Analysis of the shortest vector problems with quantum annealing to search the excited states

Katsuki Ura1,2†, Takashi Imoto2†, Tetsuro Nikuni1, Shiro Kawabata2,3, and Yuichiro Matsuzaki2,3*  

1Department of Physics, Tokyo University of Science, 1-3, Kagurazaka, Shinjuku-ku, Tokyo, 162-8601, Japan  
2Research Center for Emerging Computing Technologies, National Institute of Advanced Industrial Science and Technology (AIST), Umezono1-1-1, Tsukuba, Ibaraki 305-8568, Japan  
3NEC-AIST Quantum Technology Cooperative Research Laboratory, National Institute of Advanced Industrial Science and Technology (AIST), Tsukuba, Ibaraki 305-8568, Japan  
†These authors equally contributed to this paper.

The shortest vector problem (SVP) is one of the lattice problems and is the mathematical basis for lattice-based cryptography, which is expected to be post-quantum cryptography. The SVP can be mapped onto the Ising problem, which in principle can be solved by quantum annealing (QA). However, one issue in solving the SVP using QA is that the solution of the SVP corresponds to the first excited state of the problem Hamiltonian. Therefore, QA, which searches for ground states, cannot provide a solution with high probability. In this paper, we propose to adopt an excited-state search of the QA to solve the shortest vector problem. We numerically show that the excited-state search provides a solution with a higher probability than the ground-state search. © 2023 The Japan Society of Applied Physics

1. Introduction

Quantum annealing (QA) is one of the methods to solve combinatorial optimization problems.1–4 It is known that the combinatorial optimization problem can be mapped to the problem of finding the ground state of the Ising Hamiltonian.5–7 QA is used to find the ground state of the Ising Hamiltonian.5–7 In QA, the Hamiltonian is time-dependent; we slowly change the Hamiltonian from the independent spin model with the transverse fields (called the driver Hamiltonian) to the target Ising Hamiltonian (called a problem Hamiltonian). As long as an adiabatic condition holds,8–12 we can obtain a ground state of the problem Hamiltonian when the initial state is a ground state of the driver Hamiltonian.

D-Wave Systems Inc. has developed a quantum hardware to perform QA using thousands of superconducting flux qubits.13–16 Several other quantum hardware for QA have been proposed and developed.17–19 Previous researches mainly focused on the ground-state search for QA.

More recently, there have been studies of excited-state searches in which the excited state of the driver Hamiltonian is selected as the initial state.20–23 A crucial point of the excited-state search is that we need to use non-uniform transverse magnetic fields in the driver Hamiltonian to resolve the degeneracy of the excited state of the driver Hamiltonian.20 This procedure allows us to prepare a non-degenerate excited state of the driver Hamiltonian when we start QA. By changing the Hamiltonian from the driver one to the problem one, we obtain the excited state of the problem Hamiltonian as long as the adiabatic condition is satisfied. The excited-state search in QA is useful in quantum chemistry;24 for example, it is essential to know the photochemical properties of molecules, which requires information not only on the ground state but also on the excited state.

Post-quantum cryptography has attracted much attention from many researchers. Rivest–Shamir–Adleman (RSA) is a widely used public key cryptography with security based on the difficulty of the prime factorization.25 Once the fault-tolerant quantum computer is developed, RSA cryptography can be efficiently decrypted by Shor’s algorithm.26 Therefore, research on post-quantum cryptography, which is difficult to solve even with a gate-type quantum computer, is underway. Lattice-based cryptography (LBC)27 is one of the candidates for post-quantum cryptography.28

One of the key mathematical problems in LBC is the shortest vector problem (SVP), which is the problem of finding the shortest non-zero vector in a given lattice. There are two approaches to solving lattice problems. The first approach is to choose input vectors from a distribution on a lattice and iteratively combine the vectors so that output should be probabilistically generated as solutions.29–32 The second approach is to enumerate all vectors in a specific sphere centered at the origin. There is a guarantee that the solution is contained if it is carefully chosen.33,34 Although these are classical algorithms, it is known that the SVP can be solved using a gate-type quantum computer. A quantum tree algorithm (based on Grover’s algorithm) can solve the SVP.35 However, it still takes an exponentially longer time to solve larger problems.

Recently, a method using QA was proposed to search for solutions of the SVP. More specifically, Joseph et al. proposed a heuristic method for finding the solution to the SVP using a ground-state search for QA.36 The SVP can be mapped onto an Ising Hamiltonian with integer spins, and the first excited state of the Hamiltonian corresponds to the solution. In their method, after the ground state of the driver Hamiltonian is prepared, the Hamiltonian is changed from the driver Hamiltonian to the problem Hamiltonian over time. The goal is to obtain the desired first excited state of the problem Hamiltonian via a non-adiabatic transition from the ground state to the first excited state. However, there is no known method to find a suitable schedule to change the Hamiltonian for obtaining the first excited state in their approach. If the Hamiltonian is changed slowly, the ground

---

*SC1090-1 © 2023 The Japan Society of Applied Physics*
state is obtained. On the other hand, a rapid change of the Hamiltonian would induce non-adiabatic transitions to not only the first excited state but also to other excited states.

In this paper, we propose to use the excited-state search with QA to find a solution to the SVP. We adopt the inhomogeneous transverse fields with integer spins as the driver Hamiltonian so that we can prepare the non-degenerate first excited state of the driver Hamiltonian. By changing the Hamiltonian from the driver Hamiltonian to the problem Hamiltonian, we can obtain, with finite probability, the first excited state of the problem Hamiltonian, which is the solution of the SVP. By increasing the annealing time, the dynamics become more adiabatic, and the success probability should increase as long as the decoherence is negligible.

We also show that the first excited state of the driver Hamiltonian with integer spins is an entangled state, which is experimentally challenging to prepare. It is worth mentioning that, in our previous study,\(^3\) we actually considered such an experimentally challenging to prepare. It is worth mentioning that, unlike the ground-state search, the success probability in our method by using a specific separable state as the initial state.\(^3\)\(^-\)\(^4\)\(^0\) Moreover, we compare our method based on the excited-state search with the previous approach based on the ground-state search. We show that our method provides higher success probabilities for most parameters.

2. Quantum annealing (QA)

2.1. Ground-state search

In this subsection, we describe QA for the ground-state search. In QA, quantum fluctuations are used to find a ground state of a given Ising Hamiltonian. The total Hamiltonian for QA is given as follows:

\[
\hat{H} (t) = \left(1 - \frac{t}{T}\right)\hat{H}_D + \left(\frac{t}{T}\right)\hat{H}_P, \\
\hat{H}_D = -b \sum_{i=1}^{N} \hat{\sigma}_i^z, \\
\hat{H}_P = \sum_{i=1}^{N} h_i \hat{\sigma}_i^z + \sum_{i=1}^{N} J_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z,
\]

where \( \hat{H}_D \) is the driver Hamiltonian to induce quantum fluctuations, \( \hat{H}_P \) is the problem Hamiltonian whose ground state corresponds to the solution of the combinatorial optimization problem, \( b \) denotes the strength of the transverse magnetic field, \( h_i \) denotes the longitudinal magnetic field, and \( J_{ij} \) denotes the coupling constant of the Ising interaction. Also, \( \sigma_i \) and \( \sigma_z \) denote the Pauli matrices.

We prepare an initial state as the ground state of the driver Hamiltonian, and let this state evolve by the time-dependent Hamiltonian \( \hat{H}(t) \). As long as the dynamics is adiabatic, we can obtain the ground state of the problem Hamiltonian at \( t = T \). On the other hand, if the dynamics is not slow enough to satisfy the adiabatic condition, non-adiabatic transitions occur, and there will be a finite population in the excited states.

2.2. Excited-state search

In this section, we describe QA for the excited state search.\(^2\)\(^\text{0} - \text{23}\) We consider the following Hamiltonian

\[
\hat{H} (t) = \left(1 - \frac{t}{T}\right)\hat{H}_D^{(\text{mu})} + \left(\frac{t}{T}\right)\hat{H}_P,
\]

\[
\hat{H}_D^{(\text{mu})} = -\sum_{i=1}^{N} b_i^{(\text{mu})} \hat{\sigma}_i^{z(\text{mu})},
\]

\[
\hat{H}_P = \sum_{i=1}^{N} h_i \hat{\sigma}_i^{z(\text{mu})} + \sum_{i=1}^{N} J_{ij} \hat{\sigma}_i^{z(\text{mu})} \hat{\sigma}_j^{z(\text{mu})},
\]

where \( b_i^{(\text{mu})} \) is the amplitude of the transverse magnetic field at site \( i \). This spatially non-uniform transverse magnetic field can resolve the degeneracy of the first excited state of the driver Hamiltonian. First, we prepare the first excited state of \( \hat{H}_D \). Second, we let the system evolve according to the time-dependent Hamiltonian from \( t = 0 \) to \( t = T \). After these steps, we can obtain the first excited state of the problem Hamiltonian, as long as the adiabatic condition is satisfied. It is worth mentioning that, unlike the ground-state search, we need to prepare the first excited state of the driver Hamiltonian as the initial state in this scheme. When we use superconducting flux qubits, it is possible to implement a single-qubit gate by applying microwave pulses.\(^3\)\(^1 - \text{43}\) By using such a technique, we can prepare the first excited state of the driver Hamiltonian.

3. The shortest vector problem (SVP)

We review the SVP, which is the mathematical basis for post-quantum cryptography. We consider a set of lattice vectors as defined below:

\[
L = \{\sum_{i=1}^{N} x_i \hat{b}_i \} = \{ B \cdot x : x \in \mathbb{Z}^N \},
\]

where \( x = [x_1, x_2, \cdots, x_N] \in \mathbb{Z}^N \) is a set of integers representing the coefficients of the lattice basis vectors, \( B \) is a vector of the coefficients, \( \{ \hat{b}_1, \hat{b}_2, \cdots, \hat{b}_N \} \) is the lattice basis matrices. Each vector on the lattice is expressed as follows:

\[
v = B \cdot x = x_1 \hat{b}_1 + \cdots + x_N \hat{b}_N \in L.
\]

The SVP aims to find a non-zero vector with the smallest norm on this lattice.

4. Mapping of SVP

Let us explain how to map the SVP onto the Ising Hamiltonian.\(^3\)\(^6\) The norm of the vector \( v \) on the lattice can be written as

\[
||v||^2 = \sum_{i,j=1}^{N} x_i x_j \hat{b}_i \cdot \hat{b}_j = \sum_{i,j=1}^{N} x_i x_j G_{ij},
\]

where \( G_{ij} = \hat{b}_i \cdot \hat{b}_j \) is the element of the Gram matrix of the lattice basis vectors. We consider the search for a solution of the SVP in the range \(-k \leq x_i \leq k\). Let us consider 24N qubits, and the Hamiltonian corresponding to the norm can be written as

\[
\hat{H}_P^{(\text{SVP})} = J \sum_{i,j=1}^{N} G_{ij} \hat{Q}^{(i)} \hat{Q}^{(j)},
\]
where $\hat{O}^{(i)}$ is a diagonal matrix defined as $\hat{O}^{(i)} = \sum_{p=1}^{2k} \hat{\sigma}_z^{(p,i)} / 2$ ($i = 1, 2, \ldots, N$), $J$ denotes a constant factor with a unit of energy, and $\hat{\sigma}_z$ denotes a Pauli matrix. Throughout of this paper, by setting $J = 1$, the time and energy are normalized by this value. The ground state of the Hamiltonian (10) corresponds to the zero vector. Therefore, the first excited state is the solution of the SVP.

5. Solving SVP using a ground state search with non-adiabatic transition with QA

We briefly explain the previous study on finding the solution of the SVP using the ground-state search with QA. The driver Hamiltonian is described as

$$\hat{H}_{D}^{\text{SVP}} = \sum_{i=1}^{N} B_i \sum_{p=1}^{2k} \hat{\sigma}_z^{(p,i)},$$

(11)

where $B_i$ is the strength of the transverse magnetic field and $\hat{\sigma}_z$ denotes the Pauli operator. The total Hamiltonian is given as

$$\hat{H}(t) = \left(1 - \frac{t}{T}\right)\hat{H}_{D}^{\text{SVP}} + \left(\frac{t}{T}\right)\hat{H}_{P},$$

(12)

where $T$ is the annealing time. The QA was originally proposed to find the ground state of the problem Hamiltonian with the adiabatic dynamics. After preparing the ground state of the driver Hamiltonian, we evolve the system according to the total Hamiltonian from $t = 0$ to $t = T$. As long as the dynamics is adiabatic, the ground state of the problem Hamiltonian is obtained as a final state. However, since the first excited state of the problem Hamiltonian is the solution of the SVP, we cannot obtain the solution with high probability by using the ground-state search. In the previous approach, non-adiabatic transitions are utilized to excite the system. If one could find suitable scheduling, we may obtain the first excited state with high probability. However, finding an optimal annealing time is not straightforward as long as the ground-state search is used.

6. Solving SVP using excited-state search with QA

In this section, we propose a method for finding a solution to the SVP using the excited-state search with QA.

6.1. Preparing the first excited state as the initial state

For the excited-state search, the driver Hamiltonian is given by

$$\hat{H}_{D}^{\text{SVPE}} = \sum_{i=1}^{N} B_i \sum_{p=1}^{2k} \hat{\sigma}_z^{(p,i)},$$

(13)

where $\{B_i^{(p,i)}\}_{k=1}^{N}$ represents the strength of the non-uniform transverse magnetic field. We set $B_1^{(1)} = B_2^{(2)} = \cdots = B_N^{(N)}$, to resolve the degeneracy of the first excited state of the driver Hamiltonian. On the other hand, we adopt $\hat{H}_{P}^{\text{SVPE}}$ in Eq. (10) as the problem Hamiltonian. To save the computational resources, we consider a subspace spanned by Dicke basis. Then, the eigenvalue of the operator $\hat{O}^{(i)}$ corresponds to the coefficient of the $N$th dimensional lattice, which takes the integer value in the range of $-k \leq \alpha \leq k$. The total Hamiltonian is

$$\hat{H} = (1 - \frac{t}{T})\hat{H}_{D}^{\text{SVPE}} + \frac{t}{T}\hat{H}_{P}^{\text{SVPE}}.$$  

After we prepare the first excited state of $\hat{H}_{D}^{\text{SVPE}}$ as the initial state, we let the system evolve according to $\hat{H}$ from $t = 0$ to $t = T$. The first excited state of the driver Hamiltonian is described as

$$|W\rangle_{1-2k} = \bigotimes_{j=2k+1}^{2kN} |\alpha\rangle_{j},$$

where $\bigotimes_{j=1}^{m} |\alpha\rangle_{j} = |\alpha\rangle_{1} \cdots |\alpha\rangle_{m}$ denotes a separable state, and $|W\rangle_{1-2k}$ is the entangled state given by

$$|W\rangle_{1-2k} = \frac{1}{\sqrt{2^{2k}}} \bigotimes_{j=1}^{2k} \hat{\sigma}_z^{(p,j)} \bigotimes_{j=1}^{2k} |\alpha\rangle_{j}.$$  

(15)

Unlike the previous approach of Ref. 34, we change the Hamiltonian in an adiabatic way so that we obtain the first excited state of $\hat{H}_{P}^{\text{SVPE}}$, which is the solution of the SVP. The adiabatic theorem guarantees that we can obtain the solution with a high probability by taking a sufficiently long time.

6.2. Using spin coherent state for initial state

The aforementioned excited-state search requires QA to start from an initial state that contains an entanglement. However, preparing an entangled initial state in the actual QA device is challenging. In actual experiments, it is desirable to use a separable initial state. Therefore, we consider using the spin-coherent (SC) state as the initial state. The SC state is described as follows:

$$|\phi\rangle_{1-2k} = \bigotimes_{j=1}^{2kN} (\sqrt{\epsilon}|+\rangle_{j} + \sqrt{1-\epsilon}|\alpha\rangle_{j}),$$

(16)

where we set $\epsilon = \frac{1}{2k-1}$. The inner product of $|W\rangle_{1-2k}$ and $|\phi\rangle_{1-2k}$ is calculated as

$$\langle W|\phi\rangle_{1-2k} = \sqrt{2k\epsilon (1-\epsilon)^{2k-1}} \approx \sqrt{\frac{2k}{2k-1}} e^{-1} = \sqrt{\frac{1}{\epsilon}} \approx 0.61 (k \gg 1).$$

(17)

This means that the SC state contains the first excited state $|W\rangle_{1-2k}$ with a reasonably high probability. Therefore, we propose to use the SC state as an initial state for the excited-state search to solve the SVP. As we mentioned in 2.2, we can perform a single-qubit gate on superconducting flux qubits, and so it is possible to prepare such an SC state. We will perform numerical simulations to quantify the performance of the search with the SC state.

7. Numerical calculation

In this section, we show numerical results to compare the performance of our scheme with that of the previous scheme.1) We consider the SVP with $N = 2$, i.e. the two-dimensional lattice. The two vectors $b_1$ and $b_2$ are given in the problem. We characterize these vectors by their norms $|b_j|^2_{j=1}^k$ and the angle $\theta$ between them. By solving the time-dependent Schrödinger equation, we obtain the state after QA. We define the failure probability as the probability that the measurement result (in computational basis) for the state after QA gives an incorrect answer for the SVP. This means that the success probability is defined as a population of the first excited state of the problem Hamiltonian after QA. We calculate the failure probabilities for the ground-state and excited-state search, respectively. For the ground-state...
search, we optimize \( B_x \) to minimize the failure probability. On the other hand, for the excited-state search, we optimize \( B_x \) to minimize the failure probability while fixing \( B_{xx}^{(1)}/B_{xx}^{(2)} = 1/2 \) for the excited-state search and the search with a spin coherent state, while we fix \( B_{xx}^{(1)}/B_{xx}^{(2)} = 1 \) for the ground-state search. Moreover, we optimize the values of \( B_x^{(1)} \) to minimize the failure probability.

In Fig. 1, we plot the failure probabilities for the ground state and excited-state search against the annealing time \( T \), respectively. These results show that the failure probability for the excited-state search is smaller than that for the ground-state search. In the excited-state search, the failure probability with \( \theta = \frac{\pi}{4} \) is larger than those with \( \theta = \frac{\pi}{6} \). This may correspond to the fact that in the SVP, the problem becomes more difficult as the angle \( \theta \) becomes smaller. However, the primary advantage of our method is that, even if the problem becomes more difficult, the failure probability can be sufficiently small by taking a reasonably long annealing time \( T \), which is guaranteed by the adiabatic theorem.

The failure probability of the search with the SC state is larger than that using the first excited state. This is because the SC state includes states other than the first excited state. On the other hand, the search with the SC state provides a smaller failure probability than the ground-state search when the annealing time \( T \) is large, and this shows the practicality of our scheme.

Next, we consider the case where the ratio of the norms of the two vectors is fixed at either 1:1 or 1:2. We then plot how the failure probability changes when the angle between the vectors is changed. In each case, the amplitude of the transverse magnetic field is optimized to minimize the failure probability. Figure 2 shows that the failure probability is always lower for the excited-state search using the first excited state than that for the ground-state search. The search with SC state also shows a smaller failure probability than the
ground-state search, except for a few exceptional points (where the ratio of vectors is 1:2 and the angle is around $\pi/2$). The reason why the failure probability of the excited-state search is larger at an angle of $\pi/2$ when the ratio of vectors is 1:2 is due to the existence of the symmetry in the Hamiltonian, which causes energy-level crossing in QA. This point is explained in detail in the appendix.

In the case of the excited-state search, when the vector ratio is 1:2, the failure probability becomes large around the angle of $\pi/6$. This is due to the fact that the energies of the lowest four excited states of $H_{PSVP}^{(n)}$ are close to each other, as shown in Fig. 3. The small energy gap causes non-adiabatic transitions from the first excited state to the other excited states, which increases the failure probability. Also, when the vector ratio is 1:1, the failure probability is larger around the angle of $\pi/3$. This is due to the fact that the first excited state of $H_{PSVP}^{(n)}$ is 6-fold degenerate when the vector ratio is 1:1 and the angle is $\pi/3$. In this case, $(x_1, x_2) = (1,0), (0,1) (1, -1), (-1,0), (0,-1), (-1,1)$ provide the shortest vector. Therefore, the energy gap between the first excited state and the other excited states becomes smaller at angles around $\pi/3$, resulting in more non-adiabatic transitions.

In Fig. 4, we plot the success probability for the excited state search, the search with the spin coherent state, and the ground state search against the dimension $N$, respectively. As we increase $N$, the success probability decreases for all cases. However, the excited state search and the search with the spin coherent state show a better performance than the ground-state search. This demonstrates that our methods are more useful than the conventional methods in these parameters.

**Fig. 3.** (Color online) We plot the instantaneous eigenenergy of the total Hamiltonian during QA for the vector ratio of 1:2 and the angle is $\pi/6$. This graph shows that the energy gaps among the first, second, third, and fourth excited states of the problem Hamiltonian are very small. Except the vector ratio and the angle, we use the same parameters as those used in Fig. 2.

**Fig. 4.** (Color online) Plot of the success probability of QA. We plot the results for the excited state search (ex), the search with the spin coherent state (sc), and the ground state search (gs) against the dimension $N$, respectively. Here, we set $k = 2, T = 10, \theta = \pi/5, \delta = 0.1$, and $b_n = 1 - \delta + \frac{\delta}{n}(n - 1)$ for $n = 1, \ldots, N$. The Gram matrix is given as $G_{ij} = b_i \cdot b_j \cos \theta$ where we set $\theta = \pi/5$. Also, for the excited state search and the search with the spin coherent state, we choose $B_{i j}^{(1)} / B_{i j}^{(2)} = 1 / 2$ and $B_{i j}^{(4)} / B_{i j}^{(7)} = 1$ for $l = 3, 4, \ldots, N$. On the other hand, we choose $B_{i j}^{(1)} / B_{i j}^{(4)} = 1$ for $l = 2, 3, \ldots, N$. Moreover, we optimize the values of $B_{i j}^{(1)}$ to maximize the success probability in each case.
8. Possible physical realization

To implement the excited state search with QA, it is crucial to use a long-lived qubit, because otherwise the excited state would decay into the ground state by the energy relaxation. There was a theoretical proposal to perform QA with capacitively-shunted flux qubits,\(^ {44} \) which have a long coherence time of tens of microseconds. Therefore, we expect that our proposed protocol can be demonstrated by the capacitively-shunted flux qubits.

9. Conclusion

In conclusion, we propose to use the excited-state search with the QA to solve the SVP. Importantly, the solution of the SVP is not the ground state but the first excited state of the problem Hamiltonian. So, unlike the previous approach of solving the SVP by ground-state search using QA, the adiabatic theorem guarantees that our scheme can obtain a solution in our approach if we take a sufficiently long time.

Our numerical simulations reveal that our scheme provides a smaller failure probability than the previous scheme. Our results show the potential of our scheme to solve the SVP by efficiently long time. Importantly, we have \( P_{\hat{P}}(\hat{S}^{(1)} = 0) = |\hat{S}^{(1)} = 0| \). Therefore, the first excited states of \( H^{(\text{SVP})}_P \) have the parity \( \hat{P}_{\hat{P}} = 1 \) while the first excited state of \( H^{(\text{SVP})}_D \) has the parity \( \hat{P}_{\hat{P}} = -1 \). Since these states belong to different symmetry sectors, the excited state search by QA does not provide the solution of the SVP in this case.

Acknowledgments

K. U. and T. I. contributed to this work equally. This work was supported by MEXT’s Leading Initiative for Excellent Young Researchers, JST PRESTO (Grant No. JPMJPR1919), Japan. This paper is partly based on the results obtained from the project, JPNP16007, commissioned by the New Energy and Industrial Technology Development Organization (NEDO), Japan.

Appendix

In this appendix, we explain how the symmetry appears in the excited state search at the angle of \( \pi/2 \) when the ratio of vectors is 1:2, which causes nonadiabatic transitions in QA.

Let us define the parity operator \( \hat{P} = e^{-i\pi \hat{s}_z} \) for spin 2, where we define \( \hat{s}_z = \sum_{p=1}^{4} \hat{s}_{z(p)} \). We also define \( \hat{s}_y = \sum_{p=1}^{4} \hat{s}_{y(p)} \) and \( \hat{s}_x = \sum_{p=1}^{4} \hat{s}_{x(p)} \). The parity operator has properties such as \( \hat{P} \hat{s}_z^{(1)} \hat{P} = \hat{s}_z^{(1)} \), \( \hat{P} \hat{s}_y^{(1)} \hat{P} = -\hat{s}_y^{(1)} \), and \( \hat{P} \hat{s}_x^{(1)} \hat{P} = -\hat{s}_x^{(1)} \). In addition, the parity operator \( \hat{P} \) commutes with \( \hat{H}^{(\text{SVP})}_P \).

The lowest eigenstate of \( \hat{S}_z^{(1)} \) is described as \( |\hat{S}_z^{(1)} = -2\rangle \), and the second lowest eigenstate is described as \( |\hat{S}_z^{(1)} = -1\rangle \). We have \( \hat{P}_{\hat{P}} |\hat{S}_z^{(1)} = -2\rangle = |\hat{S}_z^{(1)} = -2\rangle \) and \( \hat{P}_{\hat{P}} |\hat{S}_z^{(1)} = -1\rangle = -|\hat{S}_z^{(1)} = -1\rangle \). For the excited state search, we prepare the first excited state of \( H^{(\text{SVP})}_D \) such as \( |\hat{S}_z^{(1)} = -1\rangle \otimes_{j=2} |\hat{S}_z^{(j)} = -2\rangle \), and the parity of this state is \( P_f = -1 \) and \( P_f = 1 \) for \( f \geq 2 \).

For the SVP, let us consider the case \( N = 2 \), \( |b_1| = \frac{1}{2} |b_2| \), and \( b_1 \cdot b_2 = 0 \). In this case, we have \( H^{(\text{SVP})}_D = \frac{\beta}{2} \hat{S}_z^{(1)} + B \hat{S}_x^{(2)} \) and \( H^{(\text{SVP})}_P = 4 (\hat{S}_z^{(1)})^2 + (\hat{S}_x^{(2)})^2 \). The first excited states of \( H^{(\text{SVP})}_P \) are \( |\hat{S}_z^{(1)} = 0\rangle |\hat{S}_z^{(2)} = 1\rangle = \frac{1}{2} \) and \( |\hat{S}_z^{(1)} = 0\rangle |\hat{S}_z^{(2)} = -1\rangle = \frac{1}{2} \).

1) B. Apolloni, C. Carvalho, and D. De Falco, Stochastic Processes Appl. 33, 233 (1989).
2) A. B. Finnmula, M. Gomez, C. Sebenik, C. Stenson, and J. D. Doll, Chem. Phys. Lett. 219, 343 (1994).
3) T. Kadowaki and H. Nishimori, Phys. Rev. E 58, 5355 (1998).
4) A. Lucas, Front. Phys. 2, 5 (2014).
5) A. Schrijver, Handbooks in Operations Research and Management Science 12, 1 (2005).
6) S. Morita and H. Nishimori, J. Math. Phys. (N.Y.) 49, 125210 (2008).
7) P. Hanke, H. G. Katzgraber, W. Lechner, H. Nishimori, and W. D. Oliver, Rep. Prog. Phys. 83, 054401 (2020).
8) E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, (2000) arXiv:quant-ph/0011056.
9) D. Aharonov et al., SIAM Rev. 50, 755 (2008).
10) E. Farhi et al., Science 292, 472 (2001).
11) T. Albash and D. A. Lidar, Rev. Mod. Phys. 90, 015002 (2018).
12) A. M. Childs, E. Farhi, and J. Preskill, Phys. Rev. A 65, 012322 (2001).
13) C. C. McGeoch, R. Harris, S. P. Reinhardt, and P. I. Bunyk, Computer 52, 38 (2019).
14) M. W. Johnson et al., Nature 473, 194 (2011).
15) S. Boixo et al., Nat. Phys. 10, 218 (2014).
16) S. Boixo, T. Albash, F. M. Spedalieri, N. Chassellon, and D. A. Lidar, Nat. Commun. 4, 1 (2013).
17) M. Maaeza et al., J. Phys. Soc. Jpn. 88, 061012 (2019).
18) D. Saida et al., IEEE Trans. Quantum Eng. 2, 1 (2021).
19) D. Saida, M. Hidaka, K. Imafuku, and Y. Yamanashi, Sci. Rep. 12, 1 (2022).
20) Y. Seki, Y. Matsuraki, and S. Kawahata, J. Phys. Soc. Jpn. 90, 054002 (2021).
21) A. Teplukhin, B. K. Kendrick, and D. Babkov, J. Chem. Theor. Comput. 15, 4555 (2019).
22) A. Teplukhin, B. K. Kendrick, S. Tretiak, and P. A. Dub, Sci. Rep. 10, 20753 (2020).
23) M.-C. Chen et al., Phys. Rev. Lett. 125, 180501 (2020).
24) L. Serrano-Andrés and M. Merchán, J. Mol. Struct.: THEOCHEM 729, 99 (2005).
25) R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM 21, 120 (1978).
26) P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” Proc. 35th Annual Symp. on Foundations of Computer Science, 1994, p. 124.
27) M. Ajtai and C. Dwork, “Public-key cryptosystem with worst-case/average-case equivalence,” Proc. of the Twenty-ninth Annual ACM Symp. on Theory of Computing, 1997, p. 284.
28) M. Ajtai, C. Dwork, “A public-key cryptosystem with worst-case/average-case equivalence,” Proc. of the Twenty-ninth Annual ACM Symp. on Theory of Computing, 2001, p. 601.
29) D. Micciancio and O. Regev, “Lattice-based cryptography,” Post-Quantum Cryptography (Springer, Berlin, 2009) p. 147.
30) D. Micciancio and P. Voulgaris, “Faster exponential time algorithms for the shortest lattice vector problem,” Proc. of the Thirty-third Annual ACM Symp. on Theory of Computing, 2001, p. 601.
31) T. Laarhoven, “Sieving for shortest vectors in lattices using angular locality-sensitive hashing,” Annual Cryptology Conf. 2015p. 3.
32) L. Ducas, “Shortest vector from lattice sieving: a few dimensions for free,” Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques, 2018, p. 125.
33) M. Pohst, ACM SigSams Bull. 15, 37 (1981).
34) N. Gama, P. Q. Nguyen, and O. Regev, “Lattice enumeration using extreme pruning,” Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques, 2010, p. 257.

35) T. Laarhoven, M. Mosca, and J. V. D. Pol, “Solving the shortest vector problem in lattices faster using quantum search,” Int. Workshop on Post-Quantum Cryptography, 2013, p. 83.

36) D. Joseph, A. Callison, C. Ling, and F. Mintert, Phys. Rev. A 103, 032433 (2021).

37) K. Ura, T. Imoto, T. Nikuni, S. Kawabata, and Y. Matsuzaki, Ext. Abstr. Solid State Devices and Materials, 2022, p. 193.

38) M. Kitagawa and M. Ueda, Phys. Rev. A 47, 5138 (1993).

39) J. Radcliffe, J. Phys. A 4, 313 (1971).

40) F. Arecchi, E. Courtens, R. Gilmore, and H. Thomas, Phys. Rev. A 6, 2211 (1972).

41) J. Mooij et al., Science 285, 1036 (1999).

42) C. H. Van Der Wal et al., Science 290, 773 (2000).

43) I. Chiorescu, Y. Nakamura, C. M. Harms, and J. Mooij, Science 299, 1869 (2003).

44) Y. Matsuzaki, H. Hakoshima, Y. Seki, and S. Kawabata, Jpn. J. Appl. Phys. 59, SGGI06 (2020).

45) T. Imoto, Y. Seki, and Y. Matsuzaki, J. Phys. Soc. Jpn. 91, 064004 (2022).

46) A. Francis, E. Zelleke, Z. Zhang, A. F. Kemper, and J. K. Freericks, Symmetry 14, 809 (2022).

47) T. Imoto and Y. Matsuzaki, arXiv:2209.10983 (2022).

48) T. Imoto, Y. Seki, and Y. Matsuzaki, arXiv:2209.09575 (2022).