ЖЭТФ, 2003, том 123, вып. 2, стр. 384–398

QUANTUM RECOGNITION OF EIGENVALUES, STRUCTURE OF DEVICES, AND THERMODYNAMIC PROPERTIES

Yu. I. Ozhigov *

Institute of Physics and Technology, Russian Academy of Sciences
117218, Moscow, Russia

Submitted 1 April 2002

Quantum algorithms speeding up the classical counterparts are proposed for the following problems: recognition of eigenvalues with a fixed precision, recognition of molecular and electronic device structures, and finding thermodynamic functions. We mainly consider structures generating sparse spectra. These algorithms require the time from about the square root to the logarithm of the time of the classical analogues and give exponential memory saving for the first three problems. For example, the time required for distinguishing two devices with the same given spectrum is about the seventh root of the time of the direct classical method, and about the sixth root for the recognition of an eigenvalue. Microscopic quantum devices can therefore recognize molecular structures and physical properties of environment faster than big classical computers.

PACS: 03.67.Lx

1. ELECTRONIC DEVICES AND QUANTUM COMPUTATIONS

1.1. Statement of the problem and outline of the work

The aim of this paper is to build effective quantum algorithms for problems of the following types:

1. given a quantum gate array generating a unitary operator U and a complex number ω, to determine whether it is an eigenvalue of U with a fixed precision,

2. to recognize the structure of an unknown electronic or molecular device given only access to its function.

The first problem is an important intermediate step in solving the second[1)]. We consider them sequentially.

Recognition of eigenvalues. This problem is closely related to finding the eigenvalue distribution or density of states (DOS), i.e., the energy levels $E_0 < E_1 < \dots$ and the dimensions of the corresponding subspaces $d_0, d_1, \dots$ The DOS plays a key role in calculating thermodynamic functions given by

$$F = \sum_j a(j) d_j \exp\left(-\frac{E_j}{k_B T}\right) \qquad (1)$$

for some values $a(j)$ such that the summands rapidly converge to zero. For example, this expression gives the partition function Q if all $a(j) = 1$, the average energy if

$$a(j) = E_j/Q$$

and the entropy if

$$a(j) = -\frac{k_B}{Q} \ln\left(\exp\left(-\frac{E_j}{k_B T}\right)/Q\right).$$

Having an efficient method of finding d_j, we would be able to obtain thermodynamic functions and to determine important properties (e.g., heat capacity) of environment consisting of such molecules. The best known classical method of finding the DOS was proposed by Hams and Raedt in [1]. Their method requires the time of the order given by the dimension N of the space of states and the memory of the same order (whereas the direct method of calculating eigenvalues requires the time of the order N^3). The first quantum algorithm for this problem proposed by Abrams and

*E-mail: ozhigov@ftian.oivta.ru

1) A straightforward calculation shows that the simulation of evolution generated by a given Hamiltonian up to a time instant τ with a fixed accuracy requires the number of steps of the order τ^2 on a quantum computer. This means that all results of this paper can be generalized to arbitrary quantum systems.

Lloyd in [2] requires the same $O(N)$ time and logarithmic memory. The method proposed in the present work requires the time of the order given by the square root of the classical one and memory of the order $\ln^2 N$.

The idea of our approach is as follows. We use a combination of the Grover search algorithm (GSA), the Abrams and Lloyd method [2] of revealing eigenvalues, and the universal quantum function of application App. The Abrams and Lloyd method of revealing eigenvalues is based on the application of U controlled by ancillary qubit α as

$$U_{cond}|x,\alpha\rangle \longrightarrow \begin{cases} |U\ x,\alpha\rangle & \text{if } \alpha = 1, \\ |x,\alpha\rangle & \text{if } \alpha = 0. \end{cases}$$

We note that it is a direct generalization of Shor's trick, which can be obtained if U is a multiplication by a given integer modulo q [3].

Recognition of device structures. We separate two versions of this general problem: recognition of molecular structures and recognition of electronic circuits.

If we want to determine a molecular structure, it is natural to assume that its functionality is given as the spectrum of its Hamiltonian, e.g., the set of its energy levels. It is therefore required to find a quantum system whose Hamiltonian has a given spectrum.

The problem of recognition of electronic circuits is stated differently. An electronic device is considered as a source of electromagnetic fields that can control some quantum system Q. Let such a field induce evolution of the system with the Hamiltonian H in the time frame δt. We then have the correspondence

$$\text{(electronic device)} \longrightarrow \text{(Hamiltonian, } \delta t\text{)}.$$

The evolution of the quantum system Q induced by this Hamiltonian can be represented as a unitary transformation

$$U = \exp\left(-\frac{i}{h} H \delta t\right).$$

Given a device C and a time instant t, we can then associate some unitary transformation U_C with it. We assume that we have recognized a circuit C if we have found some circuit C_1 such that $U_C = U_{C_1}$ with high accuracy. We write U instead of U_C for the circuit C that we want to recognize. In fact, we solve a more general problem where the tested device C can be used as a black box acting on n qubits as a function U_C such that if x is an input, then $U_C|x\rangle$ is the result of its action on this input. The tested device can contain its own quantum memory and can be entangled with Q in the course of performing the transformation U, but this entanglement must then be eliminated. The existence of such an entanglement implies that this case cannot be described by the Hamiltonian of the system Q. For simplicity, we assume that the unknown circuit is built from elementary functional elements taken from some fixed set. The next natural assumption is that the size of the circuit is limited by some constant c such that the circuit is some unknown combination of c functional elements. We let $\mathcal{E}$ denote all circuits of the length c. We can encode such $C \in \mathcal{E}$ by a string $[C]$ of ones and zeroes such that the decoding procedure is easy and we can immediately recreate a circuit given its code. We can therefore look through all circuits by looking through their codes. The same coding can be built for electronic devices.

A straightforward solution of the problems is clear. For the problem of recognition of molecular structures all that we need is to be able to recognize eigenvalues of the transformation generated by a given circuit. Each eigenvalue of a unitary operator has the form $e^{2\pi i\omega}$, where ω is a real number from $[0,1)$ called the frequency. In what follows, the spectrum is meant to be the set of all frequencies. Let all the frequencies be grouped near points of the form l/M, where M is not very large and $l = 0,1,\ldots,M-1$. We assume that the acceptable precision of the recognition of frequencies is $1/M$. Having an algorithm for the eigenvalue recognition, we can apply it repeatedly, constructing spectra generated by all possible circuits, and thus find the sought circuit with the given spectrum. If we need to recognize a circuit of an electronic device, we can examine all possible circuits taken in some order. Examination of one circuit means that we run it on all possible inputs one after another and compare the results with the corresponding result of the tested device action.

For the problem of the recognition of molecular structures, our method requires the time of the order sixth root of the time of the direct classical method, whereas memory saving is exponential. For the problem of the recognition of electronic circuits, our method gives at least square-root time saving in the case where the classical counterparts exist (this is the narrow formulation where the tested device generates a classical mapping). But the advantage can be greater in the general case. For example, we can distinguish between two devices with the same spectrum in the time about the seventh root of the time of the brute force method.

To recognize devices at the quantum level, we must be able to store and perform operations on codes of different circuits. This possibility is based on the existence of a quantum analogue of the universal Klini

function. This is a unitary operator App such that for all quantum devices C and all inputs x,

$$\mathrm{App}|x,[C]\rangle = |U_C\ x,[C]\rangle.$$

We assume that for a wide range of quantum devices C with c particles, C can be encoded as an integer $[C]$ in time $O(c)$ such that the quantum complexity of App is also $O(c)$.

We here consider a particular case of the problem where all eigenvalues of U are known a priori or can be obtained in advance. This restriction is not very constraining. To illustrate the tasks that can be solved by the proposed method, we consider several examples of the problem of recognition of an electronic device whose spectrum is known.

Recognition of quantum algorithms is designed as subroutines. Such an algorithm must restore the input if we apply it twice. Computing a function f, it acts as

$$|x,b\rangle \longrightarrow |x,b+f(x) \mod 2\rangle.$$

All known quantum algorithms can be represented in this form. For such quantum algorithms, the unitary transformation U has only two eigenvalues, 1 and -1. Given a controlling device for such an algorithm (which can also include classical elements and ancillary qubits), we can quickly recognize its construction. Alternatively, we can quickly find a quantum or classical algorithm for a given task.

We consider the «classical» particular case of the recognition problem where U maps each basic state to a basic state, which means that the matrix of U consists of ones and zeroes and in addition U equals U^{-1}. Here, the evident recognition strategy takes the number of steps of the order $\mathrm{card}(\mathcal{E})$. In this case, the problem can be reformulated as finding such t that some given predicate $A(t,s)$ is true for all s. This is the problem of verification of logical formulas. Its quantum solution in a time about the square root of the classical time based plainly on Grover's trick was proposed in [4]. This method is inapplicable in the general case where U_C is an arbitrary involutive unitary transformation, e.g., such that $U = U^{-1}$. This general case is precisely the subject of this work. Here, we cannot recognize a circuit so easily as in the «classical» case because it is difficult to compare two quantum states $U_C|x\rangle$ and $U|x\rangle$.

The general idea of our approach to the recognition of arbitrary electronic devices is as follows. We include the device C whose structure we want to recognize into the classical controlling part of a quantum computer. We consider the main system of n qubits. The tested device then generates a unitary transformation on this system. We then find the eigenvectors of U using U_{cond} by the above method and compare them with the eigenvectors of circuits from $\mathcal{E}$ choosing a circuit that gives the best approximation. Here, GSA is used at the last step and at the several intermediate steps.

The sparse spectrum assumption. In this paper, we mainly consider circuits generating sparse spectra. This means that the spectra of the operators U_C are designed such that the frequencies are assembled in groups and the minimum distance between frequencies from the different groups is greater than $1/M$ and the maximum distance between frequencies in the same group is less than $1/L$. In the problems of eigenvalue and molecular structure recognition, we require that $L = 16M$, which is not very restricting. In the problem of recognition of electronic devices, we assume that $L \gg M$, which is a stronger limitation. A spectrum is called sparse if $M = \mathrm{const}$ as $N \longrightarrow \infty$. Our algorithms show the best performance for sparse spectra.

Spectra that are not sparse are called dense. For dense spectra, our methods give less advantage over the classical algorithms (see Sec. 3.6). An example of a dense spectrum is given by $\omega_k = k/N$, $k = 0,1,\ldots,N-1$. Similar problems for dense spectra require additional investigations.

We write $\omega' \approx \omega$ iff ω' and ω belong to the same group. For simplicity, we also assume that for each group of frequencies, there exists a number of the form l/M positioned between some two frequencies of this group, where l is an integer less than M.

1.2. Abstract model of quantum computer. «Plug and play» technology

To build algorithms recognizing circuits, we need an abstract model of the quantum computer. A quantum computer consists of two parts, quantum and classical. The classical part exactly determines what unitary transformation must be performed on the quantum part at each time instant and therefore plays the role of a controller for the quantum part. These unitary transformations are of two types: working transformations, which our computer performs itself, and query transformations, which are induced by a tested device, U or U_{cond}.

We can suppose that the quantum part Q consists of nuclear spins or interacting dipoles (or some other quantum two-level systems) and the classical part is a source of electromagnetic fields determining the evolu-

tion of the quantum part. The general form of a state of the quantum part is

$$\chi = \sum_{i=0}^{2^\nu - 1} \lambda_i e_i,$$

where the basic states $e_0, \ldots, e_{2^\nu - 1}$ are simply strings of ones and zeroes of the length $\nu > n$; this length is the size of the quantum part that can contain some auxiliary qubits in addition to the input for U, $N = 2^n$ is the number of all classical input words for U, and

$$\sum_{i=0}^{2^\nu - 1} |\lambda_i|^2 = 1.$$

The classical part determines when the tested device is to be «switched on» (this usually occurs many times) and when the result of the computation is to be observed. Observation of a state χ gives every basic state e_i with the corresponding probability $|\lambda_i|^2$.

The problem of recognition of electronic devices presumes the so-called «plug and play» technology where the tested device is applied only as a black box. If query transformations are only U, then our model evidently satisfies the requirements of the «plug and play» technology, where we classically control switching the tested device. An implementation of U_{cond} in the framework of this technology is not so easy because it requires a quantum control on applications of the device[2)].

It is nevertheless possible to implement U_{cond} in the framework of the «plug and play» technology. This problem requires additional investigations; here, we simply presume that it is possible. This difficulty does not exist in the problems of the eigenvalue and molecular structure recognition. Here, we can manage without oracles because having an explicit form of a quantum gate array realizing the universal function of application App, we can control its actions in each element at the quantum level separately and simultaneously, thereby implementing U_{cond}.

Let every basic state be partitioned as

$$e_i = |\text{place for code } [C], R_{\bar{1}}, R_{\bar{2}}, \ldots, R_{\bar{l}}\rangle,$$

where each register $R_{\bar{i}}$ is in turn partitioned into a place for the argument, places for time instants, and places for the corresponding frequencies. A complex index $\bar{i}$ contains one or two integers, and the length of e_i is therefore a polynomial in c and n of at most second degree.

[2)] This would evidently be possible provided we have access to the internal details of our device and can simultaneously control their work at the quantum level. But this assumption contradicts the «plug and play» technology.

2. OBTAINING NEW ALGORITHMS FROM BASIC QUANTUM TRICKS

2.1. GSA and the amplitude amplification

The GSA proposed in [5] is one of the two basic quantum tricks. It is used for quickly obtaining a quantum state $\bar{a}$ given the inversion $I_{\bar{a}}$ along this state. The inversion along some state $\bar{a}$ is defined by

$$I_{\bar{a}}|\bar{x}\rangle = \begin{cases} |\bar{x}\rangle & \text{if } x \perp a, \\ -|\bar{a}\rangle & \text{if } x = a. \end{cases}$$

We also assume that $I_{\bar{a}}$ acts as the identity if $\bar{a}$ does not exist. A typical situation is where a state is unknown but the inversion along it can be performed easily. For example, let $\bar{a}$ be a solution of the equation $f(x) = 1$ with a simply computable Boolean function f. The inversion $I_{\bar{a}}$ can then be implemented by modulo-2 addition of $f(x)$ to an ancillary qubit initialized by

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

This transformation maps the state

$$\left| x, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\rangle$$

to the same state with the sign «+» or «−» depending on whether the equality $f(x) = 1$ is satisfied. The transformation is unitary and can easily be performed given a device performing f. All sequential transformations in our formulas are applied from right to left.

The GSA is a sequential application of the transformation $G = I_{\bar{a}} I_{\tilde{0}}$ to a randomly preset state $\tilde{0}$. If we apply this transformation $O(\sqrt{N})$ times, where N is the dimension of the main space, then an observation of the quantum part yields $\bar{a}$ with a visible probability, whereas finding $\bar{a}$ without a quantum computer would have required the number of steps of the order N.

A minor difficulty is here that we do not exactly know the time instant t at which the iterations must be terminated in order to make the probability of error negligible, as required in applying the GSA as a subroutine. The following simple trick helps here.

We define the number $B = B(N)$ such that $1/B$ is the average value of $|\langle a \mid \tilde{0}\rangle|$ for $\tilde{0}$ uniformly distributed on a sphere of radius 1 in the space of inputs. A straightforward calculation shows that $B = O(\sqrt{N})$. Let GenArg_j be operators generating arbitrary vectors $\bar{a}_j$ from the space of inputs belonging to independent uniform distributions, $j \in \{1, 2, \ldots, k\}$, and let $\mathrm{GenTimeArg}_j$ be operators generating time instants t_j from independent uniform distributions on integers

from the segment $[0, B]$. We arrange k copies of two working registers, for the input and for the storage of a time instant, and apply the corresponding operator

$$(I_{\bar{0}} I_{\bar{a}})^{t_j} \mathrm{GenArg}_j \mathrm{GenTime}_j$$

to each register. If $\bar{a}$ exists, the probability to obtain $\bar{a}$ observing any single register is at least $1/4$ (see [6]) and the probability to obtain any other fixed state is negligible because our operators GenArg_j generate independent uniformly distributed samples. If $\bar{a}$ does not exist, which implies that $I_{\bar{a}}$ is the identity, then the probability to obtain any fixed state is negligible. We let $\bar{a}_j$ denote the contents of the j-th register for the argument in the resulting state. We consider the following criterion: if at least one fifth of $\bar{a}_j$, $j = 1, 2, \ldots, k$, coincide, we decide that $\bar{a}$ is this value, otherwise $\bar{a}$ does not exist. We now calculate the error probability of this criterion. Let K be the number of those j for which $\bar{a}_j = \bar{a}$. By the central limit theorem, the probability that the fraction

$$\frac{(k/4) - K}{\sqrt{(k/4) \cdot (3/4)}}$$

belongs to the segment $[\alpha_1, \alpha_2]$ converges to

$$\frac{1}{\sqrt{2\pi}} \int\limits_{\alpha_1}^{\alpha_2} e^{-x^2/2} dx.$$

Straightforward calculations then show that the probability that $K \le k/5$ is of the order

$$\int\limits_{\alpha_1}^{\infty} e^{-x^2/2} dx$$

for α_1 of the order $\sqrt{k}$. To make the error probability of the order $1/\sqrt{N}$, it therefore suffices to choose k of the order $n = \log N$. This method can be used not only for the GSA but also for other algorithms. If the probability to obtain the correct result for each of the k registers is some positive number p independent of the dimensionality, then to make the error probability $1/N_1$, it suffices to choose k of the order $\log N_1$. In what follows, we use this simple trick without specially mentioning it and let $\bigotimes\limits_j$ denote the simultaneous operations of the same type on all working registers. We assume that all ensembles generated by the different j-th copies of operators are taken from independent distributions.

We use the standard norm

$$\|A\| = \sup_{\|\bar{x}\|=1} \|A\bar{x}\|$$

on operators in a Hilbert space. Given an operator A, we let A_ϵ denote an operator such that $\|A - A_\epsilon\| \le \epsilon$. In what follows, we use the above method requiring copies of registers, thereby raising the accuracy of our operators to the required level. When we must repeat an operator T times, the required accuracy of one application must be $1/T$ and as shown above, it can be ensured by only linear price in memory. Instead of A, we therefore always use A_ϵ, where $\epsilon = O(1/T)$, whenever an operator A must be repeated T times; we do not explicitly indicate this in the notation.

2.2. Revealing the eigenvalues

The second basic quantum trick is used for revealing eigenvalues of a given unitary operator U. We define an operator revealing frequencies in accordance with [2].

Let $M = 2^m$ and $L = 2^p$. We determine frequencies of unitary operators within $1/L$, where L is the number of applications of U required for revealing frequencies with this accuracy, which means that the accuracy $1/M$ is sufficient to distinguish the eigenvalues of U. For the recognition of eigenvalues, we put $p = m + 4$, and therefore, $L = 16M$.

We let $(0.l)_p$ denote the number from $[0, 1)$ of the form l/L. Let the operator U have the eigenvalues $e^{2\pi i \omega_k}$, where the frequencies $\omega_0, \omega_1, \ldots, \omega_{N'-1}$ are different real numbers from $[0, 1)$. Let E_k be the space spanned by all eigenvectors corresponding to ω_k. An arbitrary vector with the length 1 from E_k is denoted by Φ_k. Every state ξ therefore has the form

$$\xi = \sum_{k=0}^{N'-1} x_k \Phi_k.$$

Let N' be some integer and $\Omega = \{\tilde{\omega}_{k,i}\}$ be some set of integers from $\{0, 1, \ldots, L-1\}$, $0 \le i \le M-1$, $0 \le k \le N'-1$; $\varepsilon, \delta > 0$. We set

$$L_\varepsilon^k(\Omega) = \{i : \ |(0.\tilde{\omega}_{k,i})_p - \omega_k| \le \varepsilon$$

or $|(0.\tilde{\omega}_{k,i})_p - \omega_k - 1| \le \varepsilon\}$.

Definition 1. *A transformation W of the form*

$$W : \ |\xi, 0^{m+4}\rangle \longrightarrow \sum_{k=0}^{N'-1} \sum_{i=0}^{L-1} \lambda_{i,k} |\Phi_k, \tilde{\omega}_{k,i}\rangle$$

is called a transformation of type $W_{\delta,\varepsilon}$ if for all k and ξ,

$$\sum_{i \in L_\varepsilon^k(\Omega)} |\lambda_{i,k}|^2 \ge |x_k|^2 (1 - 2\delta).$$

Thus, δ is the error probability of obtaining the correct frequencies ω_k by observation of the second register and ε is the precision of the frequency approximations.

Definition 2. *A unitary operator R is called revealing frequencies of U if R belongs to the type $W_{\frac{1}{K},\frac{K}{L}}$ for any $K \in \{1,2,\ldots,L\}$*[3)].

The key here is the quantum version of the Fourier transform (QFT) defined by

$$\mathrm{QFT}_L: \quad |s\rangle \longrightarrow \frac{1}{\sqrt{L}} \sum_{l=0}^{L-1} \exp\left(-2\pi i s l/L\right) |l\rangle.$$

We also need the following generalization U_{seq} of the operator U_{cond}:

$$U_{seq}^L |x,a\rangle = |U^a x, a\rangle.$$

This is the result of a sequential applications of U to the main register. To implement this operator by means of U_{cond}, we perform the following cycle. For an integer counter j ranging from 1 to the maximum value $L-1$ of a, we apply U iff $j \le a$. One cycle then consists of U_{cond} with a properly prepared controller and the resulting operator is U_{seq}^L.

We define the operator revealing frequencies by

$$\mathrm{Rev} = \mathrm{QFT}_L \mathrm{U}_{seq}^L \ \mathrm{QFT}_L,$$

where quantum Fourier transformations are applied to the second register[4)]. It was proved in [7] that Rev is a transformation revealing frequencies. We now need more. For a redistribution of amplitudes x_k, we also need the transformation Rest cleaning the second register. The ideal candidate for this role would be Rev^{-1}, but it requires the application of U^{-1}, which is physically unrealizable given only the device fulfilling U, except in evident cases where, e.g., $U = U^{-1}$. We can use this simplest definition of Rest only in the case where we are given a circuit implementing U (e.g., gate array) because U^{-1} is then accessible for us as well as U. But if C is given only as a black box, the restoring operator must be defined separately.

We find the operator restoring ancilla in the form

$$\mathrm{Rest} = \mathrm{Rev} D,$$

where D is some operator of turning. Given some integers $\tilde{\omega}_k^L$ of the form q/L, where q is an integer, $\tilde{\omega}_k^L \approx \omega_k$, we can define the operator D of turning by

$$D|\Phi_k, l\rangle = \exp\left(-2\pi i (L-1)\delta_{k,l}\right) |\Phi_k, l\rangle,$$

where

$$\delta_{k,l} = \tilde{\omega}_k^L - (0.l)_m.$$

It was proved in [7] that

$$\|(\mathrm{RestRev}|\chi,\bar{0}\rangle - |\chi,\bar{0}\rangle\| < 7M/L,$$

which implies that the restoring operator thus defined indeed restores zeroes in the second register after the action of Rev if L is sufficiently large. To create these good approximations, we apply a slightly more general construction. We set

$$D = \mathrm{Enh}\ \tilde{D}\ \mathrm{Enh},$$

where the operator Enh calculates an integer function $h(l)$ giving a good approximation $(0.h(l))_p$ of frequencies within $1/L$ given their rough approximation $(0.l)_m$ within $1/M$ and places them into ancilla, $\tilde{D}$ rotates each eigenvector by an appropriate angle

$$\tilde{D}|\Phi_k\rangle = \exp\left[-2\pi i (M-1)((0.h(l))_p - (0.l)_p)\right] |\Phi_k,$$

and the last application of Enh cleans the ancilla. The operator Enh is accessible given good approximations of eigenvalues. Our operator Rest therefore restores zeroes in the ancilla within $1/L$.

We can reach the accuracy $1/L$ for all operators of type Rest that are less than $1/t$, where t is the number of all steps in the computation; this accuracy can be guaranteed with $\log L = p$ registers. We emphasize that this difficulty with the eigenvalue precision arises only when U^{-1} is inaccessible, as in the problem of recognition of electronic circuits in Sec. 3.4, where we must choose $L \gg M$.

The operators Rev and Rest can be built in the form of a quantum gate array using the universal quantum Klini function App, where the code $[C]$ of a circuit generating U is a part of the input. We write the operator U corresponding to these two operators as the superscript.

3. RECOGNITION PROBLEMS

3.1. Obtaining eigenvectors and recognition of eigenvalues

Our assumption about a sparse spectrum is now stated as $L = 16M = \mathrm{const}$. Because Rev reveals frequencies, it belongs to the type $W_{1/16,1/M}$. By definition of $W_{\delta,\varepsilon}$, this implies that Rev gives a state

$$\sum_{k=0}^{N'-1} \sum_{i=0}^{M-1} \lambda_{i,k} |\Phi_k, \tilde{\omega}_{k,i}\rangle,$$

[3)] In what follows, we use this notion only with $K = 16$.

[4)] As in [2], the first QFT can be replaced by the Walsh–Hadamard transform because it is equivalent to the QFT on zero ancilla.

where the seven eighth of the probability is concentrated on the pairs i, k such that $(0.\omega_{i,k})_m$ is close to ω_k. This implies that we can obtain eigenvalues with a high probability by observing the second register; the first register then contains the corresponding eigenvector. This procedure to obtain eigenvectors was proposed in [2, 8]. Its first disadvantage is irreversibility. Observing a state, we lose the complete information about it; we cannot use this state again, which is very important for building nontrivial quantum algorithms. The second disadvantage is that this procedure gives a random eigenvector when it is typically required to obtain the eigenvector corresponding to a given frequency.

We consider a good approximation $\tilde{\omega}^L$ of some frequency ω written as a string of p of its sequential binary digits and let $\mathcal{E}_\omega = \{\Phi_1^\omega, \dots, \Phi_l^\omega\}$ be a basis of the subspace E_ω of eigenvectors corresponding to all frequencies $\omega' \approx \omega$. We now build the operator State_ω that concentrates the bulk of the amplitude on some superposition of the corresponding eigenvectors

$$\sum_{j=1}^{l} \lambda_j \Phi_j^\omega \in E_\omega.$$

For this, we apply the GSA. Let

$$|\bar{a}\rangle = \sum_{j=1}^{l} \mu_j \Phi_j^\omega + \sum_s \nu_s \Phi_s$$

be some randomly chosen vector from the main space with all eigenvectors in the second sum corresponding to frequencies $\omega' \not\approx \omega$. Our target state is the vector

$$E_\omega(\bar{a}) = \sum_{j=1}^{l} \lambda_j \Phi_j^\omega,$$

where

$$\lambda_j = \frac{\mu_j}{\sqrt{\sum\limits_{j=1}^{l} |\mu_j|^2}}.$$

The vector is therefore of length 1 and is directed along the projection of $\bar{a}$ to the subspace E_ω.

Let A be some set of vectors. We let I_A denote the operator that changes the sign of all vectors in A and leaves all vectors orthogonal to A unchanged. Our aim is to obtain the operator I_{E_ω} constrained to the two-dimensional subspace $S(\bar{a}, \omega)$ spanned by the vectors $|\bar{a}\rangle$ and $E_\omega(\bar{a})$.

Let Rev_j and Rest_j be j-th copies of the respective operators Rev and Rest acting on the corresponding places of the j-th register. We let l_j denote the string contained in the place for the frequency of the j-th register and set

$$\tilde{I}_{E_\omega} = \bigotimes_j^v \mathrm{Rest}_j \ \mathrm{Sign}_\omega \ \bigotimes_j^v \mathrm{Rev}_j.$$

It follows that Sign_ω changes the sign if and only if

$$|(0.l_j)_p - (0.\tilde{\omega}^L)_p| \le 1/L$$

for at least a half of all j[5]. Applying the argument at the end of Sec. 2.1, we conclude that the actions of I_{E_ω} and $\tilde{I}_{E_\omega}$ restricted to $S(a, \omega)$ differ by less than $1/2^{O(v)}$; this difference can therefore be made very small with only a linear growth of memory. We thus omit the tilde from our notation.

We define

$$\mathrm{St} = \mathrm{GenArg}^{-1}\mathrm{GenTimeArg}^{-1} \circ \\ \circ (I_{\bar{a}} I_{E_\omega})^t \mathrm{GenTimeArg}\ \mathrm{GenArg},$$

where the respective operators GenArg and GenTimeArg generate the pair $\bar{a}$, $[C]$ and the time instant t, with C being a gate array implementing $I_{\bar{a}}$. Here, the actions of $I_{\bar{a}}$ are implemented by the universal function of application App. The result $\xi = \mathrm{St}|\bar{0}\rangle$ of its action on $\bar{0}$ is then close to $E_\omega(\bar{a})$. Indeed,

$$|\langle E_\omega(\bar{a})|\xi\rangle| = |\sin(2t \arcsin\langle \bar{a}|E_\omega(\bar{a})\rangle)|$$

(see [6]). The average value of $|\langle \bar{a}|E_\omega(\bar{a})\rangle|$ with the uniformly distributed probability of choosing $\bar{a}$ and t over all space and the time frame $[0, B]$ correspondingly is of the order $1/\sqrt{N}$. Therefore, if t is randomly chosen from the uniform distribution over $1, 2, \dots, B$, then the average value of $|\langle E_\omega(\bar{a})|\xi\rangle|^2$ is not less than $1/4$. Of course, it would be much more convenient to obtain $E_\omega(\bar{a})$ with the error probability converging to zero, which is possible by the method described in Sec. 2.1. Namely, we arrange h equal registers for the states χ_k, $k = 1, 2, \dots, h$, in the main space, the corresponding h registers for the frequencies, and associate the variable t_k with each k-th register. Let St_k be a pattern of the operator St acting on the k-th register. We recall that the operators GenArg_k and $\mathrm{GenTimeArg}_k$ generate independent distributions for different $k = 1, 2, \dots, h$. We now define

$$\mathrm{State}^\omega = \mathrm{St}_1 \bigotimes \mathrm{St}_2 \bigotimes \dots \bigotimes \mathrm{St}_h. \qquad (2)$$

[5] We could choose any fixed ρ: $1/8 < \rho < 7/8$ instead of $1/2$. Indeed, $\tilde{I}_{E_\omega}$ thus defined would change the sign of all $\bar{a} \in E_\omega$. If $\bar{a} \perp E_\omega$, the probability to obtain ω in observing the frequency from Rev is less than $1/8$.

Applied to zero initial state, this operator gives a state $\chi_1 \bigotimes \chi_2 \bigotimes \ldots \bigotimes \chi_h$, and the average value of $|\langle E_\omega(\chi_k)|\chi_k\rangle|^2$ is close to some number not less than $1/4$ with the vanishing probability of error. This also implies that if we then apply the corresponding operators $\mathrm{Rev}_1 \bigotimes \mathrm{Rev}_2 \bigotimes \ldots \bigotimes \mathrm{Rev}_h$ revealing frequencies to this state, the main part of the amplitude of the resulting state χ is concentrated on the basic states for which at least $5/32$ of all registers for the frequencies contain numbers l such that[6)]

$$|(0.l)_m - (0.\tilde{\omega}^L)_p| < 1/L.$$

On the other hand, if ω is not a frequency, the probability to obtain such a basic state vanishes because the distributions generated by $\mathrm{GenTimeArg}_k$ and GenArg_k are independent for different k.

The time complexity of this algorithm is of the order $M\sqrt{N}n^2$. The last factor arises because of copying the registers. We therefore have a solution of the first problem of the recognition of eigenvalues.

3.2. Finding thermodynamic functions

Given the structure of the molecule of a gas, we consider the problem of finding its thermodynamic function (1). Because the common term in this sum rapidly converges to zero, it is sufficient to find the first several summands. It is therefore sufficient to find the degree of degeneracy of the subspace corresponding to the frequencies $\omega' \approx \omega$ for any $\omega = l/M$. Let $E_0 < E_1 < \ldots < E_s$ be energy levels of the molecule (the eigenvalues of its Hamiltonian H).

The evolution operator in time frame t is then given by

$$U = \exp\left(-\frac{iH}{h}t\right).$$

Adding the diagonal matrix rI with a constant r to the Hamiltonian does not change the physical picture. Choosing

$$r = -E_s, \quad t = \frac{h}{2\pi E_s},$$

we then obtain a unitary operator U whose frequencies belong to the segment $[0, 1)$. Thus, the problem is reduced to the case considered above.

We assume that M is fixed and we must examine only several frequencies close to 0. We can first recognize all numbers of the form l/M that are frequencies within $1/L$. Let ω be such a number. We now show how to find the degeneracy degree d of the corresponding subspace. This is the dimension of the subspace E_ω spanned by the eigenvectors corresponding to frequencies $\omega' \approx \omega$. Our strategy is as follows. We build the operator I_{E_ω} of reflection along this subspace. Using a counting procedure built in [6], we then evaluate the time required for turning an arbitrary initial vector to this subspace. This time is about $\sqrt{N/d}$ and we thus find d. We fix some $\epsilon > 0$ and show how to obtain the value of d within ϵd.

Let the operators $\mathrm{GenTimeArg}_j^a$ generate time instants t_j from independent uniform distributions on the segment $[0, [a]]$, where a is a nonnegative number. For a from 1 to $\sqrt{N}$, we perform the following three-step loop:

1) apply the operator

$$\bigotimes_j \left[\bigotimes_k \mathrm{Rev}_{j,k}\right] (I_{\bar{a}} I_{E_\omega})^{t_j} \mathrm{GenTimeArg}_j^a \mathrm{GenArg}_j;$$

2) find the fidelity of the result, i.e., the number of all j for which at least $7/8 - \epsilon$ of all k are such that $\omega_{j,k} \approx \omega$; if the fidelity of this step is larger than at the previous step, we proceed the loop, otherwise we stop;

3) replace a with $4a/3$.

If we finish the computation at step 2, the current value of a is taken as a rough approximation of d from above. We have $3a/4 \le d \le a$. To find d more exactly, we divide the segment $[3a/4, a]$ into $[1/\epsilon]$ equal parts by points $a_0 < a_1 < \ldots < a_l$ and repeat the above procedure sequentially for all a_i. We thus determine d within $g(\epsilon)d$, where g is a function rapidly converging to zero with ϵ. Thus, our algorithm finds d and thermodynamic functions with an arbitrary relative error in the time $O(\sqrt{N})M$, where the constant depends on the admissible error. A more refined algorithm can be obtained if we apply the method of counting in [9]. In that work, the quantum Fourier transform is used analogously to the Abrams and Lloyd operator Rev only in order to find the time period of the function $G|\xi, t\rangle = |G^t\xi, t\rangle$, which is about $\sqrt{N/d}$. Their method gives the accuracy of the order $\sqrt{d}$, which implies that the relative error converges to zero as $d \longrightarrow \infty$.

3.3. Recognition of molecular structures

We now consider the problem of recognition of molecular structures. Given the spectrum of a molecule, we must recognize its construction. We have no access to the device, but it is sufficient to find an arbitrary device generating this spectrum. To clarify the formulation, we assume the following form of determining the spectrum. Given a set $\bar{w} = \{w_1, \ldots, w_Q\}$

[6)] We note that in this criterion, $5/32$ could be replaced by any ρ such that $0 < \rho < 1/4 \cdot 7/8 = 7/32$.

of numbers from $[0,1)$ of the form $w_i = l_i/M$ with $l_i \in \{0,1,\ldots,M-1\}$, we let F denote the subspace spanned by vectors of the form $|l_i\rangle$, $i = 1,\ldots,Q$. A spectrum S is determined by this set $\bar{w}$ if

a) for each $\omega \in S$, there exists its good approximation $w_i \in \bar{w}$, $|w_i - \omega| \le 1/L$, and

b) each $w_i \in \bar{w}$ is a good approximation of some $\omega \in S$.

We would obtain a slightly different formulation of the problem if we wished to find a circuit whose spectrum only contains one given set of frequencies and/or does not contain other sets, or if we permit some more general form of a sparse set for $\bar{w}$ instead of l_i/M. These versions of the problem have similar solutions.

As above, we find the recognizing algorithm in the GSA form

$$(I_{\tilde{0}} I_{cir,\ \bar{w}})^t, \tag{3}$$

where $\tilde{0}$ is an arbitrarily chosen vector from the space spanned by codes of the circuits, $t = O(\sqrt{T})$, where T is the number of all possible circuits, and $I_{cir,\bar{w}}$ is the reflection along all codes $[C]$ such that $\mathrm{Spectr}(U_C)$ is determined by $\bar{w}$. It now suffices to build $I_{cir,\ \bar{w}}$.

We choose $B_f = O(\sqrt{Q})$ such that a randomly chosen vector $w \in F$ satisfies

$$|\langle w|w_1\rangle| > 1/B_f$$

with probability 0.99. Let $\mathrm{GenFreq}_j$ and $\mathrm{GenTimeFreq}_j$ be the respective operators generating a linear combination of frequencies $\tilde{\omega}_j \in F$ and a time instant $t_{freq,\ j} \le B_f$; all these objects are taken from the corresponding uniform distributions over all possible values and the code of the gate array generating the inversion along the corresponding state $\tilde{\omega}_j$. These operators generate objects in the corresponding ancillary registers. We let ω_j be the frequency contained in the j-th register (initially, $\tilde{\omega}_j$).

We assume that the code of the circuit generating U is fixed and define the operator $I_{cir,\ \bar{w}}$ by

$$I_{cir,\ \bar{w}} = \bigotimes_j \left[\mathrm{GenFreq}_j^{-1}\mathrm{GenTimeFreq}_j^{-1} \circ \right.$$
$$\left. \circ\, (I_{\mathrm{BadFreq},\ \bar{w},j} I_{\tilde{\omega}_j})^{t_{freq,\ j}}\right] \mathrm{SignGoodFreq}$$
$$\bigotimes_j \left[(I_{\tilde{\omega}_j} I_{\mathrm{BadFreq},\ \bar{w},j})^{t_{freq,\ j}} \mathrm{GenFreq}_j \mathrm{GenTimeFreq}_j\right],$$

where $I_{\mathrm{BadFreq},\ \bar{w},j}$ inverts the sign of states with «bad frequencies» in the j-th register; these are the values of ω_j of the form l/M, $l \in \{0,1,\ldots,M-1\}$ that either belong to $\bar{w}$ and are not a good approximation of frequencies $\omega \in \mathrm{Spectr}(V)$ or do not belong to $\bar{w}$ but have a close frequency

$$\omega \in \mathrm{Spectr}(V): \quad |\omega_j - \omega| \le \frac{1}{L};$$

on all other frequencies, this operator acts as identity. Application of the sequence preceding SignGoodFreq concentrates the amplitude on bad frequencies. We note that $I_{\tilde{\omega}_j}$ can be implemented by a given code by means of the quantum Klini operator App. The subsequent application of SignGoodFreq inverts the sign of a state depending on whether bad frequencies are present. Namely, SignGoodFreq changes the sign for codes $[C]$ without bad frequencies and does nothing for codes $[C]$ with bad frequencies. The subsequent operators clean all ancilla. Therefore, $I_{cir,\ \bar{w}}$ defined this way inverts the sign of exactly those codes C for which $\mathrm{Spectr}(U_C)$ is determined by $\bar{w}$. We need to define two types of operators: SignGoodFreq and $I_{\mathrm{BadFreq},\ \bar{w},j}$.

With each ω_j contained in the j-th register, we associate a family of registers enumerated by two indices j,k and containing the frequencies $\omega_{j,k}$.

Definition 3. *A family of all $\omega_{j,k}$ is called good if the following property is satisfied for at least $1/5$ from all j: for at least $1/10$ of all k, $\omega_{j,k} \approx \omega_j \in \bar{w}$.*

The registers enumerated by different k for a fixed j are designed for the application of the j-th copy of the operator State^{ω} defined in the previous section. Here, it is given by $\mathrm{State}^{\omega_j}$. Each k corresponds to the operator St_k in definition (2) such that each $\omega_{j,k}$ is the frequency obtained from the result of the action of St_k.

We first build the operator $I_{\mathrm{BadFreq},\bar{w},j}$. We set

$$I_{\mathrm{BadFreq},\bar{w},j} = \bigotimes_{j,k} \left[(\mathrm{State}^{\omega_j})^{-1}\mathrm{Rest}_{j,k}\right] \circ$$
$$\circ\, \mathrm{Sign}' \bigotimes_{j,k} \left[\mathrm{Rev}_{j,k}\mathrm{State}^{\omega_j}\right],$$

where the operator Sign' changes the sign of only states with bad families of frequencies.

It was shown in the previous section that if a frequency ω_j is bad, we can only have $\omega_{j,k} \approx \omega_j \in \bar{w}$ for the vanishing part of all k, and before Sign', almost all probability is concentrated on bad families $\omega_{j,k}$; therefore, $I_{\mathrm{BadFreq},\bar{w},j}$ changes the sign.

If ω_j is good, then it belongs to $\bar{w}$ and has a close $\omega' \in S$. It follows from the previous section that about $7/8 \cdot 1/4 = 7/32 > 1/5$ of all k satisfy $\omega_{j,k} \approx \omega \in \bar{w}$ and almost all probability before Sign' is concentrated on good families, and the sign is therefore unchanged.

Hence, $I_{\mathrm{BadFreq},\bar{w},j}$ is defined correctly.

We set

$$\mathrm{SignGoodFreq} = \bigotimes_{j,k} \left[(\mathrm{State}^{\omega_j})^{-1} \mathrm{Rest}_{j,k} \right] \circ \\ \circ \mathrm{Sign} \bigotimes_{j,k} [\mathrm{Rev}_{j,k} \mathrm{State}^{\omega_j}],$$

where the operator Sign changes the sign of only states with good families of frequencies. If a frequency ω_j is not bad, then about $7/8 \cdot 1/4 = 7/32$ of all k satisfy $\omega_{j,k} \approx \omega_j \in \bar{w}$. If a frequency ω_j is bad, we can only obtain $\omega_{j,k} \approx \omega_j \in \bar{w}$ for the vanishing part of k, as shown in the previous section. Thus, SignGoodFreq acts as required[7].

We now calculate the complexity of our algorithm of recognizing a molecular circuit. The first factor $\sqrt{T}$ immediately follows from (3). The next factor $\sqrt{Q}$ follows from the definition of $I_{cir,\ \bar{w}}$. Finally, the definition of $I_{\mathrm{BadFreq},\ \bar{w}}$ gives the factor $M\sqrt{N}$. The resulting complexity is of the order $M\sqrt{TNQ}n^2$.

3.4. Distinguishing eigenvectors of two operators with the same eigenvalue

We now consider the most difficult of our problems, the problem of recognition of electronic devices. The difficulty is that we are not to find a circuit with a given spectrum, but must simulate the action of a given circuit. We recall that we now assume that frequencies can be determined within $1/L$ given their approximation within $1/M$, where $L \gg M$.

As a first step, we consider the following problem: given two operators U and V having the same eigenvalue ω, to find the difference between the corresponding eigenvectors. We let L^U_ω and L^V_ω be the subspaces spanned by the eigenvectors of U and V corresponding to all frequencies $\omega' \approx \omega$. (A particular case is where ω is a frequency of U but not of V. Here, $L^V_\omega = \emptyset$ and our algorithm is applicable in this situation.) We omit the index ω from the notation. For $u \in L^U$, $\|u\| = 1$, we set

$$\mu_u = \min\{\sqrt{1 - |\langle u|v\rangle|^2} \mid v \in L^V,\ \|v\| = 1\},$$

which is the sine of the angle between u and the subspace L^V, or the distance between u and this subspace; we define μ_v for $v \in L^V$, $\|v\| = 1$, similarly. We set

$$\mu_U = \max_{u \in U} \mu_u, \quad \mu_V = \max_{v \in V} \mu_v.$$

Then $\mu_U = 0$ implies that $U \subseteq V$. If the dimensions of the spaces L^U and L^V are equal, then $\mu_U = \mu_V$; if they are not equal, e.g., $\dim L^U > \dim L^V$, then $\mu_U = 1$. Let $d = d(N)$ be some function taking values in $(0, 1]$. We call these subspaces d-distinguishable if one of μ_U, μ_V is not less than d, or one of the subspaces is empty and the other is nonempty.

We build a procedure that determines whether these subspaces are the same provided they can be either d-distinguishable or coincident. The smaller values the function $d(N)$ takes, the more accurate our recognition is. Let $L^U \cap L^V = L_0$. Then $L^U = L_0 \bigoplus L'_U$ and $L^V = L_0 \bigoplus L'_V$. We note that if $L'_U \neq \emptyset$, then for all vectors from L'_U of length 1, their distances from L^V are exactly μ_U, and the same is true for L^V if L'_V is not empty. Let L' be the linear subspace spanned by vectors from $L'_V \cup L'_U$, and $\mathrm{Proj}_A B$ be the projection of a subspace B to a subspace A. If $\dim L^U > \dim L^V$, we have the decomposition into a sum of orthogonal subspaces,

$$L^U = L''_U \bigoplus \mathrm{Proj}_{L^U} L^V,$$

where L''_U is the subspace in L^U consisting of vectors orthogonal to L^V. Let L''_V be defined symmetrically. Then either

1. $L^U = L^V$ or
2. $\dim\ L^U = \dim\ L^V$ and $L' \neq \emptyset$, or
3. $\dim\ L^U > \dim\ L^V$ and $L''_U \neq \emptyset$, or
4. $\dim\ L^U < \dim\ L^V$ and $L''_V \neq \emptyset$.

We define the main operator determining the equality of L^U and L^V by

$$\mathrm{Difference} = \mathrm{Differ}^{-1}\ \mathrm{SignDif}\ \mathrm{Differ},$$
$$\mathrm{Differ} = \mathrm{Dif}_{same\ dim} \mathrm{Dif}_{L^U > L^V} \mathrm{Dif}_{L^U < L^V} \circ \\ \circ \mathrm{Dif}^{ort}_{L^U > L^V} \mathrm{Dif}^{ort}_{L^U < L^V}, \qquad (4)$$

where SignDif changes the sign of the main ancilla α_{dif} iff at least one ancilla in the list

$$\bar{\alpha} = \{\alpha_{same\ dim}, \alpha_{L^U > L^V}, \alpha_{L^U < L^V}, \alpha^{ort}_{L^U > L^V}, \alpha^{ort}_{L^U < L^V}\}$$

contains 1, and each operator of the type Dif changes the corresponding ancilla from $\bar{\alpha}$ in the following cases:

1. $\dim\ L^U = \dim L^V$ and $L^U \neq L^V$,
2. $\dim L^U > \dim L^V$ and $\mu_V < \sqrt{2/3}$,
3. $\dim L^U < \dim L^V$ and $\mu_U < \sqrt{2/3}$,
4. $\dim L^U > \dim L^V$ and $\mu_V > \sqrt{1/3}$, or $L^V = \emptyset$, $\dim L^U < \dim L^V$ and $\mu_U > \sqrt{1/3}$, or $L^U = \emptyset$;

these operators do nothing if $L^U = L^V$. In view of the symmetry, it is sufficient to define the Dif operators in the first, second, and fourth cases. We note that the first case, $\dim L^U = \dim L^V$, is the only nondegenerate

[7] Again, we could take arbitrary ρ_1: $0 < \rho_1 < 1$ instead of $1/10$ and ρ_2: $0 < \rho_2 < 7/32$ instead of $1/5$ in the definition of a good family.

case and the corresponding definition of Dif is more difficult.

Definition of $\mathrm{Dif}_{\text{same dim}}$. We suppose that $\dim L^U = \dim L^V$. Our first aim is to build an operator Inv that acts as the identity if L^U and L^V are coincident and acts as $I_{L'}$ if they are d-distinguishable. We arrange the first two ancillary qubits α_U and α_V that signal whether a given state has the projection to L^U or correspondingly to L^V of the length at least $1/3$. We consider the operator

$$\mathrm{Check} = \bigotimes_s \mathrm{Rest}_s^V \mathrm{Anc}_V \bigotimes_s \mathrm{Rev}_s^V \bigotimes_s \mathrm{Rest}_s^U \mathrm{Anc}_U \bigotimes_s \mathrm{Rev}_s^U,$$

where Anc inverts the corresponding ancilla if and only if at least $9/10$ of copies for the respective frequencies are equal to ω within $1/M$. It coincides with the inverse operator Check^{-1}.

Let t be some random integer from the segment $[0, [2/d]]$. We define the operator

$$\mathrm{Turn}_t = (I_{L^U} I_{L^V})^t \tag{5}$$

of Grover's type. Two subspaces L^U and L^V are said to be almost orthogonal iff $\sqrt{1-\mu^2} \le 1/30$ for some $\mu \in \{\mu_U, \mu_V\}$. If L^U and L^V are not almost orthogonal, then given some $a \in L'_U$ ($a \in L'_V$), the average distance between $\mathrm{Turn}_t|a\rangle$ and L_U (L_V) is at least $1/2$ if L^U and L^V are d-distinguishable and zero if these subspaces are coincident. To distinguish the close location and almost orthogonality cases, we build two operators, Dist_{ort} and Dist_{closed}.

We first suppose that L^U and L^V are almost orthogonal. Then $\alpha_U = 1$ implies that $\alpha_V = 0$. We introduce the notation

$$L(\alpha_U, \alpha_V) = \begin{cases} L^V & \text{if } \alpha_U = 1, \\ L^U & \text{if } \alpha_V = 1. \end{cases}$$

Let $\bar{a}$ be a vector from the space of inputs. We note that $L^U \ne L^V$ implies $\alpha_U = \alpha_V$ for each $\bar{a} \perp L'$ because $\bar{a}$ then belongs to the subspace spanned by L_0 and the orthogonal subspace to $L^U \cup L^V$. The first operator Dist_{ort} does nothing if $\alpha_U = \alpha_V$ and changes the sign and the special ancilla α_{ort} if the projection of $\bar{a}$ to $L(\alpha_U, \alpha_V)$ is less than $1/30$.

The second operator Dist_{closed} acts as the identity if $\alpha_U = \alpha_V$ and changes the sign if the following conditions are satisfied simultaneously: $\bar{a} \in L'$, L^U and L^V are distinguishable, and $\alpha_{ort} = 0$.

We set

$$\mathrm{Dist}_{ort} = \bigotimes_j \mathrm{Res}_j \mathrm{Si}_{\ne\omega} \bigotimes_j \mathrm{Re}_j,$$

where Re (Res) denotes

$$\mathrm{Rev}^V(\mathrm{Rest}^V) \quad \text{if} \quad \alpha_U = 1, \quad \alpha_V = 0,$$

$$\mathrm{Rev}^U(\mathrm{Rest}^U) \quad \text{if} \quad \alpha_V = 1, \quad \alpha_U = 0,$$

and the identity if $\alpha_U = \alpha_V$; $\mathrm{Si}_{\ne\omega}$ changes the sign and simultaneously inverts α_{ort} iff at least half the frequencies ω_j are such that $|\omega_j - \omega| > 1/M$ and $\alpha_U \ne \alpha_V$. If we want to clean the second ancilla after the action of Dist_{ort} and keep the sign change, we can use the operator

$$\mathrm{Dist}^-_{ort} = \bigotimes_j \mathrm{Res}_j S_{\ne\omega} \bigotimes_j \mathrm{Re}_j,$$

where S acts as Si but without changing the sign.

The second operator is defined by

$$\mathrm{Dist}_{closed} = D_1^{-1} \dots D_n^{-1} S' D_n D_{n-1} \dots D_1,$$

$$D_j = (\mathrm{GenTimeArg}_j)^{-1} (\mathrm{Turn}^j_{t_j})^{-1} \circ \circ \left[\bigotimes_k \mathrm{Rest}^U_{j,k}\right] \mathrm{Sig}^j_{\ne\omega} \left[\bigotimes_k \mathrm{Rev}^U_{j,k}\right] \mathrm{Turn}^j_{t_j} \mathrm{GenTimeArg}_j,$$

$$j = 1, 2, \dots, n,$$

where the operator $\mathrm{Sig}^j_{\ne\omega}$ changes the corresponding ancilla β_j only in one of the two cases:

1. $\alpha_U = 1$ and at least a half of $\omega_{j,k}$ are such that $|\omega_{j,k} - \omega| \ge 1/M$, or

2. $\alpha_U = 0$, $\alpha_V = 1$ and at least a half of $\omega_{j,k}$ are such that $|\omega_{j,k} - \omega| < 1/M$.

The operator S' changes the sign iff one of α_U, α_V is nonzero and at least $1/20$ of all β_j contain 1.

We consider the action of Dist_{closed} following Check on an input vector $\bar{a}$. We first consider the case where $L^U \ne L^V$, which implies that these subspaces are distinguishable.

If $\bar{a} \perp L^U, L^V$, then $\alpha_U = \alpha_V = 0$ and Dist_{closed} does nothing.

If $\bar{a} \in L_0$, then $\alpha_U = \alpha_V = 1$ and all $\mathrm{Sig}^j_{\ne\omega}$ does nothing because for almost all j, about $3/4$ of $\omega_{j,k}$ are close to ω, $|\omega_{j,k} - \omega| \le 1/M$, and hence, S' and Dist_{closed} do nothing.

Let $\bar{a} \in L'$. We prove that Dist_{closed} changes the sign. We decompose L' into the sum of orthogonal subspaces, $L' = L'_U \bigoplus {L'_U}^{ort}$, and let $\bar{a}_j$ denote the result of the action of $\mathrm{Turn}^j_{t_j}$ on $\bar{a}$.

If $\alpha \in L'_U$, then $\alpha_U = 1$ and for more than $1/10$ of all $\bar{a}_j$, the revealed frequencies are not close to ω with the probability about $3/4 \cdot 9/10$, and the sign is therefore changed in accordance with case 1).

If $\bar{a} \in L'^{ort}_U$, then by the same reason we obtain the change of sign in accordance with case 2). Hence, Dist_{closed} changes the sign for all $\bar{a} \in L'$.

We can now define Inv as

$$\mathrm{Inv} = \mathrm{Check}\,\mathrm{Dist}^{-}_{ort}\mathrm{Dist}_{closed}\mathrm{Dist}_{ort}\mathrm{Check}.$$

For $a \perp L^U, L^V$, we have $\mathrm{Inv}|a\rangle = |a\rangle$ because Check gives zero in the ancilla α_U, α_V, thereby depriving the subsequent operators of the ability to change the state vector. If $a \in L_0$, then $\mathrm{Inv}|a\rangle = |a\rangle$ because Dist_{ort} does nothing and Dist_{closed} does nothing as well. Thus,

$$\mathrm{Inv}|a\rangle = |a\rangle \quad \text{for} \quad \bar{a} \perp L',$$

and

$$\mathrm{Inv}|a\rangle = -|a\rangle \quad \text{for} \quad a \in L'.$$

We are now ready to build the operator $\mathrm{Dif}_{same\ dim}$ inverting the ancilla $\alpha_{same\ dim}$ iff L^U and L^V are distinguishable. Let Gen generate the list $y, [I_y], [C_Z]$, where $[C_Z]$ is the code of a circuit generating some unitary operator $Z = Z^{-1}$ whose only eigenvalues are 1 and -1 (that is, its frequencies are 0 and 1/2) and the space corresponding to frequency 0 is one-dimensional, and y is a basic vector of this space. As usual, the index j means that the corresponding vectors y_j are taken from the uniform distribution on all possible vectors. We assume that operators of the form Gen^{-1} are also accessible, and set

$$\begin{aligned}&\mathrm{Dif}_{same\ dim} = \\ &= \bigotimes_j \left[\mathrm{GenTimeArg}_j^{-1}\mathrm{Gen}_j^{-1}(\mathrm{Inv}_j\ I_{y_j})^{t_j}\mathrm{Rest}_j^{Z_j}\right] \circ \\ &\circ\mathrm{Change}\bigotimes_j \left[\mathrm{Rev}_j^{Z_j}(I_{y_j}\ \mathrm{Inv}_j)^{t_j}\mathrm{Gen}_j\mathrm{GenTimeArg}_j\right],\end{aligned} \tag{6}$$

where each copy of Inv acts on the register where y_j is placed initially and Change makes the desired change in the resulting qubit $\alpha_{same\ dim}$ if at least 5/32 of all frequencies differ from 0 by more than $1/M$.

The group $(I_{y_j}\ \mathrm{Inv}_j)^{t_j}$ of the GSA type turns the vector y_j generated by Gen_j essentially iff L^U and L^V are d-distinguishable.

If $L^U = L^V$, then y_j remains unchanged and at least 7/8 of all frequencies are close to 0.

If $L^U \neq L^V$, then at least $7/8 \cdot 1/4 = 7/32$ of frequencies for the result of the turn of y_j are far from 0 because they must be close[8)] to 1/2.

[8)] Thus, we could take any number ρ: $1/8 < \rho < 7/32$ instead of 5/32 in the definition of Change.

Definition of $\mathrm{Dif}_{L^U > L^V}$. We suppose that $\dim L^U > \dim L^V$ and $\mu_V < \sqrt{2/3}$, and recall the decomposition

$$L^U = L''_U \bigoplus \mathrm{Proj}_{L^U} L^V$$

into the sum of orthogonal subspaces with $L''_U \neq \emptyset$. We define the operator Dif in much similarity with the previous case,

$$\begin{aligned}&\mathrm{Dif}_{L^U > L^V} = \\ &= \bigotimes_j \left[\mathrm{GenTimeArg}_j^{-1}\mathrm{Gen}_j^{-1}(\mathrm{Inv}''_{j,U}\ I_{y_j})^{t_j}\mathrm{Rest}_j^{Z_j}\right] \circ \\ &\circ\mathrm{Change}\bigotimes_j \left[\mathrm{Rev}_j^{Z_j}(I_{y_j}\ \mathrm{Inv}''_{j,U})^{t_j}\mathrm{Gen}_j\mathrm{GenTimeArg}_j\right],\end{aligned}$$

where the definition of Inv''_U (which inverts L''_U) is similar to the definition of Dist_{ort} with L''_U playing the role of L',

$$\mathrm{Inv}''_U = \mathrm{Check}\left[\bigotimes_k \widetilde{\mathrm{Res}}_k^V\right] \tilde{\mathrm{Si}}_{\neq\omega} \left[\bigotimes_k \widetilde{\mathrm{Re}}_k^V\right] \mathrm{Check}.$$

Here, $\widetilde{\mathrm{Re}}^V$ and $\widetilde{\mathrm{Res}}^V$ act as Rev^V and Rest^V only if $\alpha_U = 1$; if $\alpha_U = 0$, they do nothing, the operator $\tilde{\mathrm{Si}}_{\neq\omega}$ changes the sign in only one case, if $\alpha_U = 1$ and at least 3/4 of all frequencies ω_k are far from ω: $|\omega_k - \omega| \geq 1/M$. In the operator Dif, we therefore use a set of ancillary registers enumerated by the pairs of indices j, k.

For $\bar{a}_j \in \mathrm{Proj}_{L^U} L^V$, in view of the inequality $\mu_V < \sqrt{2/3}$, the operator $\tilde{\mathrm{Si}}_{\neq\omega}$ does not change the sign because the fraction of all frequencies close to ω is then $7/8 \cdot 1/3 = 7/24 > 1/4$.

For $\bar{a}_j \perp \mathrm{Proj}_{L^U} L^V$, the operator Inv''_U does nothing.

Definition of $\mathrm{Dif}^{ort}_{L^U > L^V}$. We suppose that $\dim L^U > \dim L^V$ and $\mu_V > \sqrt{1/3}$. The definition of Dif is similar to the previous case but with the entire subspace L_U playing the role of L',

$$\begin{aligned}&\mathrm{Dif}^{ort}_{L^U > L^V} = \\ &= \bigotimes_j \left[\mathrm{GenTimeArg}_j^{-1}\mathrm{Gen}_j^{-1}(\mathrm{Inv}_{j,U}\ I_{y_j})^{t_j}\mathrm{Rest}_j^{Z_j}\right] \circ \\ &\circ\mathrm{Change}\bigotimes_j \left[\mathrm{Rev}_j^{Z_j}(I_{y_j}\ \mathrm{Inv}_{j,U})^{t_j}\mathrm{Gen}_j\mathrm{GenTimeArg}_j\right],\end{aligned}$$

where

$$\mathrm{Inv}_U = \mathrm{Check}\left[\bigotimes_k \widetilde{\mathrm{Res}}_k^V\right] \tilde{\mathrm{Si}}^{ort}_{\neq\omega} \left[\bigotimes_k \widetilde{\mathrm{Re}}_k^V\right] \mathrm{Check}.$$

Here, $\tilde{\mathrm{Si}}^{ort}_{\neq\omega}$ changes the sign if more than half the frequencies are far from ω; $|\omega_j - \omega| > 1/M$. The conditions required for the operator Dif are satisfied because

$7/8 \cdot 2/3 = 7/12 > 1/2$ and can be checked straightforwardly.

We finally estimate the complexity of the procedure constructed. The operator Turn in (5) requires the number of elementary steps of the order

$$\mathrm{Turn}_{complexity} = M\sqrt{1/d}.$$

The operator Difference in (4) then requires the number of elementary steps of the order $\mathrm{Turn}_{complexity}\sqrt{N}$, that is, $O(M\sqrt{N/d}\,)$. We note that there exists a similar form of the operator Difference that does not act on the resulting qubit α_{dif} but changes the sign instead; such an operator can be constructed similarly. We let it be denoted by $\mathrm{Difference}_{sign}$, and assume that its input contains the frequency ω.

3.5. Recognition of electronic device circuits

We are now ready to consider the recognition of circuits. We assume that for every pair of circuits with the transformations U_1 and U_2, the subspaces spanned by the corresponding eigenvalues are either coincident or d-distinguishable. We also assume that our coding procedure gives a one-to-one correspondence between circuits and the T basic states $e_0, e_1, \ldots, e_{T-1}$ in the space H_{cir}. The recognition procedure is denoted by Rec and has the GSA form,

$$\mathrm{Rec} = (I_{\tilde{0}} I_U)^t, \quad t = O(\sqrt{T}\,). \tag{7}$$

This operator acts on states of the form $|\chi\rangle$, where the basic states for χ are codes of circuits. Here, $\tilde{0} \in H_{cir}$ is chosen arbitrarily and I_U inverts the sign of every code whose circuit induces a given operator U. The implementation of $I_{\tilde{0}}$ is straightforward and all that we need is to build I_U.

We define I_U as

$$I_U = \bigotimes_j \left[\mathrm{Conc}^{-1}_{freq,\ j}\mathrm{Difference}_j\right] \mathrm{Sign} \bigotimes_j [\mathrm{Difference}_j \mathrm{Conc}_{freq,\ j}],$$

where for every basic state C of the argument, Conc_{freq} generates some arbitrary distribution of the amplitude on ancillary registers with Q basic states and then concentrates a substantial part of the amplitude on a frequency ω for which L^U and L^V are distinguishable (if such a frequency exists). The operator $\mathrm{Difference}_j$ then changes the resulting qubit for the jth copy iff these subspaces are distinguishable on this frequency. The next operator Sign changes the sign iff at least one fifth of the resulting qubits α_{dif} contain 1, e.g., iff U and U_C are the same operator. The subsequent applications of $\mathrm{Difference}_j$ to each copy of the register then clean the corresponding resulting qubits and the inverse operators to Conc_j restore the initial state of the ancillary register. Difference was constructed in the previous section and it only remains to build $\mathrm{Conc}_{freq,\ j}$. This transformation can be defined as

$$\mathrm{Conc}_{freq,\ j} = \mathrm{GenTimeFreq}_j^{-1}\ \mathrm{GenFreq}_j^{-1} \circ \circ (\mathrm{Difference}_{sign} I_{\omega_j})^{t_j}\ \mathrm{GenFreq}_j\ \mathrm{GenTimeFreq}_j. \tag{8}$$

If U and U_C are different, then their subspaces L^U and L^V are d-distinguishable for some ω by our assumption, and Conc_j concentrates a substantially large part of the amplitude over all j on some combination of such values ω. Thus, we have constructed the required procedure Rec that gives the target code with a substantial probability as the result of an observation of the register for the code C. After the observation, we can verify the fitness of the code C found by a straightforward procedure. This procedure is similar to I_U with a single change: Sign is to be replaced by a change in a special ancilla that can be observed after the procedure; we thus determine whether the code C fits.

To find the complexity of our procedure Rec, we note that the complexity $Mn^2\sqrt{N/d}$ of Difference must be multiplied by $\sqrt{Q}$ following from (8) and by $\sqrt{T}$ following from definition (7). The resulting complexity is $Mn^2\sqrt{TQN/d}$.

3.6. Advantages of the recognition algorithms

Advantages of the proposed algorithms are their high speed and small memory. In particular, the algorithm for the molecular structure recognition allows recognizing molecular circuits using microscopic memory, whereas classically this task requires exponentially large memory. We now compare the proposed algorithms with their classical counterparts; we omit logarithmic multipliers.

1. Recognition of eigenvalues and finding thermodynamic functions. We fix some value of M determining the precision of the eigenvalue approximation. We first consider the case where the number of ancillary qubits in a quantum gate array is small. By the direct classical method, we must then build the matrix of the unitary transform induced by the gate array. This requires the order N^3 steps and at least order N^2 bits. The known quantum algorithm given by Travaglione and Milburn in [8], based on the Abrams and Lloyd operator Rev, contains repeated measurements of frequencies and therefore requires time of the

order NM; for sparse spectra, it is of the same order as for the Hams–Raedt algorithm and its only advantage over the latter is exponential memory saving.

Our algorithm recognizes an eigenvalue in $\sqrt{N}Mn$ steps. This time for the sparse area of the spectrum is about the square root of the time of the best known algorithms. Here, the memory is of the order g^2 qubits (g is the size of the gate array), that is, about the squared memory used in [2], but still exponentially smaller than in classical methods. The proposed algorithm therefore gives an essential speedup over the known methods in the case where the number of ancillary qubits in a given gate array is small (as in the case of a molecular structure simulated by the gate array) and an area of the spectrum is sparse. The same advantage is possessed by the proposed method of finding thermodynamic functions.

If the spectra are dense, we assume that $M = N$, which means that eigenvalues differ by $1/N$ at least. The time of our algorithm is then $O(N)$.

We next consider the case where the number a of ancillary qubits involved in the gate array simultaneously is greater than the length n of the input. The direct classical method then requires more than 2^{2a} steps and at least 2^m bits, whereas our algorithm requires only about $g2^n$ steps and gn^2 memory and the quantum speed-up can be more than the square root.

2. Recognition of molecular structures. We first assume that the spectra are sparse. To be able to compare our method with the evident classical algorithm, we assume that the code of a molecular circuit of the length n is a string of ones and zeroes of this length. Therefore, $M = N$. The next natural assumption that can also be presumed for electronic circuits is that the sampling of the code of a circuit from the uniform distribution induces a sampling of all possible spectra from the uniform distribution. Then the number of all possible choices of spectrum approximations (or parts of the spectrum subject to the statement of the recognition problem) within $1/L$ consisting of frequencies of the form l/M is about $2^M = N$. This implies that M and Q must be logarithmic in N in our assumption. Our method therefore has the time complexity $O(N)$. With these assumptions, the time complexity of the classical direct algorithm examining all codes and calculating the corresponding spectra is about $N^3 \cdot N = N^4$, whereas our algorithm requires the time about N and the logarithmic memory. The quantum time for this problem is therefore about the fourth root of the time of the classical direct method and the quantum space is logarithmic.

If the spectra are dense, then Q and M are of the order N and our method requires the time $O(N^{2.5})$, to be compared with $O(N^4)$ of the direct classical way.

3. Recognition of electronic devices. There are no classical analogues of this problem in the general case. We compare the two algorithms constructed above with their classical and known quantum counterparts. We first consider a single quantum recognition algorithm that can easily be deduced from the previously known technique. This is the algorithm of recognizing a circuit realizing a classical involutive function of the form f:

$$Q \longrightarrow Q, \quad f = f^{-1}.$$

This task can be reduced to the search of y such that the following logic formula is true: $\forall x\ A(x, y)$, where $A(x, y)$ is some predicate. Indeed, if we take $Y(x) = U(x)$ instead of $A(x, y)$, where Y is a function whose code is y, we obtain the problem of recognition of the circuit generating U. The algorithm for such formulas given in [4] has the time complexity of the order $\sqrt{TN}$. This task is a particular case of our algorithm for involutive devices and it has the same complexity. In this particular case, quantum time is of the order given by the square root of the classical time. But if we consider a slightly more general but still restricted problem of the recognition of involutive devices producing linear combinations of basic states (like quantum subroutines), the advantage over the classical method of recognition increases. For example, we consider the restricted problem where we must choose between two alternative constructions of a tested device inducing a nonclassical unitary transformation. The naive method of observing the results of the action of the tested device on the different inputs requires the order $(1/\epsilon)N^3$ of steps to restore the matrix of the operator U_C within ϵ. This ϵ must then be less than $1/\sqrt{N}$ to give a vanishing difference between operators in the Hilbert space. Therefore, the time complexity of the naive method of recognition is roughly $N^{7/2}$. On the other hand, the method proposed in Sec. 3.4 requires choosing d that only converges to zero as N tends to infinity. The time required by our method is therefore slightly more than $\sqrt{N}$. We thus have almost the seventh degree speed-up for the problem of distinguishing electronic circuits generating transformations with nonclassical matrices.

4. CONCLUSIONS

The main conclusion is that the molecular structure and physical properties of environment can be quickly recognized on the microscopic level whereas

the classical methods require huge time and especially memory. The new algorithms of recognizing eigenvalues with a fixed precision, recognizing the molecular structure, and finding thermodynamic functions give a quadratic speed-up and an exponential memory saving compared with the best classical algorithms. The new method based on quantum computing was proposed for fast recognition of electronic devices. By this method, two devices with the same given spectrum can be distinguished in the time about the seventh root of the time of direct measurements. All these algorithms show essential potential advantages of microscopic size quantum devices compared to their classical counterparts with much bigger memory. The advantages pertain to intellectual tasks like recognition of the structure of other devices and important properties of environment. The proposed algorithms are constructed from the standard known subroutines; they have a simple structure and are entirely within the framework of the conventional quantum computing paradigm.

I am sincerely grateful to Kamil Valiev for creating the conditions for investigations in quantum computing at the Institute of Physics and Technology and for his attention and valuable advices concerning my work.

REFERENCES

1. A. Hams and H. de Raedt, E-print archives, quant-ph/0004016.

2. D. S. Abrams and S. Lloyd, E-print archives, quant-ph/9807070.

3. P. W. Shor, Siam J. Sci. Stat. Comp. **26**, 1484 (1997).

4. H. Buhrman, R. Cleve, and A. Wigderson, in *Proc. STOC 98* Los Angeles, CA, USA (1998), p 63.

5. L. K. Grover, in *Proc. STOC 96* Santa Fe, NM, USA (1996), p. 212.

6. M. Boyer, G. Brassard, P. Hoyer, and A. Tapp, Fortsch. Phys. **46**, 493 (1998).

7. Y. Ozhigov, E-print archives, quant-ph/0004021.

8. B. C. Travaglione and G. J. Milburn, E-print archives, quant-ph/0008053.

9. G. Brassard, P. Hoyer, and A. Tapp, E-print archives, quant-ph/9805082.