}{4}\frac{2}{|z-1|^2}\frac{4}{\left|\frac{z+1}{z-1}\right|^2 + 1} = \frac{|z|^2 + 1}{1}\frac{2}{|z-1|^2}\frac{|z-1|^2}{|z+1|^2 + |z-1|^2} = 1$ as we indicated.

The Möbius transformation is just an isometry of $\hat{\mathbb{C}}$, so we can concentrate on the other part $z' = \frac{2\wp(z; L = i)}{i\sqrt{g_2(L = i)}}$ of our Weierstrass function $\widetilde{\wp}$. From now on let $\wp(z) := \wp(z; L = i)$, $g_2 := g_2(L = i)$ and $\rho := \frac{|ds|}{|dz|} = \frac{|dz'|}{|dz|}\frac{|ds|}{|dz'|}$, where dz' is a tangent vector of $\mathbb{C}$ at a point z'. Just as above $\frac{|ds|}{|dz'|} = \frac{4}{|z'|^2 + 1} = \frac{4}{\frac{4}{g_2}|\wp(z)|^2 + 1}$. For the other factor $\frac{|dz'|}{|dz|} = \left|d\frac{2\wp(z)}{i\sqrt{g_2}}/dz\right| = \frac{2}{\sqrt{g_2}}|\wp'(z)|$. Now we use the well known property $\wp'^2 = 4\wp^3 - g_2\wp - g_3$. Since

$g_3(L = i) = 0$ the final formula is: $\rho^2 = \dfrac{16}{\left[\frac{4}{g_2}|\wp(z)|^2 + 1\right]^2} \dfrac{4}{g_2} |4\wp(z)^3 - g_2\wp(z)| = 64g_2 \dfrac{|4\wp(z)^3 - g_2\wp(z)|}{(4|\wp(z)|^2 + g_2)^2}$. Using the tri-

angle inequality we get $\rho^2 \le 64g_2 \dfrac{4|\wp(z)|^3 + g_2 |\wp(z)|}{\left(4|\wp(z)|^2 + g_2\right)^2} = 64g_2 \dfrac{|\wp(z)|}{4|\wp(z)|^2 + g_2}$. This function has its maximum when

$|\wp(z)|^2 = g_2/4$; substitution yields $\rho^2 \le 16\sqrt{g_2}$. Finally using that $\sqrt{g_2} \approx 13.7504$, we arrive at the conclusion $\rho < 16$.

The conformal metric $\rho < 16$ is upper bounded, so the image of any two points from the surface of the torus gets mapped to points having spherical distance less than 16 times their torical distance. Thus for any point s on the surface of the Bloch sphere and a radius ε ball $B_{d_R}(s, \varepsilon)$ around it, the ball's pre-image $\widetilde{\wp}^{-1}(B_{d_R}(s, \varepsilon))$ contains another ball $B_{d_{\mathbb{C}/\mathbb{Z}[i]}}(\widetilde{\wp}^{-1}(s), \varepsilon/16)$.

Exponential mixing. Suppose we have a one qubit state $|\psi_z\rangle$ that we know with ambiguity ε. In other words it is a pure quantum state $|\psi_z\rangle$ close to some $|\psi_{z_0}\rangle$, such that the quantum angle $d_A(|\psi_{z_0}\rangle, |\psi_z\rangle) = \arccos |\langle\psi_{z_0}|\psi_z\rangle| \le \varepsilon$. So $|\psi_z\rangle$ lies in the diameter ε ball around $|\psi_{z_0}\rangle$, i.e. $|\psi_z\rangle \in B_{d_A}(|\psi_{z_0}\rangle, \varepsilon)$. This ball corresponds to $B_{d_R}(z_0, 2\varepsilon)$ using the (Bloch) spherical representation. As we already discussed $\widetilde{\wp}^{-1}(B_{d_R}(z_0, 2\varepsilon)) \supset B_{d_{\mathbb{C}/\mathbb{Z}[i]}}(\widetilde{\wp}^{-1}(z_0), \varepsilon/8)$.

It is easy to show that after multiplying each point of $B_{d_{\mathbb{C}/\mathbb{Z}[i]}}(\wp^{-1}(z_0), \varepsilon/8)$ with $(1-i)^n$ the image covers the whole $\mathbb{C}/\mathbb{Z}[i]$, provided that $n \ge \log_{\sqrt{2}}(8/\varepsilon)$. Thus for $n = 6 + \log_{\sqrt{2}}(1/\varepsilon)$ we have $\hat{\mathbb{C}} = f^{\circ n}\left(B_{d_A}(z_0, \varepsilon)\right)$. It means that after $6 + \log_{\sqrt{2}}(1/\varepsilon)$ iterations the initial uncertainty about the state $|\psi_z\rangle$ evolves so much that $\Phi^{\circ n}(|\psi_z\rangle)$ may be any pure state. This statement is basically a translation of the fact that the linear map $\cdot(1-i)$ has Lyapunov exponent $\ln(\sqrt{2})$ on $\mathbb{C}/\mathbb{Z}[i]$, and shows exponential mixing and sensitivity on the surface of the Bloch sphere.

Construction of n-qubit unitaries for degree n rational maps. We would like to implement the rational function $z \to \dfrac{\sum_{k=0}^{n} c_k z^k}{\sum_{k=0}^{n} d_k z^k}$. Our generalised protocol starts by forming n-tuples of identical pure qubits of our ensemble, then continues by the application of a specific n-qubit unitary V. The final step is a measurement on all the qubits except the last one of every tuple. The protocol succeeds if all the measurements resulted in 0, the unmeasured qubit is kept only in such cases.

Initially the state of the n-tuples is the following product state:

$$|\phi\rangle = \overset{n}{\underset{i=1}{\otimes}}\left(\alpha|0\rangle_i + \beta|1\rangle_i\right) = \sum_{k=0}^{n} \alpha^k\beta^{n-k}|\phi_k\rangle \text{ where } |\phi_k\rangle = \sum_{\substack{b\in\{0,1\}^n \\ \#\{b_i|b_i=1\}=k}} |b\rangle \tag{5}$$

As before we use the parametrisation $z = \alpha/\beta$ for a qubit $(\alpha|0\rangle + \beta|1\rangle)$. Then the parameter of the unmeasured, post-selected qubit can be described as follows:

$$\frac{\langle \overbrace{0\ldots0}^{n-1\text{zeros}} 0|V|\phi\rangle}{\langle \underbrace{0\ldots0}_{n-1\text{zeros}} 1|V|\phi\rangle} = \frac{\sum_{k=0}^{n} \overbrace{\langle 0\ldots00|V|\phi_k\rangle}^{c_k} \alpha^k\beta^{n-k}}{\sum_{k=0}^{n} \underbrace{\langle 0\ldots01|V|\phi\rangle_k}_{d_k} \alpha^k\beta^{n-k}} = \frac{\sum_{k=0}^{n} c_k\alpha^k\beta^{n-k}}{\sum_{k=0}^{n} d_k\alpha^k\beta^{n-k}} = \frac{\sum_{k=0}^{n} c_k z^k}{\sum_{k=0}^{n} d_k z^k} \tag{6}$$

We present a linear algebraic argument showing that for any rational map of degree ≥ 2 there is a suitable unitary V. We show how to construct a unitary for any coefficients c_k, d_k describing such a rational map.

First let us introduce some vector $|\omega\rangle = (|\underbrace{0\ldots0}_{n-2\text{zeros}}10\rangle - |\underbrace{0\ldots0}_{n-2\text{zeros}}01\rangle)/\sqrt{2}$ that is orthogonal to all the $|\phi_k\rangle$ vectors. We set $\tilde{v}_0 = \sum_{k=0}^{n} \frac{c_k}{\sqrt{\binom{n}{k}}} \cdot \frac{|\phi_k\rangle}{\sqrt{\binom{n}{k}}} + x \cdot |\omega\rangle$ and $\tilde{v}_1 = \sum_{k=0}^{n} \frac{d_k}{\sqrt{\binom{n}{k}}} \cdot \frac{|\phi_k\rangle}{\sqrt{\binom{n}{k}}} + y \cdot |\omega\rangle$. Then by choosing $x, y \in \mathbb{C}$ appropriately, we can always satisfy the equalities:

$$x^*y = -\sum_{k=0}^{n} \frac{c_k^* d_k}{\binom{n}{k}} \Leftrightarrow \sum_{k=0}^{n} \frac{c_k^* d_k}{\binom{n}{k}} + x^*y = 0 \Leftrightarrow \langle\tilde{v}_0|\tilde{v}_1\rangle = 0 \tag{7}$$

$$|x|^2 - |y|^2 = \sum_{k=0}^{n} \frac{|d_k|^2 - |c_k|^2}{\binom{n}{k}} \Leftrightarrow \sum_{k=0}^{n} \frac{|c_k|^2}{\binom{n}{k}} + |x|^2 = \sum_{k=0}^{n} \frac{|d_k|^2}{\binom{n}{k}} + |y|^2 \Leftrightarrow |\tilde{v}_0|^2 = |\tilde{v}_1|^2 \tag{8}$$

Finally, setting $\langle \underbrace{0\cdots0}_{n-1\text{zeros}} 0|V := \langle\tilde{v}_0|/|\tilde{v}_0|$ and $\langle \underbrace{0\ldots0}_{n-1\text{zeros}} 1|V := \langle\tilde{v}_1|/|\tilde{v}_0|$ satisfies (6). Due to (7),(8) $\langle\tilde{v}_0|/|\tilde{v}_0|$ and $\langle\tilde{v}_1|/|\tilde{v}_0|$ are orthonormal vectors so we can extend V to a full n-qubit unitary by defining the remaining $2^n - 2$ orthonormal rows arbitrarily.

Without loss of generality we can assume that $\sum_{k=0}^{n} c_k z^k$ and $\sum_{k=0}^{n} d_k z^k$ has no common roots; otherwise we can cancel it. So the probability that the process succeeds $|\langle 0\cdots00|V|\phi\rangle|^2 + |\langle 0\cdots01|V|\phi\rangle|^2$

$=(|\sum_{k=0}^{n}c_k z^k|^2 + |\sum_{k=0}^{n}d_k z^k|^2)/|\tilde{v}_0|^2$ is non-zero. Then this success probability is also greater than some p probability for a fixed map, regardless the state $|\phi\rangle$ due to compactness of the state space. (However, depending on the map, this lower bound may be arbitrarily low.)

Thus using the above defined V unitary we can implement the rational function $\frac{\sum_{k=0}^{n}c_k z^k}{\sum_{k=0}^{n}d_k z^k}$ where as before this means a transformation

$$(\alpha|0\rangle + \beta|1\rangle) \rightarrow N\left(\sum_{k=0}^{n}c_k \alpha^k \beta^{n-k}|0\rangle + \sum_{k=0}^{n}d_k \alpha^k \beta^{n-k}|1\rangle\right) \tag{9}$$

where $z = \alpha/\beta$ and N is a norming factor.

References

1. Rabitz, H. Focus on Quantum Control. *New J. Phys.* **11,** 105030 (2009).
2. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
3. Gendra, B., Ronco-Bonvehi, E., Calsamiglia, J., Muñoz-Tapia, R. & Bagan, E. Quantum Metrology Assisted by Abstention. *Phys. Rev. Lett.* **110,** 100501 (2013).
4. Duan, L. M., Lukin, M. D., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414,** 413–418 (2001).
5. Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. A. & Wootters, W. K. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.* **76,** 722 (1996).
6. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54,** 3824 (1996).
7. Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. & Sanpera, A. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.* **77,** 2818 (1996).
8. Bechmann-Pasquinucci, H., Huttner, B. & Gisin, N. Non-linear quantum state transformation of spin-1/2. *Phys. Lett. A* **242,** 198–204 (1998).
9. Scott, A. J. & Milburn, G. J. Quantum nonlinear dynamics of continuously measured systems. *Phys. Rev. A* **63,** 042101 (2001).
10. Habib, S., Jacobs, K. & Shizume, K. Emergence of Chaos in Quantum Systems Far from the Classical Limit. *Phys. Rev. Lett.* **96,** 010403 (2006).
11. Everitt, M. J. On the correspondence principle: implications from a study of the nonlinear dynamics of a macroscopic quantum device. *New J. Phys.* **11,** 013014 (2009).
12. Cvitanović, P., Artuso, R., Mainieri, R., Tanner, G. & Vattay, G. Chaos: *Classical and Quantum*, ChaosBook.org (Niels Bohr Institute, Copenhagen, 2012).
13. Kiss, T., Jex, I., Alber, G. & Vymĕtal, S. Complex chaos in the conditional dynamics of qubits. *Phys. Rev. A* **74,** 040301(R) (2006).
14. Kiss, T., Vymĕtal, S., Tóth, L. D., Gábris, A., Jex, I. & Alber, G. Measurement induced chaos with entangled states. *Phys. Rev. Lett.* **107,** 100501 (2011).
15. Guan, Y., Nguyen, D. Q., Xu, J. & Gong, J. Reexamination of measurement-induced chaos in entanglement-purification protocols. *Phys. Rev. A* **87,** 052316 (2013).
16. Devaney, R. L. *An Introduction to Chaotic Dynamical Systems* (Westview Press, 2003).
17. Pan, J. W., Simon, C., Brukner, S. & Zeilinger, A. Entanglement purification for quantum communication. *Nature* **410,** 1067–1070 (2001).
18. Pan, J. W., Gasparoni, S., Ursin, R., Weihs, G. & Zeilinger, A. Experimental entanglement purification of arbitrary unknown states. *Nature* **423,** 417–422 (2003).
19. Milnor, J. W. *Dynamics in One Complex Variable* (Princeton Univ. Press, 2006).
20. Milnor, J. W. On Lattès maps. in *Dynamics on the Riemann Sphere* [Hjorth, P. & Petersen, C. L. (eds.)] (Eur. Math. Soc., Zürich, 2006).
21. Bolsinov, A. V. & Fomenko, A. T. *Integrable Hamiltonian Systems: Geometry, Topology, Classification* (CRC Press, 2004).
22. Mahadev, U. & de Wolf, R. Rational approximations and quantum algorithms with postselection. *Quant. Inf. & Comp.* **15,** 295–307 (2015).
23. Lloyd, S. & Slotine, J. E. Quantum feedback with weak measurements. *Phys. Rev. A* **62,** 012307 (2000).
24. Aaronson, S. Quantum computing, postselection, and probabilistic polynomial-time. *Proc. R. Soc. A* **461,** 3473–3482 (2005).
25. Helstrom, C. W. *Quantum Detection and Estimation Theory* (Academic Press, 1976).
26. Bagan, E., Muñoz-Tapia, R., Olivares-Rentería, G. A. & Bergou, J. A. Optimal discrimination of quantum states with a fixed rate of inconclusive outcomes. *Phys. Rev. A* **86,** 040303(R) (2012).
27. Herzog, U. Optimal state discrimination with a fixed rate of inconclusive results: Analytical solutions and relation to state discrimination with a fixed error rate. *Phys. Rev. A* **86,** 032314 (2012).
28. da Luz, M. G. E. & Anteneodo, C. Nonlinear dynamics in meso and nano scales: fundamental aspects and applications. *Phil. Trans. R. Soc. A* **369,** 245–259 (2011).
29. Madhok, V., Riofrío, C. A., Ghose, S. & Deutsch, I. H. Information Gain in Tomography – A Quantum Signature of Chaos. *Phys. Rev. Lett.* **112,** 014102 (2014).
30. Douady, A. Does a Julia set depend continuously on the polynomial? in *Complex dynamical systems* [Devaney, R. L. (ed.)] *Proc. Sympos. Appl. Math.* **49,** 91–138 (1994).

Acknowledgements

Author Contributions

A.G., T.K. and I.J. contributed to the theoretical research described in the paper and the writing of the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Gilyén, A. *et al.* Exponential Sensitivity and its Cost in Quantum Physics. *Sci. Rep.* **6**, 20076; doi: 10.1038/srep20076 (2016).