Algorithmic Complexity and Entanglement of Quantum States

Caterina E. Mora[1] and Hans J. Briegel[1,2]

[1]*Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften, Innsbruck, Austria*
[2]*Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*

(Received 30 May 2005; published 9 November 2005)

We define the algorithmic complexity of a quantum state relative to a given precision parameter, and give upper bounds for various examples of states. We also establish a connection between the entanglement of a quantum state and its algorithmic complexity.

DOI: 10.1103/PhysRevLett.95.200503 PACS numbers: 03.67.Lx, 03.65.Ud, 03.67.Mn

Algorithmic information provides a concise notion of complexity, or randomness, for individual classical objects. It is measured by the length of the shortest computer program that produces a faithful image of the object, usually represented as a string of binary numbers [1–3]. This notion of complexity has not only added a new perspective to abstract areas such as mathematical proof theory (Gödel's theorem) [3] but it has also been applied successfully to a range of problems in thermodynamics. Examples are the Maxwell demon paradox [4,5], and the treatment of irreversibility in classical chaotic systems [6,7].

Quantum theory has changed our conception of physical objects, whose states are described as vectors in a Hilbert space. For composite objects, this leads to the fundamental property of quantum entanglement, which cannot be explained by any classical theory. A consistent discussion of the thermodynamics of systems that are monitored by quantum information processing devices should therefore be based on an appropriate definition of the algorithmic complexity of quantum states.

In this Letter, we propose a definition for the algorithmic complexity of a quantum state that depends on a given precision parameter, and give upper bounds on complexity for various examples of states. We also establish a connection between the entanglement of a quantum state (in terms of its Schmidt measure [8]) and its algorithmic complexity. Earlier proposals for the algorithmic complexity exist; they are based either on the reproducibility of a quantum state via Turing machines [9,10] or on universal probability [11]. Our proposal is based on the idea that each quantum state is ultimately identified with an experimental preparation process [12]. The definition of the algorithmic complexity of a quantum state is thus naturally reduced to the description complexity of its (abstract) preparation process. A similar approach has been introduced in Ref. [13] in the analysis of relations between computation complexity and entanglement.

To motivate our definition of the algorithmic complexity of a quantum state, we consider the following scenario. Alice has created a certain quantum state in her laboratory and wants to describe this state to Bob, who is supposed to reproduce it in his laboratory. How difficult is it for Alice to describe to Bob the state of her system? In order to answer this question we may distinguish the two situations in which Alice and Bob communicate via a classical or a quantum channel. In the latter case, Alice may send to Bob the quantum state altogether (or in some Schumacher compressed form) [14]. If the communication is classical, this is not possible. On the other hand, as a quantum state can be regarded as the result of some experimental preparation procedure, Alice may choose to send to Bob the latter. In this case, the complexity of a quantum state is identified, in a very natural way, with the description complexity of an experimental preparation procedure [15].

Even though the first approach may seem "more quantum," it lacks an important feature that we usually associate with the *description* of an object. Even if Bob has the state sent by Alice, he might not know what state he has received. In this Letter, we shall thus follow the second approach and identify the algorithmic complexity of a quantum state with its preparation complexity, i.e., the classical description complexity of the preparation procedure.

To be able to communicate, Alice and Bob must first have agreed on a common language which they are using to describe their preparation procedure. Ideally, they will also use the same "toolbox" to compose their experiments and the same words when referring to elements of this toolbox. The toolbox is in general an abstraction from any real experimental scenario: in quantum information theory such an abstraction leads to defining the toolbox by a set of elementary operations on a Hilbert space with a given tensor-product structure and dimension. In particular such a toolbox will include the ability to prepare some standard reference state, and a finite set of elementary operations. A complete preparation procedure is then described as a sequence of unitary transformations and possibly measurements applied to the reference state.

In classical information theory, the algorithmic complexity of an object measures the amount of information necessary to reproduce it. The Kolmogorov complexity K_{Cl} of a binary string $\boldsymbol{\omega}$ is defined as *the length of the shortest program that, running on a universal Turing machine, gives* $\boldsymbol{\omega}$ *as output*. We stress that algorithmic complexity takes into account only the length of the program (and thus the length of the description of the object) and not the time needed by the computer to actually run the program. This

last quantity is instead studied by the computational complexity and is related to a different property of objects, that is, their logical depth [16].

It is always possible to reproduce a string $\boldsymbol{\omega} = \omega_{i_1}\omega_{i_2}\cdots$ by means of a program of the form "*write* $\omega_{i_1}\omega_{i_2}\cdots$." This implies that the length of a string constitutes (up to a constant) an upper bound for the complexity of the string itself: $K_{\mathrm{Cl}}(\boldsymbol{\omega}_n) \lesssim l(\boldsymbol{\omega}_n) = n$ [17]. Naturally there are sequences for which this upper bound is far too large: the complexity of a periodic string, for example, grows only logarithmically with the length of the sequence. A string is said to be *complex* (or structureless, or random) if its algorithmic complexity grows linearly with its length: these are the strings typically generated by random sources (e.g., a coin toss).

Considering that a quantum state can be characterized by a sequence of elementary operations (represented, e.g., as a "circuit"), we define the complexity of a state referring to that of the circuit itself. A finite set of gates (constituting a *complete gate basis*) is suitable to prepare any state up to an arbitrary precision. Through adequate *coding*, the circuit is reduced to a (classical) string whose Kolmogorov complexity is well-defined and which can be associated with the original state. In this way the algorithmic complexity of a state satisfies the intuitive idea of complexity as a measure of "how difficult" it is to prepare a state. Since with a finite number of gates only a countable set of states can be prepared exactly, it is necessary to introduce a *precision parameter* in such a definition.

From now on we represent with $\mathcal{Q}_N$ the space generated by N qubits and with $|0\rangle_N \in \mathcal{Q}_N$ the vector $|0\rangle_N = |0\rangle^{\otimes N}$, where each $|0\rangle$ is an element of the computational basis $\{|0\rangle, |1\rangle\}$ of a single-qubit Hilbert space. We represent with $C|0\rangle_N$ the result of the application of a circuit C on the state $|0\rangle_N$; if $|\langle\varphi|C|0\rangle_N|^2 \geq 1-\varepsilon$ we will say that C prepares $|\varphi\rangle$ with precision ε (where $0 \leq \varepsilon \leq 1$). We say that two states $|\varphi\rangle$ and $|\psi\rangle$ are ε *distinguishable* if $|\langle\psi|\varphi\rangle|^2 \leq 1-\varepsilon$.

Once we fix a complete gate basis B and a code Ω, the procedure to compute the algorithmic complexity of state $|\varphi\rangle$ is the following. (1) With the gates contained in the basis B, build a circuit $C^{B,\varepsilon}$ that prepares $|\varphi\rangle$ with precision ε. (2) Code the circuit, obtaining a classical sequence $\boldsymbol{\omega}^{\Omega}(C^{B,\varepsilon}) = \omega^{\Omega}_{i_1}\cdots\omega^{\Omega}_{i_m}$ of symbols $\omega^{\Omega}_{i_k} = \omega^{\Omega}_{i_k}(C^{B,\varepsilon}) \in \Omega$. The algorithmic complexity of a state, relative to the basis B, the code Ω, and the circuit C^B, with precision parameter ε is $K^{\Omega,B,C^{B,\varepsilon}}_{\mathrm{Net}}(|\varphi\rangle) = K_{\mathrm{Cl}}[\boldsymbol{\omega}^{\Omega}(C^{B,\varepsilon})]$. (3) In general, there are more circuits that prepare the same state $|\varphi\rangle$, and, in principle, the corresponding complexities can be different. In order to define a property of the state itself (and not related to the circuit used to reproduce it) we minimize over all of them.

Definition.—The algorithmic complexity of the state $|\varphi\rangle$, relative to the code Ω and the gate basis B, with precision parameter ε is

$$K^{\Omega,B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle) = \min_{C^{B,\varepsilon}\in\tilde{C}^{B,\varepsilon}} K^{\Omega,B,C^{B,\varepsilon}}_{\mathrm{Net}}(|\varphi\rangle) \qquad (1)$$

where $\tilde{C}^{B,\varepsilon}$ is the set of all the circuits built with gates from B that prepare $|\varphi\rangle$ with precision ε.

Considering that the *choice of code* and *basis* is arbitrary, it is necessary to study how it influences the complexity of the state. It is also relevant to consider how the complexity of a quantum state depends on the *precision* with which we are required to reproduce it.

Dependence on the code.—If Ω and $\underline{\Omega}$ are two different codes, then, for any state $|\varphi\rangle$ and any precision parameter ε: $K^{\Omega,B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle) = K^{\underline{\Omega},B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle) + k_{\Omega,\underline{\Omega}}$, where $k_{\Omega,\underline{\Omega}}$ is a constant that depends only on Ω and $\underline{\Omega}$. $k_{\Omega,\underline{\Omega}}$ is the length of a "dictionary" with which it is possible to translate the description made using one code to that made using the other. Since both codes are finite, such a dictionary is finite too and, in the limit of big values of $K^{\Omega,B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle)$, its contribute is negligible. Considering this code-invariance property we can omit explicating the dependence on the code (we can imagine fixing it once and for all) and write simply: $K^{B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle)$.

Complexity and precision.—Let us consider now how the complexity of a state depends on the precision parameter. It has been shown [18] that using just the set of all 1-qubit gates, plus the controlled-NOT, it is possible to reproduce any unitary operation U over $\mathcal{Q}_N$ using $\mathcal{O}(4^N)$ gates. However, if one is interested in reproducing the action of a unitary operation on one particular (given) state, $\mathcal{O}(2^N)$ such gates are sufficient. Thus, to prepare any state $|\varphi\rangle$ from the given initial state $|0\rangle_N$ we need at most $\mathcal{O}(2^N)$ gates. We consider now the Solvay-Kitaev theorem [19] which implies that any circuit acting on $\mathcal{Q}_N$ built with m 1-qubit and C-NOT gates and can be reproduced up to precision ε using $\mathcal{O}[m\log^c(\frac{m}{\varepsilon})]$ gates from a finite gate basis ($c \in [1,2]$ is a constant whose exact value is not yet known). It follows that the action of any unitary transformation on $|0\rangle_N$ can be implemented (and thus any $|\varphi\rangle \in \mathcal{Q}_N$ can be prepared) up to precision ε via a circuit built with gates from any finite and complete basis; futhermore, the number of gates in such a circuit is $M \sim 2^N \log\frac{1}{\varepsilon}$.

The length of the string that codes the circuit grows linearly with the number of gates of the circuit itself: to code a circuit that prepares a general state $|\varphi\rangle \in \mathcal{Q}_N$ we need thus a sequence whose length is (proportional to) M. From what seen above we then have

$$K^{B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle \in \mathcal{Q}_N) \lesssim 2^N \log\frac{1}{\varepsilon}. \qquad (2)$$

We notice that this bound is much higher than the classical one, where the complexity grows at most linearly with the number of bits of the string. Intuitively this reflects the fact that the space of quantum objects is much richer than that of classical ones. In the last part of this work we will also see that such difference can be explained by quantum entanglement.

Dependence on the basis.—The definition of the algorithmic complexity of a state has a dependence on the choice of the basis. Given any state $|\varphi\rangle$ there always exists

a particular basis whose usage makes the preparation of $|\varphi\rangle$ trivial. If Alice wants to describe to Bob a state and they have previously agreed on using a certain gate basis, then Alice has only to describe the circuit (passing the sequence $\boldsymbol{\omega}_C$). If they have not agreed on a particular gate basis, then Alice could indeed build a circuit using the "best" basis, but in this case she would have to describe the basis itself to Bob, and this would be a similarly difficult task [20].

One might nevertheless wonder whether there is some particular basis that can describe all (or almost all) states with simple circuits. If such a basis existed it would obviously be convenient for Alice and Bob to agree on using that and (almost) all states would be noncomplex. In the following we show that such a basis cannot exist as, once *any* gate basis is fixed, the number of noncomplex states is small in relation to the total number of states.

In classical information theory it is known that the number of compressible (bit) strings is "small;" more precisely the ratio between the strings with complexity smaller than a constant k and the total number of n-bit strings is bound by $(2^k - 1)2^{-n}$.

As we have seen in the previous paragraphs, once we fix a basis B and a precision parameter ε, we can associate with every quantum state $|\varphi\rangle$ a $(2^N \log\frac{1}{\varepsilon})$-bit string $\hat{\boldsymbol{\omega}}^B_\varepsilon(|\varphi\rangle)$ whose classical algorithmic complexity coincides with the complexity of $|\varphi\rangle$. The result seen above for classical bit strings can thus be generalized to quantum states and one finds that the ratio between compressible quantum states [such that $K^B_\varepsilon(|\varphi\rangle) < k$] and the total number of ε-distinguishable normalized states is bound by $2^{2^N \log\varepsilon}(2^k - 1) \simeq 2^{2^N \log\varepsilon + k}$. Such a relation holds true also in the case when $k = k(N, \varepsilon)$ is a function. State $|\varphi\rangle$ will be noncomplex only if its complexity is $o(2^N \log\frac{1}{\varepsilon})$: this means that the right member of the inequality becomes $2^{2^N \log\varepsilon + o[2^N \log(1/\varepsilon)]} \sim 2^{2^N \log\varepsilon} \ll 1$. Thus, one obtains that for any fixed basis B, the number of noncomplex states is exponentially small [21].

Note that there are cases in which the complexity is invariant for basis choice. This happens, for example, when we consider a *coarsening* of the gate basis; that is, if we consider two gate bases B and $\underline{B}$, one of which ($\underline{B}$) is constituted of gates that can be built with gates from B (e.g., $\underline{B}$ contains a Toffoli gate, while B contains Hadamard and C-NOT). In this case, any circuit made by gates from $\underline{B}$ can be reproduced by one made by gates from B. The string that codes this circuit will, in general, be longer than that of the original circuit, but their complexities will change only for a (small) constant $k_{B,\underline{B}}$ (that represents the length of a dictionary between the two gate bases).

From a less abstract point of view, this property translates into a form of invariance with respect to the choice of the experimental apparatus. It is not required that the circuit be actually built only with the elementary gates: the use of more complex components does not modify the complexity of the description as long as they are themselves composed of elementary parts.

Entanglement and complexity.—The nature of quantum correlations has been a central issue of long-lasting debates on the interpretation of quantum mechanics. In recent years, the notion of entanglement has been recognized as central to quantum information processings [23]. As a result, the task of characterizing quantum entanglement, and the properties related to it, has emerged as one of the prominent themes of quantum information theory. In the last part of this Letter we investigate the relations between the algorithmic complexity of a state and its entanglement properties.

Let us begin by considering the case of a J-separable state $|\varphi\rangle \in \mathcal{Q}_N$ of the type $|\varphi\rangle = \bigotimes_{j=1}^J |\varphi_j\rangle$, with $|\varphi_j\rangle \in \mathcal{Q}_{N_j}$, $\dim(\mathcal{Q}_{N_j}) = 2^{N_j}$, and $\sum_{j=1}^J N_j = N$. State $|\varphi\rangle$ is not totally entangled, as it can be written as the tensor product of other (possibly entangled) states $|\varphi_j\rangle$ [with $K^{B,\varepsilon}_{\mathrm{Net}}(|\varphi_j\rangle) \leq 2^{N_j} \log\frac{1}{\varepsilon}$]. As a consequence of this fact we have $K^{B,\varepsilon}_{\mathrm{Net}}(|\varphi_j\rangle) \leq \sum_{j=1}^J K^{B,\varepsilon/J}_{\mathrm{Net}}(|\varphi_j\rangle) < 2^N \log\frac{1}{\varepsilon}$, where we have used the fact that $|\varphi\rangle$ is prepared with precision ε if all states $|\varphi_j\rangle$ are prepared with precision ε/J [24]. Given any $J \geq 1$, there thus exist $(J-1)$-separable states whose complexity is larger than that of *any* J-separable state.

Thus, the *maximal complexity* can be obtained *only* by a truly N-party entangled state (in the sense that it cannot be written as tensor product of states contained in subspaces of $\mathcal{Q}_N$). We stress that this consideration does not imply that all totally entangled states have maximal complexity. Counterexamples are given by W, GHZ [25], and the N-qubit graph states. The latter are highly entangled, but nevertheless their complexity is bound by $N^2 \log\frac{1}{\varepsilon}$ [24]. As another example let us consider a state $|\varphi\rangle \in \mathcal{Q}_N$ of the form $|\varphi\rangle = \bigotimes_{j=1}^N |\varphi_j\rangle$, $|\varphi_j\rangle \in \mathcal{Q}_1$. In this case we have $K^{B,\varepsilon}_{\mathrm{Net}}(|\varphi\rangle) \leq \sum_{j=1}^N K^{B,\varepsilon/N}_{\mathrm{Net}}(|\varphi_j\rangle) \leq 2N \log\frac{N}{\varepsilon}$. Thus the complexity of a separable state can grow only at most linearly with the number of qubits.

The relation, illustrated by the examples above, between complexity and entanglement can be formalized if we choose the *Schmidt measure* [8] as a measure of entanglement. Given a quantum state $|\Phi\rangle \in \mathcal{Q}_N$, its Schmidt measure $E_S(|\varphi\rangle)$ is defined as the logarithm of the minimum number r of separable states $|\varphi_i\rangle \in \mathcal{Q}_N$ such that $|\Phi\rangle = \sum_{i=1}^r \alpha_i |\varphi_i\rangle \in \mathcal{Q}_N$. In the following, we show how the knowledge of the Schmidt measure of a quantum state $|\Phi\rangle$ allows us to give an upper bound on its complexity.

In order to do this we specify a circuit that prepares $|\Phi\rangle$. The general idea is to compose such a circuit "using" the circuits that prepare the states $|\varphi_i\rangle$ that appear in the decomposition of $|\Phi\rangle$. Such a circuit is built with the aid of $\log r$ "ancilla" qubits, initially prepared in the superposition state $|a\rangle = \sum_{i=0}^r \alpha_i |i\rangle$ (where $|i\rangle$ is the state whose binary representation gives the state of the $\log r$ qubits). We then apply to the initial state $|0\rangle$ a circuit consisting of controlled $C^B_\varepsilon(|\varphi_i\rangle)$ (in series), the application of each conditional on the ancilla being in state $|i\rangle$. The last step

is to project the ancilla on state $\sum_{i=1}^{r}|i\rangle/\sqrt{r} = \bigotimes_{j=1}^{\log r}(|0\rangle_j + |1\rangle_j)/\sqrt{2}$: state $|\Phi\rangle$ is prepared if the result is nonzero. If this is not the case, it is sufficient to repeat the procedure from the beginning [26]. The complexity of the state $|\Phi\rangle$ can now be expressed in terms of the complexity of the ancilla state $|a\rangle$ and of that of the remaining circuit.

The ancilla can, in principle, be any state of $\log r$ qubits; from what was seen in the above sections we thus have $K_{\mathrm{Net}}^{B,\varepsilon}(|a\rangle) \leq 2^{\log r}\log\frac{1}{\varepsilon} = r\log\frac{1}{\varepsilon}$. Once the ancilla is prepared in the required state, it is necessary to describe the remaining circuit. First of all we must describe the individual circuits $C_{\varepsilon}^{B}(|\varphi_i\rangle)$ (and this requires a number of bits bounded by the sum of the complexities of the single states $|\varphi_i\rangle$). Performing each of these circuits as a controlled operation requires additional $\mathcal{O}(\log r\log\frac{1}{\varepsilon})$ gates from B. We thus have

$$K_{\mathrm{Net}}^{B,\varepsilon}(|\Phi\rangle) \lesssim 3N2^{E_S(|\Phi\rangle)}\log\frac{1}{\varepsilon}, \tag{3}$$

where we have used the fact that, as the states $|\varphi_i\rangle$ are separable, their complexity is bound by $2N\log\frac{1}{\epsilon}$. If $|\Phi\rangle$ is separable, in fact, we have $E_S(|\Phi\rangle) = 0$, and the equation above takes the form $K_{\mathrm{Net}}^{B,\epsilon}(|\Phi\rangle) \leq 3N\log\frac{1}{\epsilon}$. Alternatively, when the state $|\Phi\rangle$ is truly entangled, with Schmidt measure $\log r = N$, we have $K_{\mathrm{Net}}^{B,\varepsilon}(|\Phi\rangle) \leq 2N2^N\log\frac{1}{\varepsilon} \sim 2^N\log\frac{1}{\varepsilon}$ (up to a polynomial term).

The notion of complexity described in this Letter can be extended to mixed quantum states. Given a state ρ its algorithmic complexity is defined as $K_{\mathrm{Net}}^{B,\varepsilon}(\rho) = \min\prod_i[K_{\mathrm{Net}}^{B,\varepsilon}(|\varphi\rangle)]^{\lambda_i}$, where the minimum is taken over all pure state mixtures such that $\rho = \sum_i\lambda_i|\varphi_i\rangle\langle\varphi_i|$. Thus the complexity of a mixed state is the average complexity of the states that appear in its (optimal) mixture. The choice of the geometric average is dictated by the necessity of giving an adequate weight to the probability distribution. Such a definition coincides with the one we have introduced in this Letter in the pure state case. Furthermore, one finds that the relationship between entanglement and complexity also holds. In particular we have $K_{\mathrm{Net}}^{B,\varepsilon} \lesssim 3N2^{E_S(\rho)}\log\frac{1}{\varepsilon}$, where $E_S(\rho)$ is the Schmidt measure of the mixed state ρ as defined in Ref. [8].

In this Letter we have introduced a new notion of algorithmic complexity of a quantum state, based on the classical description of its preparation procedure. We have seen how the complexity of a quantum state grows, in general, exponentially with the number of qubits and this is significantly different from the algorithmic complexity of classical objects (where the upper bound is linear with the number of bits). In the last part we have shown how this difference can be interpreted as a consequence of the presence of quantum correlations, by giving a bound on the complexity of a state in terms of its entanglement. A consequence of this is that the absence of entanglement (i.e., in completely separable states) reestablishes the classical limit for the complexity bound. Entanglement thus again proves to be a fundamental feature that distinguishes quantum objects from classical ones.

We wish to thank M. Bremner and M. Piani for their help in editing the manuscript. This work was supported in part by the FWF, the DFG, and the EU (IST-2001-38877, -39227, OLAQUI, SCALA).

[1] R. J. Solomonoff, Inf. Control **7** 1 (1964).
[2] A. N. Kolmogorov, Probl. Inf. Transm. (Engl Trans) **1** 1 (1965).
[3] G. J. Chaitin, *Information, Randomness & Incompleteness* (World Scientific, Singapore, 1987).
[4] C. H. Bennett, Int. J. Theor. Phys. **21** 905 (1982).
[5] W. H. Zurek, Nature (London) **341** 119 (1989).
[6] R. Schack and C. M. Caves, Phys. Rev. Lett. **69**, 3413 (1992).
[7] C. M. Caves, Phys. Rev. E **47**, 4010 (1993).
[8] J. Eisert and H. J. Briegel, Phys. Rev. A **64**, 022306 (2001).
[9] A. Berthiaume, W. van Dam, and S. Laplante, J. Comput. Syst. Sci. **63** (2001).
[10] P. Vitanyi, IEEE Trans. Inf. Theory **47** 2464 (2001).
[11] P. Gács, J. Phys. A **34** 6859 (2001).
[12] N. Bohr, *Atomic Physics and Human Knowledge* (Wiley, New York, 1958).
[13] T. Yamakami, quant-ph/0412172.
[14] Adopting this scenario we arrive at a notion of complexity similar to that introduced in Ref. [9].
[15] This approach is close to Bohr's viewpoint that the quantum state is essentially an expression of an experimental scenario [12].
[16] C. H. Bennett, *How to Define Complexity in Physics and Why* (Addison-Wesley, Redwood City California, 1990), pp. 137–148.
[17] Here and in the following we use the "approximate" signs ($\simeq, \lesssim$) when the relationships are expressed up to the leading order.
[18] J. J. Vartiainen, M. Möttönen, and M. M. Salomaa, Phys. Rev. Lett. **92**, 177902, (2004).
[19] A. Y. Kitaev, Russ. Math. Surv. **52** 1191 (1997).
[20] This, in fact, would again require us to describe arbitrary unitary transformations.
[21] Even though almost all states are complex, it is impossible to prove that any given state is. This derives from the fact that the statement "The complexity of the classical string $\boldsymbol{\omega}$ is greater than N" is unprovable [22].
[22] G. J. Chaitin, Sci. Am. **232**, 5 (1975).
[23] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England 2000).
[24] C. E. Mora and H. J. Briegel, quant-ph/0412172.
[25] The W and GHZ states are N-qubit entangled states of the form, respectively, $(|0\ldots01\rangle + |0\ldots10\rangle + |1\ldots00\rangle)/\sqrt{N}$ and $(|00\ldots0\rangle + |11\ldots1\rangle)/\sqrt{2}$.
[26] This procedure succeeds with exponentially low probability, but this is not relevant from our point of view: we are, in fact, interested in the description of the procedure, not in the time or resources needed to apply it.