Physics Letters A ••• (••••) •••–•••

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Computing with a single qubit faster than the computation quantum speed limit

Nikolai A. Sinitsyn

Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA

A R T I C L E I N F O

Article history:
Received 30 September 2017
Received in revised form 16 December 2017
Accepted 20 December 2017
Available online xxxx
Communicated by A. Eisfeld

Keywords:
Quantum speed limit
Quantum resource
Quantum gate fidelity
Quantum computing

A B S T R A C T

The possibility to save and process information in fundamentally indistinguishable states is the quantum mechanical resource that is not encountered in classical computing. I demonstrate that, if energy constraints are imposed, this resource can be used to accelerate information-processing without relying on entanglement or any other type of quantum correlations. In fact, there are computational problems that can be solved much faster, in comparison to currently used classical schemes, by saving intermediate information in nonorthogonal states of just a single qubit. There are also error correction strategies that protect such computations.

Introduction. The quantum phase space of a qubit is a sphere (Fig. 1). One can discretize this space into any number of states and then apply field pulses to switch between the chosen states in an arbitrary order. In this sense, a qubit comprises the whole universe of choices for computation. For example, a qubit can work as finite automata [1] when different unitary gates act on this qubit depending on arriving digital words. However, different states of a qubit are generally not distinguishable by measurements. So, if the final quantum state encodes the result of computation, we cannot generally extract this information because we cannot distinguish this state by a measurement from other non-orthogonal possibilities reliably.

For such reasons, qubits are believed to provide computational advantage over classical memory only when they are used to create purely quantum correlations, i.e., entanglement or quantum discord [2]. While very powerful algorithms have been designed based on such correlations, the degree of control over the state of many qubits that is needed for implementation of commercially competitive quantum computing is far from the level of the modern technology.

In this note, I will argue that the ability to use non-orthogonal states for computation should be considered as the completely independent resource that is provided by quantum mechanics. With a specific example, I will show that there are computational problems for which the access to just one high quality qubit may provide speed of computation that, fundamentally, cannot be reached by a classical computer under the specified restrictions on raw resources such as memory coupling strength to control fields.

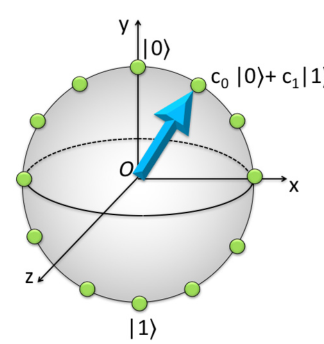

Fig. 1. Up to overall phases that do not influence measurement outcomes, states of a qubit correspond to points on the 2D sphere. This phase space can be discretized to create a register of states (green circles) for computation. However, only opposite points on this sphere, such as the poles marked by $|0\rangle$ and $|1\rangle$, are distinguishable by measurements.

The idea of this article is based on the well known observation that time-energy uncertainty relation in quantum mechanics imposes limits on computation speed at fixed power supply for classical schemes of computer operation [3,4]. Such claims are generally justified by the fact that digital computers save information in the form of clearly distinguishable states, such as 0 and 1 that encode one bit of information. Quantum mechanically, distinguishable states must be represented by orthogonal vectors that produce definitely different measurement outcomes. However, the switch-

E-mail address: nsinitsyn@lanl.gov.

https://doi.org/10.1016/j.physleta.2017.12.042
0375-9601/© 2017 Published by Elsevier B.V.

ing time between two orthogonal quantum states is restricted from below by a fundamental computation speed limit $T = h/(4\Delta E)$, where ΔE is characteristic energy of the control field coupling to the memory that is needed to update one bit of information [5]. So, restrictions on strength of control fields automatically restrict the speed of classical computation that saves information in physically distinguishable states. While the existence of this *computation quantum speed limit* is a mathematically proved fact, I will show an explicit elementary example that demonstrates possibility of solving a computational problem faster than the lowest time bound that is imposed by this limit on classical computation hardware. Access to the quantum memory makes this possible because information can then be processed using nonorthogonal quantum states. So, there is no more direct linear relation between the minimal time and the number of elementary logic operations required to implement an algorithm at given energy constraints.

The remainder of the Hamming weight. If there is only a single available qubit for computation, there is no possibility to discuss quantum correlations. However, one can still perform switches between state vectors of this qubit that are arbitrarily close to each other in the phase space. At fixed strength of control fields this can be done much faster than switching between orthogonal states. The question is only whether we can effectively read the result of such manipulations in order to solve a legitimate computational problem.

Imagine that our computer receives a long string of zero and unit numbers:

$$1, 1, 0, 0, 1, 0, 1, \ldots, 0, 1, 1, \tag{1}$$

with the total number of $N \gg 1$ characters. The number N_1 of unit characters in such a string is called the Hamming weight. We assume that it is unknown, and computer has the task to answer the question: "which one of the integer numbers, 0 and n, is *not* the remainder of division of N_1 by $2n$?". This is a legitimate computational problem. For example, let $2n = 4$ and $N_1 = 1729 = 432 \cdot 4 + 1$. Since the remainder is 1 then neither 0 nor 2 is the remainder. Hence, if machine returns either 0 or 2 it gives a correct answer in this case. Another example: $N_1 = 8 = 2 \cdot 4 + 0$. The remainder is 0 so the only correct answer that machine must return should be 2.

Let me consider that $N > n > 1$ and estimate the minimal time and hardware resources that are needed to solve this problem classically. Suppose that characters of the string are processed with constant time intervals τ per character, while units are separated by unknown chains of zeros. Each time a unit number arrives, we must update our records. Since only remainder of division by $2n$ matters, we need only $\log_2(2n)$ classical memory bits that should be updated to keep information about the remainder of the division of the already arrived number of units by $2n$. Since classically distinguishable states must be quantum mechanically orthogonal, each flip of a memory bit should be induced by a pulse with field-memory coupling energy $\Delta E \geq h/(4\tau)$. This is the energy cost of counting each unit character classically. Conversely, if our computer has restrictions on the strength of control fields that it can create, the time of processing one character has to be restricted as $\tau \geq h/(4\Delta E)$, so the total time of computation is fundamentally restricted as

$$T \geq Nh/(4\Delta E). \tag{2}$$

Quantum mechanically, the same computational problem can be solved with only a single qubit. Indeed, let us assume that this qubit is a spin-1/2, which points up along y-axis initially, i.e., it is in the state $|0\rangle$ in Fig. 1. Each time a unit character arrives, it triggers a magnetic field pulse, along the z-axis, that rotates the spin counterclockwise by an angle π/n in the xOy plane. Remainders $\{0, 1, 2, \ldots 2n-1\}$ are then encoded in spin rotation angles, respectively, $\{0, \pi/n, 2\pi/n, \ldots (2n-1)\pi/n\}$. Note that we identify rotation angles that are different by multiples of 2π because they represent the same spin state vector.

After the full string of characters passes through such a computation, we perform measurement by a projection operator on the state with zero rotation angle:

$$\hat{X} = |0\rangle\langle 0|.$$

Although the spin states that encode possible remainders are generally not orthogonal, particular states that represent remainders of interest, 0 and n, are represented by quantum mechanically orthogonal states with spin rotation angles, respectively, 0 and π. Suppose the outcome of measurement is $X = 1$. This outcome is possible for all possible spin rotation angles except π. So, receiving $X = 1$ we will conclude that the number n is definitely not the remainder of division of N_1 by $2n$. In the alternative case when the measurement outcome is $X = 0$, we will conclude that 0 is definitely not the remainder of division of N_1 by $2n$. So, our task will be fulfilled.

Let me now examine energetics of this computation. At each elementary step spin rotates by an angle π/n, which is n times smaller than what is needed to switch between orthogonal spin states. Repeating standard arguments, e.g. from Ref. [6,5], I find that such an elementary operation requires coupling energy that is limited by $\Delta E = h/(4n\tau)$, i.e., n times less than what is needed for switching between orthogonal states. For spin-1/2, this limit is reachable because it is achieved by a square pulse of a constant magnetic field along the z-axis. Consequently, by using the quantum memory we reduce the coupling between the field and the memory in our processor by the factor n or, equivalently, speedup calculations n times at fixed strength of this coupling.

The most time and energy consuming step is the final measurement. It is done only once and therefore does not influence scaling of the performance of the algorithm with N. Moreover, any other computation scheme would require at least one such a measurement to obtain the result. So, this step does not reduce the performance in comparison to classical schemes.

Finally, let me compare the qubit to a classical rotator in the same computation scheme, i.e., assuming the same discretization of the spherical phase space and the same switching protocols. A classical rotator is physically realized by a magnetic grain with a large effective spin $S \gg 1$. Although our algorithm requires discretization of the spin phase space into $2n$ different rotation angles, we do not assume that we have to make records of transient states during computation. We can even assume that $n > S$, so motion in the continuous classical spin phase space does not lead to infinite energy requirement.

Coupling of the classical spin to the magnetic field is described by the Hamiltonian $\hat{H} = \mathbf{B} \cdot \mathbf{S}$. Characteristic energy of this coupling is $\Delta E = |B|S$. The spin rotation frequency, $|B|/\hbar$, is independent of S, while $\Delta E \propto S$. The classical spin switches between rotation angles $2S$ times slower at the same characteristic coupling ΔE than a qubit with spin 1/2. Thus, replacing a qubit with a classical spin, while keeping the same scheme of computation, slows the computation speed at fixed ΔE down.

Gambling example. The considered computational problem may look quite artificial at first view. However, the access to one qubit computer that implements the above algorithm can actually give an advantage in realistic gambling games. Imagine the virtual online game with a roulette that has $2n$ discrete states, as in Fig. 2. Stakes are received only on two states: 0 and n. The pointer is initially set at zero and then rotates. If it ends on one of the numbers 0 or n then players who bet on that number *loose* everything. In

Please cite this article in press as: N.A. Sinitsyn, Computing with a single qubit faster than the computation quantum speed limit, Phys. Lett. A (2018), https://doi.org/10.1016/j.physleta.2017.12.042