

Increasing complexity with quantum physics

Janet Anders^{1, a)} and Karoline Wiesner^{2, b)}

¹⁾*Department of Physics and Astronomy, University College London,
W1E6 BT London, U.K.*

²⁾*School of Mathematics, Centre for Complexity Sciences, University of Bristol,
BS8 1TW Bristol, U.K.*

We argue that complex systems science and the rules of quantum physics are intricately related. We discuss a range of quantum phenomena, such as cryptography, computation and quantum phases, and the rules responsible for their complexity. We identify correlations as a central concept connecting quantum information and complex systems science. We present two examples for the power of correlations: using quantum resources to simulate the correlations of a stochastic process and to implement a classically impossible computational task.

^{a)}Electronic mail: j.anders@ucl.ac.uk

^{b)}Electronic mail: k.wiesner@bristol.ac.uk

LEAD PARAGRAPH

A common notion of a complex system is many members acting together to produce an orchestrated and structured ensemble. Hence, an important feature of a complex system is that it contains a high amount of correlations. Typical examples are neurons in the brain, molecules in a living cell, individual ants in a colony, people in a social network, and the natural forces that together produce climate. Complexity in the regime where quantum mechanics dictates the rules is of a different kind. It arises not because of the sheer number of participants but because the underlying rules of logic change. The Heisenberg principle, for instance, forbids the perfect knowledge of a particle's position and momentum. In this paper we survey how the rules of quantum mechanics lead to a number of unexpected phenomena, such as unbreakably secure communication, quantum parallel computing, and new states of matter, such as a superfluid. Similar to complexity science, in this wealth of quantum phenomena correlations play a central role. The central role of correlations in both quantum computation and complex systems has practical consequences: To capture all correlations of a complex system in a compact description, it turns out, quantum physics can be very useful.

I. INTRODUCTION

In complex systems it is often the sheer number of components which is considered to be responsible for the emergence of “complexity”. However, there is another perspective to how complexity can arise. When the underlying rules of the game change, new structures and phenomena can arise. This is the situation encountered in quantum physics, where quantum objects obey a logic very different from our intuition stemming from the classical world. Quantum laws such as superposition, entanglement and Heisenberg's uncertainty principle imply configurations and relationships that go well beyond what is usually called complexity. And they do so already with two constituent parts.

The aim of this paper is to inform researchers in complex systems about the intimate relation between quantum information and complexity science. It is not intended as a comprehensive review. Rather its aim is to communicate the aspects of the research on quantum systems produced over the last two decades which is relevant to complex systems

science. We give a selective account of a multitude of situations where quantum many-body systems acquire a higher “complexity” than classical systems. We then draw the connection between the two fields by focusing on the importance of correlations for both quantum information and complex systems science. While in complex systems it is intricate (classical) correlations between individual members that are responsible for coherent phenomena such as structure formation and concerted behaviour, quantum complexity relies on quantum correlations that arise as a result of quantum rules.

The paper is structured as follows. We will first give a brief overview over the relevant quantum phenomena of superposition and entanglement. We will then present a selection of phenomena showing overwhelming evidence that quantum mechanical correlations are responsible for new, classically unseen phenomena such as unbreakably secure communication, quantum phases, and enhanced computational complexity. We then present two examples that illustrate the relationship between computation, correlation and complexity. The first example shows that structure, i.e. classical correlations, can be generated with fewer computational resources when quantum resources are available. The second example discusses how a limited computer can be enabled to calculate computational task beyond its own capability by accessing quantum correlated resources. Finally we discuss the central role of correlations in both quantum information and complex systems science.

II. LAWS OF QUANTUM PHYSICS

A. Superposition

The superposition principle lies at the heart of quantum mechanics (see for example¹). Formally, it is rooted in the linearity of the Hilbert space. Any quantum state can be represented as a vector in Hilbert space. The superposition principle states that any sum of such vectors is also an admissible quantum state. We use the standard *bra*, *ket* notation, where a bra ($\langle v|$) is a column vector and a ket ($|v'\rangle$) is a row vector. Hence, $\langle v|v'\rangle$ denotes the inner product between v and v' . In other words, if the kets $|\psi_i\rangle$ are quantum states then the superposition

$$|\psi\rangle = \sum_i c_i |\psi_i\rangle \tag{1}$$

is also a quantum state. The c_i here are complex coefficients with the normalisation condition $\sum_i c_i^* c_i = 1$. For a two-state system, any such superposed state is called a *qubit* and its most general form is

$$|\psi\rangle = \cos(\theta)|0\rangle + e^{i\phi} \sin(\theta)|1\rangle , \quad (2)$$

where θ and ϕ are real numbers representing the complex coefficient c . It is important to distinguish between such a *coherent* superposition and a purely classical probability distribution over states of which a given system really only occupies one and we just don't know which. Such a classical probability distribution of quantum states $|\psi_i\rangle$ is formalised by a density operator ρ whose form is independent of the basis of representation

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| , \quad (3)$$

with $p_i \geq 0$ and $\sum_i p_i = 1$. A so-called *pure* state is a trivial mixture of only one quantum state $\rho = |\psi\rangle \langle \psi|$. The *von Neumann entropy* of a density operator is defined as

$$S(\rho) = -\text{tr}(\rho \log_2 \rho) , \quad (4)$$

where tr is the trace of the matrix. For any pure state $S(\rho) = 0$.

B. Entanglement

Entanglement is a key feature of quantum mechanics (for a review see⁴²). It is the most prominent kind of quantum correlation. However, there are many others such as *discord*⁵, *quantum conditional entropy*⁶ and minimum entanglement potential⁷. Entanglement is a property assigned to two or more subsystems. Assume that we have two subsystems S_1 and S_2 and a state vector $|\psi\rangle$ describing the whole system. We say that the subsystems are *entangled* if $|\psi\rangle$ cannot be written as a tensor product of two states $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ where $|\phi_1\rangle$ and $|\phi_2\rangle$ are the states of the subsystems S_1 and S_2 , respectively. As an example consider what is commonly called a *Bell state*:

$$|\psi_B\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2) \quad (5)$$

which is a superposition of two two-dimensional quantum states where the subscript denotes the subsystem. $|\psi_B\rangle$ cannot be written as a tensor product of two separate states for the

subsystems S_1 and S_2 . Consequently it is not possible to derive the properties of $|\psi_B\rangle$ from the sum of the properties of the individual subsystems. $|\psi_B\rangle$ contains correlations between S_1 and S_2 which go beyond what is classically possible. This is expressed in the so-called CHSH inequality¹⁹. Consider a Bell state which is physically separated and S_1 is sent to Alice and subsystem S_2 is sent to Bob. Each can then choose one of two bases in which to measure their subsystem in, A and a for Alice, and B and b for Bob. Each local measurement has binary outcomes, either 0 or 1. A measure for the correlations of their shared system before the measurement (i.e. of the correlations in $|\psi_B\rangle$) is given by

$$C = 2(p_{AB}^s + p_{Ab}^s + p_{aB}^s - p_{ab}^s - 1) \quad (6)$$

where p_{ij}^s is the probability that both, Alice and Bob, will get the same outcome when they measure i and j , respectively. The probabilities are normalised such that $p_{ij}^s + p_{ij}^d = 1$, where p_{ij}^d is the probability that the outcomes of the local measurements are different. If Alice and Bob had classical states, the amount of correlation between the measurement outcomes is upper bounded by $|C_{\text{classical}}| \leq 2$. However, for quantum states there is a higher bound, $|C_{\text{quantum}}| \leq 2\sqrt{2}$. The Bell state reaches the maximum of correlations $|C_{\text{quantum}}| = 2\sqrt{2}$ known as the Tsirelson bound⁸.

C. Heisenberg Uncertainty Principle

Heisenberg stated his uncertainty principle originally as follows: If you make a measurement of an object's momentum with precision Δp you cannot at the same time determine its position with a precision more accurately than $\Delta x = \frac{h}{4\pi\Delta p}$, where h is Planck's constant.

Consider the well-known double-slit experiment. An electron is emitted by an electron gun and sent through a wall with two parallel slits in it. Behind the wall there is a fluorescing screen which detects the impact of the electron. After many repetitions of this experiment the screen will show an interference pattern of electron impacts. This is just what is predicted by the superposition principle: The electron's path consists of two superposed paths, one which goes through the left and one which goes through the right slit. Now we move the wall with a well-known speed perpendicular to the two slits. The impact of the electron onto either the left slit or the right slit will change the momentum of the wall and hence, without measuring the electron, just by measuring the change in momentum of the wall, we

can determine which of the two paths the electron has actually taken. This contradicts the superposition principle of two perfectly simultaneous realisations in one system. However, this contradiction is solved when Heisenberg's uncertainty principle is taken into account. Since we cannot measure the momentum of the wall with perfect accuracy while also determining its position with the same accuracy we cannot know exactly where the two slits are. This is enough to smear out the interference pattern of the electrons. Hence, it is a general rule of quantum mechanics that one cannot design equipment that determines which of two alternatives in a superposition is realised without, at the same time, destroying the superposition².

III. QUANTUM COMPLEXITY

Given the rules of quantum physics we may expect new kinds of complexity at the atomic level. Here we will give an overview of a range of phenomena where quantum resources lead to the emergence of a higher complexity.

A. Quantum cryptography

Cryptography is the science of encoding and transmitting a secret message in such a way that it is very hard for an eavesdropper to break the code and learn the message. This problem can be reduced to transmitting a secret key, such as a sequence of *random* binary numbers with which a binary message is encrypted by adding the two, e.g. random key = 0011001, message to be encoded = 1110000 and cipher = 1101001. The randomness of the key then guarantees the security of the encoded message. However, this still means that a *secret key* has to be shared in the first place between two communicating parties, traditionally called Alice and Bob. Today many cryptographic techniques that achieve this, so called key distribution schemes, rely on mathematical functions that behave like a trapdoor: it is easy to get in, but hard to get out. An example is the public key RSA scheme that relies on the difficulty of factoring. Here the easy direction of the trap door is the simplicity of multiplying two (rather large) prime numbers. The difficulty lies in the reverse direction - finding the two unknown prime factors of a large number. In fact there is no known classical algorithm that can factor in any reasonable time (polynomial time), and

the factoring problem lies in a computational complexity class (NP) that is conjectured to contain problems that require exponential time to solve^{9,10}. However, the bottom line is that the security of RSA, and all classical algorithms that use mathematical trap door functions, relies solely on the *assumption* that reversing the trap door is computationally hard, i.e. it takes exponentially long to solve.

This is why the excitement was big when in 1984 Brassard, a computer scientist, and Bennett, a physicist, realised that quantum physics allows the sharing of a provably secure key¹¹. They developed the first quantum key distribution scheme, the BB84 protocol, in which the sender, Alice, prepares her key in a qubit. For this she chooses one of two bases at random, the computational basis $\{|0\rangle, |1\rangle\}$ or the superposed x -basis $\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. She then sends the qubit to her communication partner, Bob, who will measure in the same two bases, also at random. In the classical world an intercepting eavesdropper wanting to learn the key would take a copy of the transmitted information and then attempt to decrypt the message. Copying an unknown qubit, however, is not permitted. This is known as the *no-cloning principle*, a theorem that results from Heisenberg's uncertainty principle. So an eavesdropper is faced with the task of intercepting the actual message carrier, attempt to decrypt it, and pass the resulting qubit - or a totally new qubit - on to Bob. To successfully decrypt the eavesdropper has to guess in which basis, the computational or the superposition basis, Alice used to encode the qubit in. This has two effects. Firstly a measurement in the "correct" basis will reveal perfectly which state was encoded, while measuring in the "wrong basis" results in no information for the eavesdropper. This is because the x -basis corresponds to equal probabilities to find $|0\rangle$ or $|1\rangle$, and vice versa. The second effect is that when the eavesdropper measures in the "wrong" basis the state changes. This is another consequence of the Heisenberg uncertainty principle and it is this second feature which makes BB84 unbreakably secure. More precisely, the communicating parties are able to monitor how much an eavesdropper could have learnt by sifting for only those bits where they happened to use the same basis. They can then identify if and how much the information sent was tinkered with. This knowledge allows Alice and Bob to ensure that the amount of leaked information to the eavesdropper about their key is arbitrarily small (through a classical scheme, called privacy amplification). To summarise, BB84 achieves a feat no classical cryptographic scheme can dream of - a provably secure key distribution protocol. This security relies solely on the laws of quantum physics, in particular, the

superposition principle and Heisenberg’s uncertainty principle⁷ .

B. Quantum computing

It was a quirk of (quantum) history, that in 1994 Shor, a mathematician, showed that factoring, the mathematical function safeguarding the widely used RSA protocol, can be solved in polynomial time on a quantum computer¹⁵. Shor’s algorithm not only made it clear that the security of governments, banks and private persons was at a very real risk if a quantum computer was built, it also implied that the complexity of computational problems could change significantly when quantum rules come into play. To clarify what constitutes a quantum computer, the straightforward way is to think of a classical computer with some input bits and a series of gates, such as XOR, NOT and AND, that are applied to produce the output of the computation. This setup can be “quantised”, i.e. instead of the classical states, 0 or 1, the input for a quantum computer is the superposition state of Eq. (2). A reversible gate set, consisting, for instance, of Pauli gates, Hadamard, and CNOT gates¹², can then coherently manipulate the superposition states. This intrinsic parallel capability can be identified as the fundamental reason for the quantum computer to lead to the immense speed up over (known) classical algorithms. Simply speaking, instead of one computation, starting with say a single input 0, the quantum computer runs two computations, with both inputs 0 and 1, in parallel.

However, there are other, equivalent, models of quantum computation where other quantum effects lie behind the change of computational complexity. Known models include adiabatic quantum computation and topological quantum computation^{13,14}. One radically different way of performing a quantum computation, and one that lacks a classical analogy, is measurement-based quantum computation (MBQC)¹⁶. Here computation relies on the use of a computational resource state, a highly *entangled* multi-qubit state. Many resource states can be represented by graphs. The graph vertices symbolise qubits and the graph edges indicate that entangling CNOT operations were applied to the connected vertices. A computation in MBQC is achieved by applying a sequence of adaptive measurements on individual qubits. Due to the underlying correlations between the qubits this allows information to be processed. The adaptiveness of measurements further guarantees that even though measurements are inherently random the overall output of the computation is de-

terministic. The “resource” for the exponential speed up of the MBQC model of quantum computation lies in the presence of entanglement in the resource state.

It is clear that (still theoretical) quantum computers allow an exponential speed up over (known) classical algorithms of solving certain computational problems. The reason for this increase in computational complexity can be traced to quantum rules, such as superposition and especially entanglement, in different computational models. However, it remains unresolved whether the exponential speed up is a truly quantum feature in the sense that there exists no classical algorithm that could achieve a solution exponentially quickly¹⁰. In contrast, we will present a computational situation in subsection IV B where quantum devices lead to not just a speed up but a provable increase of the actual ability to compute a certain task.

C. Quantum phases

Standard phase transitions appear when the temperature of a material, such as water, is varied across a critical value. Thermal fluctuations in the material then cause the formation of a new phase, such as ice. However, in classical systems, when absolute zero temperature is reached all thermal fluctuations are frozen out and the material is fixed in its state even when other parameters are changed, such as the pressure. In contrast, a quantum system shows fluctuations even at zero temperature as a consequence of Heisenberg’s uncertainty principle. Now these quantum fluctuations can drive phase transitions, between quantum phases, even at zero temperature. One example is the *quantum phase transition* from a superfluid to a Mott insulator, first observed in the lab in 2002¹⁸. A three-dimensional optical lattice is created with local trapping potentials of depth U at each of the M lattice points. N quantum particles, i.e. Rubidium atoms, are then loaded into the lattice and allowed to hop between neighbouring sites with a probability proportional to J . An important quantum characteristic is here that the atoms are Bosons, that is, they follow Bose-Einstein statistics instead of classical Boltzmannian statistics. Again this is a consequence of the non-commutativity of quantum mechanics and thus related to Heisenberg’s uncertainty principle. In the limit of weak interaction $U \gg J$, the trapped atomic gas is in the Mott insulator

phase, with its quantum state being given by

$$|\psi_{MI}\rangle \propto \bigotimes_{j=1}^M \left(a_j^\dagger\right)^n |0\rangle. \quad (7)$$

Here $|0\rangle$ is the vacuum state of the lattice on which $n = N/M$ creation operators, $(a_j^\dagger)^n$ are applied, each filling a Boson in the individual lattice site, j . Since the atoms are pin-pointed to their lattice sites and do not move, they can not help a current to flow, and the material is an insulator. However, when the trapping potential is reduced and crosses a *critical value*, a new phase is formed. For $J \gg U$ the gas of atoms behaves as a superfluid. This is because the atoms are shared coherently, in superposition, across the whole lattice, as expressed in the superfluid state

$$|\psi_{SF}\rangle \propto \left(\sum_{j=1}^M \frac{a_j^\dagger}{\sqrt{M}}\right)^N |0\rangle, \quad (8)$$

where each single Boson is coherently spread, in superposition, over the whole lattice, $\frac{a_1^\dagger + a_2^\dagger + \dots + a_M^\dagger}{\sqrt{M}}$. The superfluid phase is a genuinely quantum phase with exceptional characteristics, in particular, it flows without any friction. Quantum rules thus open up a plethora of qualitatively new arrangements of materials that would be impossible in a classical world. For a wide range of important physical phases it is now clear that quantum entanglement plays a central role. One example is the formation of a truly quantum phase, the Bose-Einstein condensate, another is the BCS theory of superconductivity^{24,25}.

D. Quantum effects in biology and thermodynamics

Quantum mechanics is crucial for our understanding of the stability of atoms, the periodic table of chemical elements, and determining how molecules are formed. However, when it comes to macroscopic organisms, such as cats and humans, our reasonable assumption is that all quantum effects vanish at this scale, due to decoherence²⁶. Yet exactly where the crossover is where quantum mechanics ceases to be relevant is a topic of intense debate. Excitingly, biological structures, such as the helical structure of DNA, and biological functions such as photosynthesis and the navigation mechanism that allows birds to find their way using the earth magnetic field have all been linked to quantum effects²⁷⁻²⁹. In photosynthesis, for example, energy in form of photons from the sun is captured by chromophores in bacteria or the leaves of plants. These photons are converted into electronic excitations

on a molecular level and are transported to a so-called reaction centre. Curiously, this transport happens with a much higher efficiency than what classical models predict. Now quantum transport models are being applied to this process and show good agreement²⁸. The ability of organisms to make use of absorbed sun light would then rely on the ability of a quantum excitation to be shared between different parts of the cell, in superposition, just like in the quantum superfluid phase. But it is not just biology at the microscopic scale where quantum effects bring a new twist. Even on macroscopic scales, where statistical mechanics and thermodynamics describe the behaviour, quantum mechanics could lead to qualitatively different phenomena. Even the laws of thermodynamics have been questioned and modified³⁰ when applied to quantum systems. Revising thermodynamics in the light of the development of quantum mechanics over the last century is an emerging field where some questions on the foundations of statistical mechanics have already been resolved³¹.

IV. COMPLEXITY AND COMPUTATION

Choosing correlations as the starting point the following two examples illustrate the intricate relationship between complexity and computation. The first example is concerned with the number of bits needed to fully characterise the structure of a given system, i.e. all its correlations. It turns out that this requires fewer qubits than classical bits.

A key question in the field of computational complexity is what tasks a given system can perform. The second example is concerned with a particular computational task and illustrates that quantum correlations are necessary to solve it under certain constraints.

A. Generating correlations more efficiently with quantum resources

A stochastic process is a toy model of a complex system. Being discrete and one-dimensional, it is well suited to analyse the formation of structure, a key feature of a complex system. Stochastic processes have been used to study structure formation in for example self-organisation, protein dynamics, neural dynamics³⁷⁻³⁹).

For our purposes, a stochastic process is a probability distribution $\Pr(\overleftarrow{X}; \overrightarrow{X})$ over a bi-infinite sequence of random variables X . A random variable X is a probability distribution $\Pr(X = x)$ over an alphabet $x \in \mathcal{X}$, the letters in the alphabet are the possible observa-

tions. We assume stationarity, i.e. $\Pr(X_{t_0}^{t_{n-1}} = x^n) = \Pr(X_{t_0+k}^{t_{n-1+k}} = x^n)$. \vec{X} denotes the observations of the process after some reference time t_0 and \overleftarrow{X} are the observations up to t_0 . *Structure* is simply the sum of all correlations in such a sequence of observations.

The resources required to generate a stochastic process – that is to realise the probability distribution $\Pr(\overleftarrow{X}; \vec{X})$ – are measured by the minimal size of a representation storing all the information about the correlations^{33,34}. Such a representation needs to distinguish between differing sequences of observations only if their conditional future observations statistically differ. This yields an equivalence relation \sim between all past observations, such that $\overleftarrow{x} \sim \overleftarrow{x}'$ iff $\Pr(\vec{X} | \overleftarrow{X} = \overleftarrow{x}) = \Pr(\vec{X} | \overleftarrow{X} = \overleftarrow{x}')$. Grouping together equivalent observations into *equivalence classes* $s_i \equiv \epsilon(\overleftarrow{x}) = \{\overleftarrow{x}' : \overleftarrow{x} \sim \overleftarrow{x}'\}$ we obtain a provably minimal representation of the correlations as a list of the equivalence classes \mathcal{S} , and a transition function between them $T_{ij}^x = \Pr(X = x, \mathcal{S} = s_j | \mathcal{S} = s_i)$ ^{34?}. The entropy of the probability distribution over these states is a measure of the resources required to generate the stochastic process:

$$C_\mu \equiv H(\mathcal{S}) = - \sum_i \Pr(s_i) \log \Pr(s_i) . \quad (9)$$

C_μ is called the *statistical complexity* and is measured in bits³³.

To break the classical limit of C_μ , we construct the following quantum finite-state representation. The basis set of the quantum states are constructed from the classical states \mathcal{S}_i and the letters in the alphabet x . Hence, a measurement of such a state will yield a new state and an output symbol. This way, the original stochastic process is generated through successive measurements³⁵:

$$|\psi_j\rangle = \sum_{\mathcal{S}_i \in \mathcal{S}} \sum_{x \in \mathcal{X}} \sqrt{T_{ij}^x} |\mathcal{S}_i\rangle |x\rangle . \quad (10)$$

The resulting mixed state $\rho = \sum_j \Pr(\mathcal{S}_j) |\psi_j\rangle \langle \psi_j|$ has an entropy of

$$C_q \equiv S(\rho) = -\text{tr} \rho \log \rho , \quad (11)$$

C_q is measured in qubits. It was shown that $C_q \leq C_\mu$, and in most cases C_q is strictly less than C_μ ³⁵. In other words, to generate the same amount of correlations requires fewer quantum resources than classical resources. The relevant resources are the classical and quantum states, respectively, which are the equivalent to the number of bits and quantum bits, respectively, which need to be stored by some computational device. If, for example,

C_μ is just above 2 bits and C_q just under 2 qubits it means that the classical implementation requires 3 bits where the quantum implementation only requires 2 qubits, as we will see in the example in Section IV A.

We illustrate this with the following example of a stochastic process. Consider an infinite sequence of concatenated blocks of three symbols where the first two are random and the third symbol is the logical AND of the first two (see Table II). Later on we will add a stochastic element. The alphabet is $\mathcal{X} = \{0, 1\}$. There are five equivalence classes for this process, labeled $A - E$ and represented as circles or *states* in Fig. 1. The T_{ij}^x label the *edges* between the states (setting $p = 1$ for now). We can compute the state probabilities from the left eigenvector of the transition matrix $\sum_{x \in \mathcal{X}} [T_{ij}^x]$ and obtain for the statistical complexity $C_\mu = 2.19$ bits. Hence, the generation of these correlations requires classical resources of at least 2.19 bits.

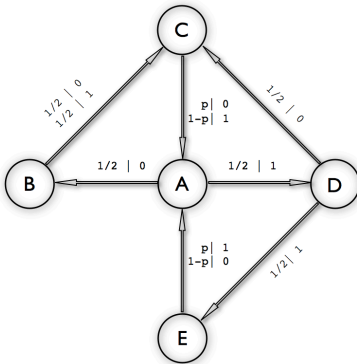


FIG. 1. Equivalence classes for the AND process. States represent equivalence classes, edges are labeled with transition probabilities and output symbols (T_{ij}^x). Going from state to state according to the probabilities on the edges will generate the AND process. $p(1-p)$ is the probability of outputting the result of a logical AND (NAND) on the last two output bits.

Constructing the quantum states using Eq. 10 we obtain the following set of states

Computing the quantum and classical complexity for the process we obtain $C_\mu = 2.19$ bits and $C_q = 2.13$ qubits. So, the amount of quantum resources required to simulate this stochastic process is slightly lower than classically. Now, we introduce an element of stochasticity into the logical operation. The probability of computing AND will now be p and the probability of computing NAND will be $1-p$. This is equivalent to a *noisy* AND gate. The T_{ij}^x change accordingly, see Fig. 1. Two of the quantum states change to the

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(|B\rangle \otimes |0\rangle + |D\rangle \otimes |1\rangle) \\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}(|C\rangle \otimes |0\rangle + |C\rangle \otimes |1\rangle) \\
|\psi_3\rangle &= |A\rangle \otimes |0\rangle \\
|\psi_4\rangle &= \frac{1}{\sqrt{2}}(|C\rangle \otimes |0\rangle + |E\rangle \otimes |1\rangle) \\
|\psi_5\rangle &= |A\rangle \otimes |1\rangle
\end{aligned}$$

following states

$$\begin{aligned}
|\psi_3\rangle &= \sqrt{p}|A\rangle \otimes |0\rangle + \sqrt{1-p}|A\rangle \otimes |1\rangle \\
|\psi_5\rangle &= \sqrt{p}|A\rangle \otimes |1\rangle + \sqrt{1-p}|A\rangle \otimes |0\rangle
\end{aligned}$$

Computing C_μ and C_q anew we notice that the C_μ is independent of p . In other words, although we are generating a process with fewer correlations we still need the same amount of classical resources (only for $p = 1/2$ $C_q = C_\mu = 0$). C_q , however, drops steadily as p increases from 0 to 1/2. So, indeed, the fewer correlations we want to generate the fewer resources we require. C_μ and C_q are plotted in Fig. 2.

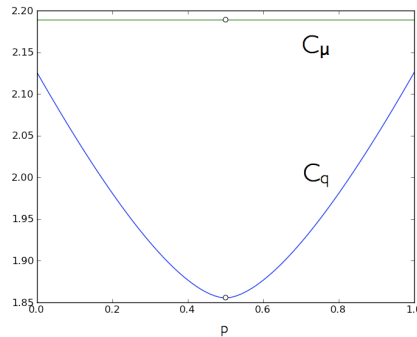


FIG. 2. C_μ and C_q for the AND process. (For $p = 1/2$ both are zero.)

The reason that C_q changes as a function of p is the ability of quantum states to be in a superposition of varying degree. For increasing p the distinction between states $|\psi_3\rangle$ and $|\psi_5\rangle$ becomes less and less relevant and we can put them closer and closer to each other in Hilbert space. Classically we can't do this. There is no analogue to a quantum superposition in classical physics.

There are processes for which there is no difference in the number of required bits and qubits, $C_\mu = C_q$. In³⁵ it was shown that this is the case if and only if the generation using the equivalence classes is reversible in the following sense: Given the current state and observation the previous state is determined³⁶. Indeed, if we choose the XOR logical operation (see Table I) instead of the AND operation we find that $C_\mu = C_q$ for any p and no gain with quantum resources is possible. We will see a similar (ir)reversibility in the next example.

Recently, evidence started emerging that some biological processes contain a quantum component. Most prominent are suggestions that photosynthesis is such an example^{40,41}. There are still many open questions. The above framework provides tools for analysing classical and a quantum aspects of information processing in a stochastic process from a rather general starting point – a data sequence only. Although the example is constructed from logic gates it illustrates the advantage of quantum over classical resources for a stochastic process. The following will illustrate the other side of the same coin: What role do quantum correlations play for the power of simple classical and quantum logic operations.

B. Raising the computational complexity using quantum correlations

In Section III B we saw that quantum computation promises algorithms that solve a range of problems exponentially faster than known classical algorithms. However, since no proof excludes the possibility of an equally fast classical algorithm the quantum speed up remains a (likely) conjecture[?]. In contrast we will now discuss an example where quantum correlations provide truly new computational power, not just a speed up, to solve an otherwise impossible task.

Suppose we are given two classical bits of information, the inputs $a, b \in \{0, 1\}$ and a very limited (and therefore totally old fashioned) pocket calculator. This pocket calculator can only do the following operations: output a constant, output the input, and output the binary sum, the XOR, of two inputs, see Tab. I. Now our task is to calculate the product of the two inputs, $a \otimes b$, also known as the AND gate, see Tab. II, with the help of our pocket computer. We notice that binary addition is a *balanced* or *linear* Boolean function, which is invertible when one of the inputs is kept as an output. In contrast, the product is an *unbalanced*, or *non-linear*, Boolean function and hence not invertible. It is easy to prove that

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

TABLE I. Truth table for the binary sum (\oplus), also called XOR gate. (Its reversible version with outputs a and $a \oplus b$ is known as the CNOT gate.)

a	b	$a \otimes b$
0	0	0
0	1	0
1	0	0
1	1	1

TABLE II. Truth table for product (\otimes), also called AND gate.

any combination of balanced functions can never result in an unbalanced function. We thus conclude it is impossible for our pocket computer to perform the required multiplication.

From the discussion of quantum cryptography, computation and phases we took the insight that quantum correlations can lead to a substantial qualitative change. Inspired by these examples one may wonder if the impossible task would become feasible by allowing our pocket computer to access *correlated sites*. To answer this let us consider two sites, as depicted in the left panel in Fig. 3, that may share correlations between them, either classical or quantum. The type of shared correlations is not specified here as we want to determine what sort of correlations we *require* to solve the computational task. We use the pocket computer to send inputs to the correlated sites and receive outputs, as depicted in Fig. 3. For two sites, the best option is to input the two bits we want to multiply, a and b , each to one of the two sites. As a consequence of the sites' previously shared correlations the returned outputs, m_1 and m_2 , may now be correlated too. The possibility that emerges here is that the correlations of the outputs could be such that their binary sum is just the required product of the inputs, $m_1 \oplus m_2 = a \otimes b$. Importantly, this sum is computable with the pocket computer. So all we need is to find the correct correlations between the sites

that produce the required correlated outputs. This can be analysed in terms of the average probability of success of this strategy,

$$P_{\text{av.succ.}} = \frac{1}{4} \sum_{a,b \in \{0,1\}} p_{\text{succ}}(m_1 \oplus m_2 = a \otimes b), \quad (12)$$

where $p_{\text{succ}}(m_1 \oplus m_2 = a \otimes b)$ is the probability that the outputs m_1 and m_2 add to give the product for a specific pair of inputs a and b . The average success probability can be rearranged³² to bring it into the form of the CHSH correlation measure introduced in Eq. (6),

$$P_{\text{av.succ.}} = \frac{p_{00}^s + p_{01}^s + p_{10}^s - p_{11}^s + 1}{4} \quad (13)$$

$$= \frac{C}{8} + \frac{1}{2} \quad (14)$$

where p_{ab}^s are the probabilities that given their two respective inputs, a and b , the two sites output the same bits, i.e. $m_1 = m_2$, and C quantifies the CHSH correlations between the two sites. The maximum success of calculating $a \otimes b$ thus directly depends on the upper bound of correlations between the two sites. As discussed in section II, classical correlations are bounded by $|C_{\text{classical}}| \leq 2$ and therefore $P_{\text{av.succ.}}^{\text{classical}} \leq \frac{1+2}{4} = 75\%$. This is a trivial result since 75% is just the success rate of adopting a constant 0 output to predict the multiplication of two arbitrary inputs a, b , see Tab. II. However, when the two sites are quantum correlated the maximum probability grows beyond the trivial benchmark of 75%, up to $P_{\text{av.succ.}}^{\text{quantum}} \approx 85\%$ for the maximally entangled Bell state, Eq. (5), with $|C_{\text{quantum}}| = \sqrt{2}$. Moreover, it can be shown that with three sites the success probability for $a \otimes b$ can be brought to 100% while classical states can never achieve 100%³. The quantum state with the required correlations is the three-party Greenberger-Horne-Zeilinger (GHZ) state²⁰,

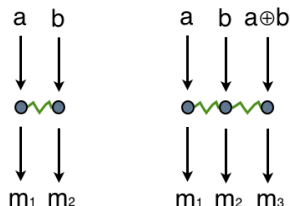


FIG. 3. Left panel: Two sites (circles) with shared correlations (zig-zag line) receive the inputs a and b and output m_1 and m_2 , respectively. Right panel: Three correlated sites, receiving inputs a, b and $a \oplus b$, respectively.

$|\psi_{GHZ}\rangle = \frac{|0_1 0_2 1_3\rangle + |1_1 1_2 0_3\rangle}{\sqrt{2}}$, a famous entangled state²¹. To make the result explicit, the inputs a , b and $a \oplus b$ will determine measurements on the three sites of the state, see right panel in Fig. 3. Two different measurement bases are used depending on the input bit. For input 0 the measurement basis is the x -basis $\{|+\rangle, |-\rangle\}$ while for input 1 the measurement basis is the y -basis $\{|+i\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}, |-i\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\}$. The output bits are 0 for a “+” outcome and 1 for a “-” outcome. In conclusion, we have found that a limited XOR computer can be boosted to compute incomputable functions, such as AND, when given access to quantum correlations. While the exponential speed up of quantum computers over classical computers remains a conjecture, the increase in computability due to quantum correlations is a provable fact clearly exposing the computational advantage of quantum correlations over classical ones.

C. Discussion of complexity and correlations

In both examples we consider the logical operations AND and XOR. Figure 4 summarises the commonalities. In Section IV B we saw that under certain constraints the implementation of the AND gate can only be done error free if one has access to quantum correlations. The implementation of the XOR gate, on the other hand, is unaffected by access to quantum resources. The reason for this lies in the linear vs non-linear character of the XOR and AND operation, respectively, an intriguing subject unfortunately outside of the scope of this article. The example in Section IV A gave a complimentary perspective on the power of correlations. Here, it was the simulation of correlations which could be done with fewer computational resources when quantum physics was used. Here, too, this advantage was only present for a process involving the AND logical operation and not for the XOR operation. This is for the same reasons as above, the non-linearity of the AND operation leads to this gain in efficiency.

V. DISCUSSION

We have seen that quantum physics offers a wide range of new phenomena, including unbreakably secure cryptography, exponentially fast computations, the superfluid phase, and even fast exciton transport in photosynthesis. In the field of complex systems such

task ★gate	description of stochastic process with ★ using classical or quantum states	computation of ★ gate using classical or quantum correlated states
AND	bits required: quantum $C_q = 1.85$ classical $C_\mu = 2.19$	probability of success: quantum 100% classical 75%
XOR	bits required: quantum $C_q = 2.00$ classical $C_\mu = 2.00$	probability of success: quantum 100% classical 100%

FIG. 4. A summary of the two examples. Left column: The stochastic process involving the AND logical operation is more efficiently simulated using quantum resources. Right column: The computational task of an AND logical gate can only be performed with 100% accuracy using quantum correlations (under certain constraints). For details see text.

qualitatively new properties that *emerge* out of the constituent parts and their interactions are considered a feature of *complexity*. The striking effect of quantum resources in all of the above examples is that they assist in increasing the complexity. A high amount of correlations between constituent parts is also a feature of a complex system, and often used to quantify its complexity. In the field of quantum information entanglement, a well-defined and particularly striking type of (quantum) correlations, has turned out to be of central importance for exactly that reason. It effectively measures the complexity of quantum systems and processes. However, entanglement is not the only indicator of complexity, weaker quantum correlations exist, such as discord, quantum relative entropy and minimum entanglement potential⁵⁻⁷. They have in common that they are all purely quantum features and their presence can enhance quantum computations⁴.

In the light of the above we believe that complex systems science, despite the different physics, can learn from the central role quantum correlations play for such ‘emergent’ phenomena. Taking correlations as our starting point we have exemplified that two originally separate meanings of the term complexity can be united. On the one hand one speaks of complexity in a complex system which represents the amount of structure, among other

things. On the other hand we speak of computational complexity as a measure of difficulty of solving a computational task. The examples illustrated that the use of the word *complexity* in both cases is not a coincidence but rather a signature of the commonalities between the two research areas. Both are concerned with the power of correlations.

Acknowledgements JA acknowledges funding from the Royal Society. KW acknowledges funding through EPSRC grant EP/E501214/1 and the Santa Fe Institute for their hospitality during the workshop.

REFERENCES

- ¹M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2000.
- ²R. P. Feynman, R. B. Leighton, and M. Sands, Lectures on Physics: Quantum Mechanics v. 3, 1st ed. Addison Wesley, 1971.
- ³J. Anders, D. E. Browne, Phys. Rev. Lett. 102, 050502 (2009).
- ⁴Z. Merali, Nature 474, 24 (2011).
- ⁵H. Ollivier and W.H. Zurek, Phys. Rev. Lett. 88, 017901 (2001).
- ⁶M. Horodecki, J. Oppenheim and A. Winter, Nature 436, 673 (2005)
- ⁷M. Piani, S. Gharibian, G. Adesso, J. Calsamiglia, P. Horodecki, A. Winter, Phys. Rev. Lett. 106, 220403 (2011).
- ⁸B. S. Tsirelson, Lett. Math. Phys. 4, 93 (1980).
- ⁹Factoring is a function problem and actually in the complexity class FNP, http://en.wikipedia.org/wiki/Integer_factorization , a sister of the more famous NP¹⁰.
- ¹⁰The computational complexity class NP has appeared in the popular media recently, <http://www.newscientist.com/article/dn19287-p--np-its-bad-news-for-the-power-of-computing.html>, both, because of its central importance for computer science and quantum computing, and because of its prize money of 1 Million USD, http://www.claymath.org/millennium/P_vs_NP/.
- ¹¹C. H. Bennett and G. Brassard, in Proceedings of IEEE Intern. Conf. on Computer Systems and Signal Processing (1984), Volume: 11, IEEE Press , 175 (1984).
- ¹²C. H. Bennett, IBM Journal of Research and Development 17, 525 (1973).

- ¹³E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, arXiv:quant-ph/0001106v1 (2000).
- ¹⁴First proposed by A. Kitaev; S. Das Sarma, M. Freedman and C. Nayak, Phys. Rev. Lett. 94, 166802 (2005).
- ¹⁵P. W. Shor, SIAM J.SCI.STATIST.COMPUT. 26, 1484 (1997). arXiv:quant-ph/9508027v2 (1995).
- ¹⁶R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001); R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A 68, 022312 (2003); H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf and M. Van den Nest, Nature Physics 5, 19 (2009).
- ¹⁷J. Anders, M. Hajdusek, D. Markham, V. Vedral, Foundations of Physics 38, 506 (2008).
- ¹⁸M. Greiner, O. Mandel, T. Esslinger, T. Hänsch, I. Bloch, Nature 415, 39 (2002).
- ¹⁹J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
- ²⁰D. M. Greenberger, M. A. Horne, and A. Zeilinger, in Bells Theorem, Quantum Theory, and Conceptions, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 69.
- ²¹N. D. Mermin, Am. J. Phys. 58, 731 (1990).
- ²²A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
- ²³L. Lydersen, et al., Nature Photonics 4 686 (2010).
- ²⁴J. Anders, V. Vedral, Open Systems & Information Dynamics 14, 1 (2007); E. Rieper, J. Anders, V. Vedral, New Journal Physics 12, 025017 (2010).
- ²⁵J. Anders, D. Kaszlikowski, Ch. Lunkes, T. Ohshima, V. Vedral, New Journal of Physics 8, 140 (2006).
- ²⁶W. H. Zurek, Reviews of Modern Physics 75, 715 (2003).
- ²⁷E. Rieper, J. Anders, V. Vedral, arXiv:1006.4053v2 (2010).
- ²⁸M. Mohseni, P. Rebentrost, S. Lloyd, and A. Aspuru-Guzik, The Journal of Chemical Physics, 129(17):174106, (2008); F. Caruso, A. W. Chin, A. Datta, S. F. Huelga, and M. B. Plenio, The Journal of Chemical Physics, 131(10):105106, (2009); F. Fassioli, A. Olaya-Castro, S. Scheuring, J. N. Sturgis, and N.F. Johnson, Biophysical journal, 97(9):24642473, 11 (2009).
- ²⁹E. M. Gauger, E. Rieper, J. J. L. Morton, S.C. Benjamin, and V. Vedral, Phys. Rev. Lett. 106, 040503 (2011); J. Cai, G.G. Guerreschi, and H.J. Briegel, Phys. Rev. Lett. 104, 220502 (2010).
- ³⁰S. Hilt, S. Shabbir, J. Anders, E. Lutz, Physical Review E (Rapid), 83, 030102 (2011).

- ³¹S. Popescu, A. J. Short, A. Winter, *Nature Physics* 2, 754 (2006).
- ³²W. van Dam, arXiv: quant-ph/0501159 (2005). M. Hoban, E. Campbell, K. Loukopoulos, D.E. Browne, *New Journal of Physics* 13, 023014 (2011).
- ³³J. P. Crutchfield and K. Young, *Phys. Rev. Lett.* 63, 105 (1989).
- ³⁴C. R. Shalizi and J. P. Crutchfield, *J. Stat. Phys.* 104, 817 (2001).
- ³⁵M. Gu, K. Wiesner, E. Rieper, and V. Vedral, arXiv:1102.1994 (2011).
- ³⁶K. Wiesner, M. Gu, E. Rieper, and V. Vedral, arXiv:0905.2918 (2009).
- ³⁷C.-B. Li, H. Yang, and T. Komatsuzaki, *Proc. Nat. Acad. Sci.* 105, 536 (2008).
- ³⁸C. R. Shalizi, K. L. Shalizi, and R. Haslinger, *Phys. Rev. Lett.* 93, 118701 (2004).
- ³⁹R. Haslinger, K. L. Klinkner, and C. R. Shalizi, *Neural Computation* 22, 121 (2010)
- ⁴⁰G. S. Engel et al., *Nature* 446, 782 (2007).
- ⁴¹H. Lee, Y.-C. Cheng, and G. R. Fleming, *Science* 316, 1462 (2007).
- ⁴²R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, *Rev. Mod. Phys.* 81, 865 (2009).