

Efficient lattice Hamiltonian encoding for the shortest vector problem

Eden Schirman^{1,2,*}, Cong Ling,³ and Florian Mintert^{1,4}¹*Physics Department, Imperial College London, London SW7 2BU, United Kingdom*²*Raymond and Beverly Sackler School of Physics and Astronomy, Tel-Aviv University, Tel-Aviv 6997801, Israel*³*Electrical and Electronic Engineering Department, Imperial College London, London SW7 2BU, United Kingdom*⁴*Helmholtz-Zentrum Dresden-Rossendorf, Bautzner Landstraße 400, 01328 Dresden, Germany*

(Received 22 July 2023; accepted 11 September 2026; published 2 October 2026)

The advent of quantum computing necessitates the transition of worldwide cryptosystems to postquantum cryptography (PQC), which is founded upon the problem of finding short vectors in high-dimensional structured lattices. It is assumed that the structure of these lattices cannot be exploited by quantum or classical algorithms attempting to find short vectors. In this work, we focus on the structure of the lattices used in PQC protocols—negacyclic (and cyclic) lattices—and provide a quantum algorithmic framework that efficiently encodes the structured lattices into Hamiltonians by exploiting their underlying symmetries. The efficient encoding substantially reduces the dimension of the corresponding Hilbert space by limiting it to a relevant subspace where short vectors are likely to be found—leading to significant savings in quantum resources (e.g., qubit count and circuit depth) required to implement a quantum algorithm for finding short vectors. We analytically prove the efficient encoding procedure and benchmark the proposed framework using the variational quantum eigensolver, demonstrating improved results with reduced quantum resources.

DOI: [10.1103/zv7d-3vby](https://doi.org/10.1103/zv7d-3vby)

I. INTRODUCTION

Quantum computing poses a substantial threat to the worldwide cryptosystem [1,2] as Shor's algorithm can efficiently solve the mathematical problem on which most cryptographic protocols are based—factoring [3]. This threat will become tangible with the availability of fault-tolerant quantum computers [4,5]. To counter it, the American National Institute of Standards and Technology (NIST) announced in 2024 a new set of cryptographic protocols believed to be secure against both quantum and classical attacks [6].

The main postquantum cryptography (PQC) protocols are based on the mathematical problem of finding the shortest nonzero vector in a high-dimensional lattice—the shortest-vector problem (SVP) [7]. That is, given a nonorthonormal basis for a lattice, the task is to find the minimal distance between two distinct lattice points. PQC protocols are actually based on a softer version of the problem [6], the approximate SVP—one where the goal is to find sufficiently short vectors whose length exceeds that of the shortest vector by at most a given polynomial factor of the lattice dimension.

To increase the efficiency of these protocols, lattices with some special structure—structured lattices—are used [8]. It is conjectured that the structure of these lattices does not provide any advantage to quantum (or classical) attacks [7]; i.e., it is

as hard to solve the approximate SVP for these lattices as it is for general lattices, even with a quantum computer. Since this is still an unproven conjecture, the search for counterexamples is still open [9,10].

Exploiting the structure and symmetries of a system for efficient encoding is a cornerstone technique in quantum physics. Tensor networks provide an efficient encoding of many-body quantum states by exploiting system structure [11,12] and are used in multiple disciplines such as condensed matter physics [13], quantum chemistry [14], and quantum information science [15]. Quantum simulation, which deals with simulating one quantum system using another, also relies heavily on exploiting system structure and symmetries for efficient implementation [16–18].

Hamiltonian encodings of lattices for the SVP have been proposed and used in previous works by some of us [19,20] and others [21–30]. To the best of our knowledge, this is the first work that leverages lattice structure for efficient Hamiltonian encoding, leading to a significant reduction in the quantum resources required for finding short lattice vectors. In addition to notable savings in qubit count and circuit depth, we show that our method increases the probability of finding short vectors.

The core idea of our method is to limit the search for short vectors to a small subspace very likely to contain a state corresponding to a sufficiently short vector. The existence of such subspaces and their characterization stem from the structure of the target lattices. The likelihood of finding short vectors in these subspaces is conjectured and numerically supported, whereas the subspaces themselves are rigorously characterized.

The rest of the paper is organized as follows. The necessary preliminaries regarding lattices are described in Sec. II.

*Contact author: schirman.eden@gmail.com

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

The symmetries of cyclic and negacyclic lattices that are reflected in the quantum formulation of the SVP and numerical support for our claim are described in Sec. III. The exploitation of these symmetries for efficient Hamiltonian encoding—the main result of our work—is the subject of Sec. IV, while Sec. V gives an explicit detailed description of the proposed method. Benchmarking of the method using the variational quantum eigensolver (VQE) [31] is presented in Sec. VI.

II. LATTICES

A lattice is a periodic arrangement of points in an N -dimensional Euclidean space. It can be defined in terms of a basis B comprised of N linearly independent vectors $\vec{b}_i$. While any point in the N -dimensional space can be expressed as a linear combination $\sum_i n_i \vec{b}_i$ of the basis vectors, lattice vectors are characterized by the constraint that the expansion coefficients n_i are integers. The collection of all lattice vectors is the lattice.

A. Structured lattices

Cyclic and negacyclic lattices are lattices with additional symmetries. Historically, cyclic lattices were first used in the NTRU cryptosystem [32] and have received much attention since then [33,34]. Meanwhile, cryptographic protocols in the NIST final list are actually based on negacyclic lattices [35,36]. Since, however, situations with cyclic symmetries are better known in physics and since the classification for the cyclic case is rather instructive for the subsequent discussion of the negacyclic case, we will study both cyclic and negacyclic lattices.

Their formal definition requires the cyclic permutation operator Π such that $\Pi \vec{b} = (b_{N-1}, b_0, b_1, \dots, b_{N-2})^T$ for any vector $\vec{b} = (b_0, b_1, \dots, b_{N-1})^T$, and the negacyclic permutation operator Γ , such that $\Gamma \vec{b} = (-b_{N-1}, b_0, b_1, \dots, b_{N-2})^T$. A basis of cyclic and negacyclic lattices can be defined in terms of a single vector $\vec{b}_0$ via the relation $\vec{b}_{i+1} = \Pi \vec{b}_i$ for cyclic lattices and $\vec{b}_{i+1} = \Gamma \vec{b}_i$ for negacyclic lattices.

Most of the relevant properties of a lattice are encoded in its Gram matrix G , comprised of all the scalar products of basis vectors, i.e., the matrix with the elements $G_{ij} = \vec{b}_i \cdot \vec{b}_j$.

The symmetries of the bases of cyclic and negacyclic lattices are also reflected in the corresponding Gram matrices, i.e., $G = \Pi G \Pi^\dagger$ for cyclic lattices and $G = \Gamma G \Gamma^\dagger$ for negacyclic lattices. From the unitarity of Π and Γ also follows the commutativity $[G, \Pi] = 0$ for cyclic and $[G, \Gamma] = 0$ for negacyclic lattices, so that the Gram matrix G shares a joint set of eigenvectors with Π or Γ , respectively.

Since the N th power of the permutation reduces to the identity, the eigenvalues of Π are given by $\exp(2\pi i j / N)$ with $j = 0, \dots, N-1$. Analogously, the eigenvalues of Γ are given by $\exp(\pi i (2j+1) / N)$ with $j = 0, \dots, N-1$, because of the relation $\Gamma^N = -\mathbf{1}$.

The matrix $U^{(c)}$ containing all eigenvectors of Π is given by the Fourier transformation matrix with elements

$$U_{qp}^{(c)} = \frac{1}{\sqrt{N}} \exp\left(-i \frac{2\pi}{N} pq\right), \quad (1a)$$

and the matrix $U^{(n)}$ containing all eigenvectors of Γ has the elements

$$U_{qp}^{(n)} = \frac{1}{\sqrt{N}} \exp\left(-i \frac{2\pi}{2N} p(2q+1)\right) \quad (1b)$$

for $0 \leq p, q \leq N-1$.

B. Length of lattice vectors

Since the squared Euclidean length of any lattice vector $\vec{b} = \sum_i n_i \vec{b}_i$ can be expressed as

$$|\vec{b}|^2 = \sum_{ij} G_{ij} n_i n_j \quad (2)$$

in terms of the Gram matrix, a quantum mechanical Hamiltonian

$$\hat{H} = \sum_{ij} G_{ij} \hat{N}_i \hat{N}_j \quad (3)$$

with mutually commuting operators $\hat{N}_i$ that have integer spectra can also encode the length of all the vectors in a given lattice [19]. The eigenstates of $\hat{H}$ are simultaneous eigenstates of all the operators $\hat{N}_i$ and read $|\vec{n}\rangle = |n_0, n_1, \dots, n_{N-1}\rangle$, where n_i denotes the eigenvalue of $\hat{N}_i$.

III. SYMMETRIES IN THE PROBLEM HAMILTONIAN

The quantum formulation of the approximate SVP is to find a low-excited state of the problem Hamiltonian given in Eq. (3). This formulation is applicable for any lattice, irrespective of potential symmetries.

Our central goal is to exploit the symmetries of cyclic and negacyclic lattices in order to formulate problem Hamiltonians that are beneficial for the approximate SVP. Their main benefit is the reduction in the number of operators $\hat{N}_q$ required for their representation. This yields a reduction in the quantum resources needed in practical implementations on quantum devices.

To this end, it is crucial to notice that any Hamiltonian of the form in Eq. (3) can be expressed as

$$\hat{H} = \sum_q g_q \hat{S}_q^\dagger \hat{S}_q, \quad (4)$$

in terms of the eigenvalues g_q of the Gram matrix and the operators

$$\hat{S}_q = \sum_p U_{qp} \hat{N}_p, \quad (5)$$

defined in terms of the unitary matrix U comprised of the eigenvectors of G . Commutativity of the operators $\hat{N}_q$ implies that also the operators $\hat{S}_q$ commute. Additionally, Hermiticity of the operators $\hat{N}_p$ implies $[\hat{S}_q, \hat{S}_p^\dagger] = 0$. The spectrum of $\hat{H}$ can thus be characterized completely by the simultaneous eigenstates of all the individual operators $\hat{S}_q$.

While in the case of a general lattice, the eigenvectors of G depend on the details of the lattice, in the case of cyclic and negacyclic lattices, the eigenvectors are lattice independent and are given by Eq. (1). Thus, the operators $\hat{S}_q$ are completely

determined by the type of symmetry and dimension of the lattice.

Since properties of a specific lattice enter the system Hamiltonian in Eq. (4) only via the eigenvalues g_q , there is the prospect of facilitating the quest for short vectors in terms of the eigenspaces of the operators $\hat{S}_q$.

By construction, any quantum state $|\vec{n}\rangle$ is an eigenstate of $\hat{S}_q$ and of $\hat{S}_q^\dagger \hat{S}_q$ with the corresponding eigenvalues s_n^q and $|s_n^q|^2$. The eigenvalue of the problem Hamiltonian associated with the state $|\vec{n}\rangle$ is thus given by

$$E_{\vec{n}} = \sum_q g_q |s_n^q|^2. \quad (6)$$

The eigenvalues g_q of the Gram matrix are non-negative due to its positive semidefiniteness. Thus, the eigenvalues $E_{\vec{n}}$ of the problem Hamiltonian (and equivalently the lengths of the lattice vectors) are given as a sum over non-negative terms. Each of these terms is associated with one of the operators $\hat{S}_q$.

One might expect that the Hamiltonian's first excited state (which corresponds to the shortest nonzero vector of the lattice) is a ground state of most operators $\hat{S}_q$, and a low-lying excited state of only one or a few of the operators. This, however, is not necessarily the case, because the condition that a given state $|\vec{n}\rangle$ is a ground state of one operator $\hat{S}_q$ might imply that $|\vec{n}\rangle$ is a highly excited eigenstate to some other operator $\hat{S}_p$.

Still, in practice, there is a high probability of finding a low-excited state of the problem Hamiltonian in the kernel of the operator $\hat{S}_q$ that corresponds to the largest eigenvalue g_q of the Gram matrix. Such an operator is referred here as the principal operator. Crucially, the existence of kernels for the $\hat{S}_q$ operators with nonzero states $|\vec{n}\rangle$ is guaranteed because of the lattice's cyclic (negacyclic) structure. The sole exception is the negacyclic case with a power-of-two lattice dimension, whose principal operator kernel contains only the zero vector (see Sec. VB). This is based on the theory of cyclotomic polynomials [37]. In order to provide a basis for the subsequent rigorous construction of low-lying eigenspaces, we will first give numerical evidence that the first excited state (corresponding to the shortest vector of the lattice) or a sufficiently low-excited state lies within the kernel of the principal operator.

We denote by γ the ratio of the length of the shortest vector contained in a given subspace and the length of the lattice's shortest vector, so that $\gamma = 1$ whenever the subspace contains the shortest vector. Sampling 1000 lattices per lattice dimension, Fig. 1 shows, on a logarithmic scale, the percentage of lattices with $\gamma = 1$ for the principal operator kernel (blue dots) and, for comparison, for a random subspace with the same cardinality (red squares). The cardinality of a subspace denotes the number of lattice states it contains within the examined range of integer coefficient. The values for the principal operator kernel exceed that for the random subspace and their expected value—the mean cardinality ratio (green triangles)—by 1–2 orders of magnitude.

The $\gamma = 1$ percentages for the principal operator kernel range from $(15.8 \pm 1.2)\%$ at $N = 14$ to $(47.4 \pm 1.6)\%$ at $N = 9$. The statistical uncertainty on these percentages is small at this sample size, such that the variation of the $\gamma = 1$

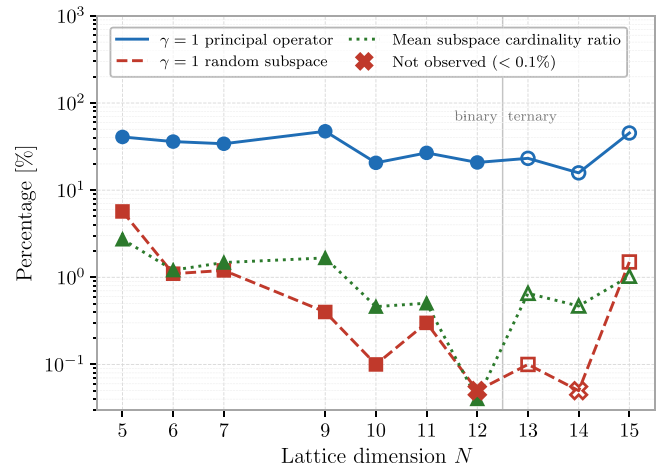


FIG. 1. Percentage of sampled lattices with $\gamma = 1$ (the shortest vector lies within the subspace), out of 1000 lattices per dimension, on a logarithmic scale. Values for the principal operator kernel (blue dots) are 1–2 orders of magnitude higher than for a random subspace of the same cardinality (red squares). Green triangles show the mean subspace-to-lattice cardinality ratio, i.e., the expected $\gamma = 1$ percentage for the random subspace. For $N = 12$ and $N = 14$, the shortest vector was not found in the random subspaces (crosses, plotted at the $< 0.1\%$ detection threshold). Binary (filled markers) and ternary (hollow markers) refer to the coefficient ranges defined in the text.

percentage across dimensions reflects the intrinsic number-theoretic structure of the kernels. The variation seems to track the mean subspace-to-lattice cardinality ratio. Overall, this indicates a high probability of finding the shortest vector within the kernel of the principal operator.

The range of examined integer coefficients is limited by available computational resources, which impose $KN \leq 24$. For lattice dimensions $N = 5$ to $N = 12$ (excluding $N = 8$, a power of 2), the coefficients n_q are within the range $[-2^{K-1}, 2^{K-1} - 1]$ with $K = 2$, labeled binary in Figs. 1 and 2. For $N = 13, 14, 15$, the coefficients are restricted to $\{-1, 0, 1\}$ [an effective $K = \log_2(3)$], labeled ternary; this restriction is justified because the majority of the shortest vectors have coefficients within this range.

For the approximate SVP, only a sufficiently short vector is required. Figure 2 therefore shows the 90th-percentile value of γ , $P_{90}(\gamma)$, over the sampled principal operator kernels as a function of the lattice dimensions (blue dots), separated into prime (solid lines) and nonprime (dashed line) dimensions. As characterized in Sec. VB, the principal operator kernel for prime N is typically one dimensional. Therefore, the corresponding $P_{90}(\gamma)$ values are higher than for nonprime lattice dimension, whose kernels are larger on average. Even for prime lattice dimensions, $P_{90}(\gamma)$ is on the order of $\mathcal{O}(2N)$ —linear in the lattice dimension.

For nonprime N , the percentile $P_{90}(\gamma)$ appears to be upper bounded by the logarithm of the inverse cardinality ratio between the smallest principal operator kernel and the full lattice. This quantity approximately equals the difference between the lattice dimension and the minimal number of kernel degrees of freedom multiplied by the range coefficient K , i.e., $\sim K \times [N - \min(\text{\#DOF})]$ (green triangles). The

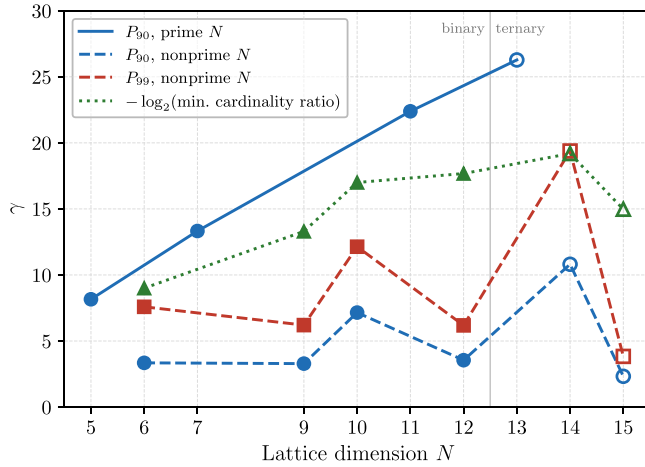


FIG. 2. The 90th percentile of γ , $P_{90}(\gamma)$, for the principal operator kernels: Blue dots joined by a solid line for prime lattice dimensions and by a dashed line for nonprime N . Red squares show the 99th percentile, $P_{99}(\gamma)$, for the nonprime dimensions. Both are qualitatively upper bounded by the logarithm of the inverse cardinality ratio between the smallest principal operator kernel and the full lattice (green triangles). Binary (filled markers) and ternary (hollow markers) refer to the coefficient ranges defined in the text.

99th-percentile values, $P_{99}(\gamma)$ (red squares), lie closer to this qualitative bound and follow the same trend.

To assess the influence of the coefficient range K , we repeated the simulations for $N = 5$ and $N = 6$ with $K = 2, 3, 4$. For both dimensions, the $\gamma = 1$ percentage and $P_{90}(\gamma)$ of the principal operator kernel are independent of K . The only residual K dependence is in $P_{99}(\gamma)$ for $N = 6$, which changes from 6.78 at $K = 2$ to 7.59 at both $K = 3$ and $K = 4$. The weak K dependency therefore indicates that the statistics reported here are representative of the method's behavior.

The resulting prospect that low-excited states (which correspond to short lattice vectors) lie within the kernel of an operator $\hat{S}_q$ motivates the formulation of a reduced problem Hamiltonian that represents the problem Hamiltonian with the restriction to the kernel. These reduced problem Hamiltonians are derived in Sec. IV, and the kernels themselves are derived in Sec. V in the form of constraints matrices.

IV. REDUCED PROBLEM HAMILTONIANS

The likelihood of finding low-excited states within the kernels of the operators $\hat{S}_q$ motivates the definition of reduced problem Hamiltonians that allow for the search of short vectors within such kernels. This formulation leverages the symmetries of cyclic and negacyclic lattices and leads to a more efficient search for low-excited states of the problem Hamiltonian, i.e., for short lattice vectors.

A lattice state $|\vec{n}\rangle$ is an eigenstate of the operator $\hat{S}_q = \sum_p U_{qp} \hat{N}_p$ with the corresponding eigenvalue $s_{\vec{n}}^q = \sum_p U_{qp} n_p$. The kernel of $\hat{S}_q$ is thus given by the span of all states $|\vec{n}\rangle$ with integer coefficients n_p that satisfy

$$\sum_{p=0}^{N-1} U_{qp} n_p = 0. \quad (7)$$

In both the cyclic and the negacyclic cases, the complex coefficients U_{qp} are of the form of phase factors and a constant factor $1/\sqrt{N}$ that has no influence on the solution of Eq. (7).

Since the general solution of linear algebraic equations is given by a linear combination of individual solutions, the characterization of the kernel of an operator $\hat{S}_q$ can be represented by all integer vectors $\vec{n} = (n_0, n_1, \dots, n_{N-1})^T$ that satisfy the vector equation

$$\vec{n} = A\vec{m}, \quad (8)$$

for an $(N \times M)$ -dimensional constraint matrix A , and any M -dimensional integer vector $\vec{m} = (m_0, m_1, \dots, m_{M-1})^T$, with $M < N$. That is, the solutions to Eq. (7) are given by a constraint matrix A , which relates the M degrees of freedom represented by any integer vector $\vec{m}$, to the vector of integers $\vec{n}$ according to Eq. (8). The analytical characterizations of the constraints matrices, i.e., the explicit solutions to Eq. (7), are derived in Sec. V.

While the problem Hamiltonian for an N -dimensional lattice is given in terms of N operators $\hat{N}_i$ with $\hat{H} = \sum_{ij} G_{ij} \hat{N}_i \hat{N}_j$, the characterization of the kernels of the operators $\hat{S}_q$ with associated constraints matrices A , can be exploited to represent the problem Hamiltonian with a reduced number of operators $\hat{N}_i$.

The eigenvalues of the problem Hamiltonian (equivalent to the length of lattice vectors) that lie within the kernel of $\hat{S}_q$ with the constraint matrix A are given by

$$\sum_{i,j=0}^{N-1} G_{ij} n_i n_j = \sum_{i,j=0}^{M-1} F_{ij} m_i m_j, \quad (9a)$$

where

$$F = A^\dagger G A. \quad (9b)$$

The reduced problem Hamiltonian

$$\hat{H} = \sum_{i,j=0}^{M-1} F_{ij} \hat{N}_i \hat{N}_j \quad (10)$$

thus represents the problem with the restriction to the kernel of $\hat{S}_q$, just like the original problem Hamiltonian formulation defined in Eq. (3). The reduction from N to M operators $\hat{N}_i$, however, implies a substantial reduction in the quantum resources required in an explicit implementation, such as qubit count and circuit depth. For example, the spectrum of the operators $\hat{N}_i$ can be represented with K qubits. In that case, comparing the same implementation with and without our method, the total number of qubits saved using our approach is $K \times (N - M)$. The value of $(N - M)$ can be as large as $N - 1$. It depends on the value of the lattice dimension N and the index of the principal operator q , as rigorously characterized in the next section. A concrete example is discussed in Sec. VI.

V. CHARACTERIZATION OF THE CONSTRAINT MATRIX

In this section, the constraints matrices A that lead to the formulation of reduced problem Hamiltonians [Eq. (10)] are

derived. First, the most general solution to Eq. (7) is characterized in Sec. V A in terms of the constraints matrices. That is, the kernels of all operators $\hat{S}_q$ are characterized.

These characterizations require a numerical method to find a solution. Therefore, in Sec. V B, another method for deriving explicit analytical solutions to Eq. (7) is described. These solutions yield constraints matrices that are used for explicitly representing reduced problem Hamiltonians with restrictions to subspaces within the kernels of the operators $\hat{S}_q$.

A. Characterization of the kernels

For lattices with cyclic symmetry, the kernel of an operator $\hat{S}_q^{(c)}$ is spanned by the states $|n_0, n_1, \dots, n_{N-1}\rangle$ with integers n_p that solve the explicit form

$$\vec{U}_q^{(c)} \vec{n} = 0 \quad (11a)$$

of Eq. (7) for cyclic lattices, with

$$\vec{U}_q^{(c)} = \begin{pmatrix} 1 & e^{-i\frac{2\pi}{N}q} & e^{-i\frac{2\pi}{N}2q} & \dots & e^{-i\frac{2\pi}{N}q(N-1)} \end{pmatrix}^T \quad (11b)$$

and $\vec{n} = (n_0, n_1, \dots, n_{N-1})^T$. Therefore, characterizing the orthogonal space to the vector $\vec{U}_q^{(c)}$ over the integers is equal to characterizing the kernel of the operator $\hat{S}_q^{(c)}$.

The following characterization refers to the case where the greatest common divisor (gcd) of the dimension N and the index q is unity, i.e., $\gcd(N, q) = 1$. In this case, the linear space spanned by the elements of $\vec{U}_q^{(c)}$ over the integers (the complementary subspace to the orthogonal space) has dimension $\varphi(N)$ [37]. The function $\varphi(N)$ is Euler's *totient function*, which is defined as the number of integers between 1 and $N - 1$ coprime with N [e.g., for $N = 6$, $\varphi(6) = 2$ since only 1 and 5 are coprime with 6]. The quantity $N - \varphi(N)$ is also known as the *cototient function*.

Because the space spanned by $\vec{U}_q^{(c)}$ over the integers has dimension $\varphi(N)$, there are $\varphi(N)$ independent exponential components in the vector $\vec{U}_q^{(c)}$, and all other exponentials can be written as their integer linear combination [37,38]. Explicitly, the relation is given by

$$\begin{pmatrix} e^{-i\frac{2\pi}{N}q(\varphi(N))} \\ e^{-i\frac{2\pi}{N}q(\varphi(N)+1)} \\ \vdots \\ e^{-i\frac{2\pi}{N}q(N-1)} \end{pmatrix} = C \begin{pmatrix} 1 \\ e^{-i\frac{2\pi}{N}q} \\ \vdots \\ e^{-i\frac{2\pi}{N}q(\varphi(N)-1)} \end{pmatrix}, \quad (12)$$

with the matrix C being an integer matrix of size $(N - \varphi(N)) \times \varphi(N)$.

Therefore, Eq. (11a), for the case of $\gcd(N, q) = 1$, can be rewritten as

$$\begin{pmatrix} 1 & e^{-i\frac{2\pi}{N}q} & \dots & e^{-i\frac{2\pi}{N}q(\varphi(N)-1)} \end{pmatrix} (I | C^T) \vec{n} = 0, \quad (13a)$$

where I is the identity matrix of size $\varphi(N) \times \varphi(N)$ and $(I | C^T)$ stands for a flat matrix concatenating I and C^T . The phase factors $\{1, \exp(-i\frac{2\pi}{N}q), \dots, \exp(-i\frac{2\pi}{N}q(\varphi(N) - 1))\}$ are linearly independent over the integers. Equation (18) is thus satisfied if and only if

$$(I | C^T) \vec{n} = \vec{0}. \quad (13b)$$

The solution of Eq. (13b) in terms of the N -dimensional integer vector $\vec{n}$ can be found from the Hermite normal form

(see Chapter 2 of Ref. [39]) of the matrix $(I | C^T)$. Given an integer matrix X , there is a unique matrix Y in the Hermite normal form, in the form of $Y = XU$, where U is a unimodular matrix, i.e., an integer matrix whose determinant is ± 1 . The matrix Y is upper triangular, that is, $Y_{ij} = 0$, for $j < i + N - \varphi(N)$, and $Y_{ij} < Y_{ii}$, for $j > i + N - \varphi(N)$. The Hermite normal form can be found numerically in polynomial time (see Chapter 2 of Ref. [39]).

The Hermite normal form

$$Z = (I | C^T)U \quad (14)$$

of the matrix $(I | C^T)$ defines a matrix Z whose first $N - \varphi(N)$ columns contain only zeros. We denote the first $N - \varphi(N)$ columns of the matrix U by the submatrix A .

Given the matrix A , the solution to Eq. (13b) is given by Eq. (8), with $\vec{n} = A\vec{m}$ (see Proposition 2.4.9 of Ref. [39]), for any $(N - \varphi(N))$ -dimensional integer vector $\vec{m} = (m_0, m_1, \dots, m_{N-\varphi(N)-1})^T$. That is, the matrix A fully characterizes the orthogonal space of the vector $\vec{U}_q^{(c)}$. Therefore, the kernel of the corresponding operator $\hat{S}_q^{(c)}$ [for the case of $\gcd(N, q) = 1$] is given by all states $|\vec{n}\rangle$ such that $\vec{n} = A\vec{m}$, for an arbitrary integer vector $\vec{m}$ and the constraint matrix A .

The above characterization is simply extended to cyclic operators $\hat{S}_q^{(c)}$ for which the greatest common divisor of N and q is greater than unity (as explained in Appendix A) as well as for the negacyclic operators $\hat{S}_q^{(n)}$, as explained in the following. For all cases, however, the solution is fully determined by a constraint matrix A , which is used to derive reduced problem Hamiltonians according to Eq. (10) for the specified kernels.

For lattices with negacyclic symmetry, the defining equation of the kernels of the operators $\hat{S}_q^{(n)}$ is

$$\sum_{p=0}^{N-1} n_p \exp\left(-i\frac{\pi}{N}p(2q+1)\right) = 0, \quad (15)$$

[a special case of Eq. (7)]. Here, let us assume $q = 0$ for convenience, whereas the general case $q > 0$ is handled in Appendix A. We proceed as in the case of cyclic lattices, with the difference that there are $\varphi(2N)$ independent exponential components. Again, all other exponentials can be written as their integer linear combination:

$$\begin{pmatrix} e^{-i\frac{\pi}{N}(\varphi(2N))} \\ e^{-i\frac{\pi}{N}(\varphi(2N)+1)} \\ \vdots \\ e^{-i\frac{\pi}{N}(N-1)} \end{pmatrix} = C \begin{pmatrix} 1 \\ e^{-i\frac{\pi}{N}} \\ \vdots \\ e^{-i\frac{\pi}{N}(\varphi(2N)-1)} \end{pmatrix}, \quad (16)$$

with the matrix C being an integer matrix of size $(N - \varphi(2N)) \times \varphi(2N)$. Then, we can apply the same procedure to find the Hermite normal form, and hence the kernel. Now, the kernel has dimension $N - \varphi(2N)$ rather than $N - \varphi(N)$.

B. Explicit characterization of subspaces within the kernels

The characterization of the kernels described in Sec. V A requires the use of numerical methods in order to find the constraint matrix A that represents the restriction to a specific kernel. In this section, however, the explicit analytical characterization of subspaces within the kernels is described.

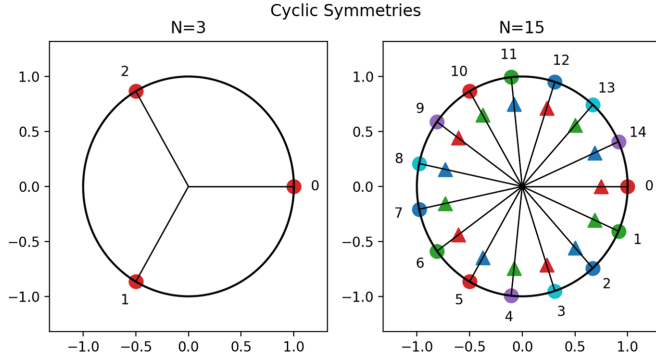


FIG. 3. Schematic solutions of Eq. (11a) for the case of $N = 3$ on the left and for $N = 15$ on the right. On the left, a unit circle with three equally distributed phases across it is depicted. All three phases are marked with a circle, meaning there is only one solution. All three circles have the same color (red), meaning their corresponding integer coefficients must be equal. On the right, next to each phase there are two shapes—circles and triangles, meaning two sets of solutions are depicted. For each solution set separately, all integer coefficients corresponding to the phases marked with shapes with the same color must be equal.

These are used for explicitly formulating reduced problem Hamiltonians restricted to these subspaces.

While the explicit characterization of these subspaces will turn out a bit cumbersome, it can be understood to some extent by the observation that an equation $\sum_p n_p \exp(i\phi_p) = 0$ with the phases ϕ_p evenly distributed over the unit circle has nontrivial solutions for the integer coefficients n_p .

If there are N evenly distributed phases, i.e., $\phi_p = \frac{2\pi}{N}p$, and N is a prime number, then the general solution of the equation $\sum_p n_p \exp(i\frac{2\pi}{N}p) = 0$ reads $n_0 = n_1 = \dots = n_{N-1}$ with only one free integer to choose. In that case, the constraint matrix A is $(N \times 1)$ dimensional and it reads $A_{i0} = 1$, such that the solution is given by $\vec{n} = (1, 1, \dots, 1)^T m$ for an arbitrary integer m .

If, however, N is a product of two prime numbers Q and R (i.e., $N = QR$), then there are at least two sets of independent solutions. The first reads $n_p = n_{p+Q} = n_{p+2Q} = \dots = n_{p+Q(R-1)}$, with Q free integer parameters $n_0, \dots, n_{Q-1}$, and the associated constraint matrix is the $(N \times Q)$ -dimensional block matrix $A_{ij} = \delta_{i \% Q, j}$ with the Kronecker delta $\delta_{i,j}$ and the modulus operation $\%$. The second solution is $n_p = n_{p+R} = \dots = n_{p+R(Q-1)}$, with R free integer parameters $n_0, \dots, n_{R-1}$, and the associated constraint matrix is $(N \times R)$ dimensional such that $A_{ij} = \delta_{i \% R, j}$.

An example is schematically given in Fig. 3 for the cases of $N = 3$ as a prime number and for $N = 15$ as a product of prime numbers. In both plots, N equally distributed phases $\frac{2\pi}{N}p$ of the unit circle are shown, with the index p next to each. Solutions to the equation $\sum_p n_p \exp(i\frac{2\pi}{N}p) = 0$ are schematically indicated by the colored shapes attached to each phase. Each shape represents one solution, and all coefficients having the same color within the solution need to be equal.

For the case of $N = 3$ on the left, there is only one solution since 3 is a prime number, and all the coefficients must be equal ($n_0 = n_1 = n_2$). For the case of $N = 15$ on the right, two sets of solutions indicated by circles and triangles are

depicted. For each set, all integer coefficients n_j with the same color must be equal, e.g., $n_0 = n_5 = n_{10}$ for the circles and $n_0 = n_3 = n_6 = n_9 = n_{12}$ for the triangles.

The generalization for any dimension N stems from the fact that every positive integer can be decomposed uniquely into a product of prime factors. Solutions to Eq. (7) and therefore the characterization of the subspaces within the kernels will depend on the prime factors p of the lattice dimension N . In the simplest case, each prime factor p has an associated class of states, with an associated constraint matrix. The identified subspace of the kernel is spanned by all these classes of states, and the reduced problem Hamiltonian with the associated constraint matrix thus represents the problem Hamiltonian with restriction to the subspace.

This idea generalizes directly to more complicated cases where prime factors of different functions of N are taken into account. The multiplicity of the prime coefficients for any of the cases has no influence on the structure of the kernels.

The explicit characterization of the subspaces within the kernels of each of the operators is rather technical, and the reader who is interested in the derivation that relies on number theory is referred to Appendix B. Any reader who is happy to skip the derivation can find the classification in the following, where the cyclic case is described in Sec. VB 1 and the negacyclic case in Sec. VB 2.

1. Cyclic case

The explicit form of Eq. (7) for lattices with cyclic symmetry is given by Eq. (11a). The classes of states spanning the subspaces within the kernel depend on the dimension N of the lattice and on its greatest common divisor with the index q of the operator $\hat{S}_q^{(c)}$, that is, $K := \gcd(N, q)$. Five cases should be distinguished:

- (1) $q = 0$;
- (2) $K = 1$ and N is odd or some power of 2;
- (3) $K = 1$ and N is even, but not a power of 2;
- (4) $K > 1$ and $\frac{N}{K}$ is odd or some power of 2;
- (5) $K > 1$ and $\frac{N}{K}$ is even, but not a power of 2.

For each case, the associated constraint matrix (matrices) A is (are) explicitly characterized. The subspace is spanned by all states $|\vec{n}\rangle$ for which $\vec{n} = A\vec{m}$, and the reduced problem Hamiltonian is given by Eq. (10) for each constraint matrix. The constraints matrices read

- (1) The constraint matrix A^1 is $(N \times N - 1)$ dimensional with elements

$$A_{ij}^1 = \delta_{i,j} - \delta_{i,N-1}, \quad (17)$$

where $\delta_{i,j}$ is the Kronecker delta (see Theorem B1 in Appendix B 1).

- (2) Each prime factor p of N has an associated $(N \times \frac{N}{p})$ -dimensional constraint matrix $A^{2,p}$ with elements:

$$A_{ij}^{2,p} = \delta_{i \% \frac{N}{p}, j}, \quad (18)$$

where $\%$ is the modulo operator (see Theorem B3 in Appendix B 1). The associated subspace is spanned by all states $|\vec{n}\rangle$ that obey $\vec{n} = A^{2,p}\vec{m}$ for any arbitrary integer vector $\vec{m}$ and for all matrices $A^{2,p}$ according to all prime coefficients p of the lattice dimension N .

(3) Each prime factor $p > 2$ of $\frac{N}{2K}$ has an associated constraint matrix $A^{3,p}$ with dimensions $(N \times (N - \frac{N}{2Kp}(p-1)))$. It reads

$$A_{ij}^{3,p} = \delta_{ij} + \sum_{k=0}^{K-1} \delta_{i+(k+\frac{1}{2})\frac{N}{K}-N,j} + (-1)^{[j]} \left(\delta_{i\%(\frac{N}{2Kp})+k\frac{N}{K},j} - \delta_{i\%(\frac{N}{2Kp})+(k+\frac{1}{2})\frac{N}{K},j} \right) - \sum_{l=0}^{K-2} \delta_{i+(l+1)\frac{N}{K}-N,j}, \quad (19)$$

where $[j]$ stands for the floor of the quotient of $(j + \frac{N}{2K} - N)$ and $\frac{N}{2Kp}$ (see Theorem B9 in Appendix B 3).

The associated subspace is spanned by all states $|\vec{n}\rangle$ for which $\vec{n} = A\vec{m}$ for all constraints matrices $A^{2,p}$ and $A^{3,q}$ according to all prime factors p of N and prime factors q of $\frac{N}{2K}$, as defined in Eqs. (18) and (19), respectively. Each constraint matrix is associated with a reduced problem Hamiltonian according to Eq. (10).

(4) Each prime factor p of $\frac{N}{K}$ has an associated constraint matrix $A^{4,p}$ with dimensions $(N \times (N - \frac{N}{Kp}(p-1)))$, and it reads

$$A_{ij}^{4,p} = \delta_{ij} + \delta_{i\%(\frac{N}{Kp}),j} + \sum_{k=1}^{K-1} \delta_{(k\frac{N}{K}+i)\%(\frac{N}{Kp}),j} - \delta_{k\frac{N}{K}+i-N,j} \quad (20)$$

(see Theorem B4 in Appendix B 1).

(5) The associated subspace is spanned by all states $|\vec{n}\rangle$ for which $\vec{n} = A\vec{m}$ for all constraints matrices $A^{3,p}$ and $A^{4,q}$ according to all prime factors p of $\frac{N}{2K}$ and prime factors q of $\frac{N}{K}$, as defined in Eqs. (19) and (20), respectively (see Theorem B4 in Appendix B 1 and Theorem B9 in Appendix B 3). Each constraint matrix is associated with a reduced problem Hamiltonian according to Eq. (10).

2. Negacyclic case

In the case of negacyclic symmetry, the explicit form of Eq. (7) reads

$$\sum_{p=0}^{N-1} n_p \exp\left(-i\frac{\pi}{N}p(2q+1)\right) = 0, \quad (21)$$

so the kernel of the operators $\hat{S}_q^{(n)}$ is spanned by all states $|n_0, n_1, \dots, n_{N-1}\rangle$ with integer coefficients n_p that solve Eq. (21).

Solutions for the general case are based on the solution for the simplest case for the operator $\hat{S}_0^{(n)}$ with the operator index $q = 0$. Equation (21) then reduces to

$$\sum_{p=0}^{N-1} n_p \exp(i\omega_p) = 0, \quad (22a)$$

with the phases $\omega_p = -\frac{\pi}{N}p$ evenly distributed in the bottom half of the unit circle.

If the dimension N is a prime number greater than 2, the solution is identified in terms of the solution to the equation $\sum_p n_p \exp(-i\frac{2\pi}{N}p) = 0$ with evenly distributed phases among the whole unit circle as discussed above. This is

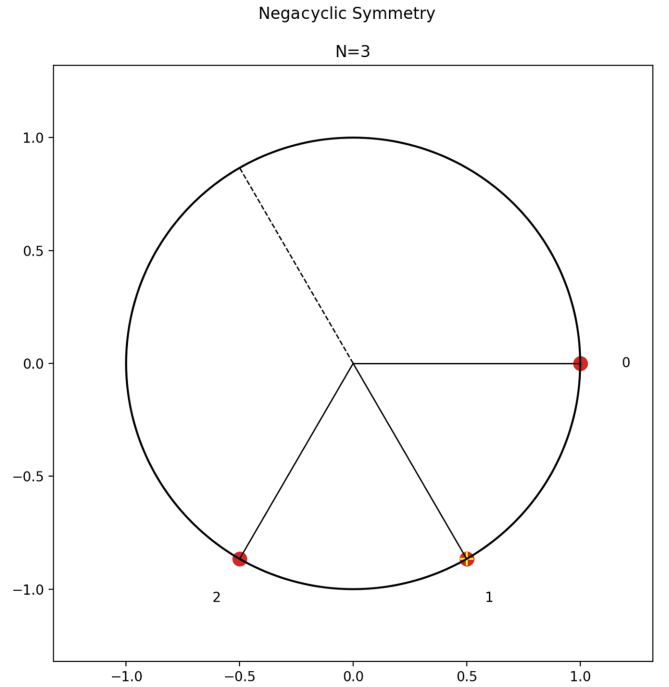


FIG. 4. A schematic solution for Eq. (22a), with $N = 3$. Three phases are equally distributed in the bottom half of the unit circle. Next to each phase, a red circle is drawn, indicating that the integer coefficient associated with the phases must be equal in their absolute value. The yellow cross within the circle associated with the phase indexed 1 indicates the negation of corresponding coefficient, i.e., $n_1 \rightarrow -n_1$, and the addition of π radians to the corresponding phase. The flip of the phase, which is indicated by the dashed black line, results in the same distribution of phases across the entire unit circle as depicted in Fig. 3 for the cyclic case.

done by adding π to all phases ω_p with odd index p in Eq. (28) and negating the corresponding coefficients. That is, $n_p \exp(i\omega_p) = -n_p \exp(i(\omega_p + \pi))$ for all the integer coefficients with an odd index. Equation (28) can then be rewritten as

$$\sum_{p=0}^{N-1} y_p \exp\left(-i\frac{2\pi}{N}p\right), \quad (22b)$$

where

$$y_p = \begin{cases} n_{2p}, & \text{if } p \leq \frac{N-1}{2} \\ -n_{2p-N}, & \text{if } p \geq \frac{N+1}{2}. \end{cases} \quad (22c)$$

Based on the cyclic case with a prime N , the solution to the above equation in the integer coefficients n_p has only one free parameter (e.g., n_0) and it reads $n_0 = -n_1 = n_2 = -n_3 = \dots = -n_{N-2} = n_{N-1}$.

The solution can be depicted graphically and an example for the case of $N = 3$ is presented in Fig. 4, with three roots of unity evenly distributed among the bottom half of the unit circle. By negating the only odd-indexed coefficient n_1 , its corresponding phase factor is reflected across the unit circle as indicated by the dashed black line. After the negation, the phases are evenly distributed among the unit circle; thus, the solution requires all integer coefficient to have the same value. The negation is depicted with the yellow cross

within the circle associated to the integer coefficient n_1 , and all circles have the same color as they are equal in absolute value.

As in the cyclic case, the above characterization can be extended to solutions of Eq. (22a) for general lattice dimension N . Each prime factor of N , which is greater than 2, has an associated class of states, and all classes corresponding to all prime factors p span the associated subspace within the kernel of $\hat{S}_0^{(n)}$.

The characterization of subspaces within the kernel of a general negacyclic operator $\hat{S}_q^{(n)}$ depends on the dimension of the lattice N and on the greatest common divisor of $2N$ and $2q + 1$ denoted by L , i.e., $L := \gcd(2N, 2q + 1)$. Four cases should be distinguished:

- (1) $N = 2^l$ for some positive integer l ;
- (2) $L = 1$ and N is not some power of 2;
- (3) $L > 1$ and $N = 2^l L$ for some positive integer l ;
- (4) $L > 1$ and $N \neq 2^l L$ for any positive integer l .

As in the cyclic case (Sec. VB 1), explicit constraints matrices are characterized for each case. The associated subspace is spanned by all states $|\vec{n}\rangle$ that obey $\vec{n} = A\vec{m}$ for all the associated constraints matrices, and for an arbitrary integer vector $\vec{m}$. The reduced problem Hamiltonian associated with each constraint matrix is given by Eq. (10). The constraints matrices are characterized as follows:

(1) The constraint matrix is a zero matrix such that the subspace (and the kernel) equals the zero state $|0, 0, \dots, 0\rangle$ (see Theorem B5 in Appendix B 2).

(2) Each prime factor $p > 2$ of N has an associated constraint matrix $A^{II,p}$ with dimensions $(N \times \frac{N}{p})$ and with elements

$$A_{ij}^{II,p} = (-1)^{\lfloor \frac{i}{N} \rfloor} \delta_{i \% \frac{N}{p}, j}, \quad (23)$$

where $\lfloor \cdot \rfloor$ is the floor operator (see Theorem B7 in Appendix B 2).

(3) The constraint matrix A^{III} has dimensions $(N \times (N - \frac{N}{L}))$ and its elements are given by

$$A_{ij}^{III} = \delta_{i,j} + \sum_{k=1}^{\frac{L-1}{2}} \delta_{i-(k-\frac{1}{2})\frac{N}{L}, j} - \delta_{i-k\frac{N}{L}, j} \quad (24)$$

(see Theorem B8 in Appendix B 2).

(4) Two types of constraints matrices are defined. First, for each prime factor p of $\frac{2N}{L}$, a constraint matrix $A^{IV,p}$ with dimensions $(N \times (\frac{2N}{L} - \frac{2N}{Lp}))$ is defined according to

$$A_{ij}^{IV,p} = \delta_{i \% \frac{2N}{Lp}, j} + \sum_{k=1} \delta_{i \% (\frac{2N}{Lp}) + k\frac{2N}{L}, j} - \delta_{i+k\frac{2N}{L}, j}. \quad (25a)$$

Second, for each prime factor $q > 2$ of $\frac{N}{L}$, a constraint matrix $A^{V,q}$ with dimensions $(N \times \frac{N}{L} - \frac{N}{Lq})$ is given by

$$A_{ij}^{V,q} = \delta_{i,j} - \sum_{k=1} \delta_{i+k\tilde{N}, j} + \sum_{l=0} \delta_{i+(l+\frac{1}{2})\tilde{N}, j} + (-1)^{\lfloor \frac{l}{N} \rfloor} \left(\delta_{i \% (\frac{N}{Lq}) + l\tilde{N}, j} - \delta_{i \% (\frac{N}{Lq}) + (l+\frac{1}{2})\tilde{N}, j} \right), \quad (25b)$$

where $\tilde{N}$ is a shorthand notation for $\frac{2N}{L}$.

The associated subspace within the kernel is spanned by all states $|\vec{n}\rangle$ that obey the relation $\vec{n} = A^{IV,p}\vec{m}$ or $\vec{n} = A^{V,q}\vec{m}$ for an arbitrary vector of integers $\vec{m}$, for all prime factors p of $\frac{2N}{L}$, and all prime factors q of $\frac{N}{L}$ (see Theorem B10 in Appendix B 4). Each constraint matrix has its associated reduced problem Hamiltonian according to Eq. (10).

VI. BENCHMARKING WITH THE VARIATIONAL QUANTUM EIGENSOLVER

The reduced problem Hamiltonian $\hat{H} = \sum_{ij} F_{ij} \hat{N}_i \hat{N}_j$ defined in Eq. (10) represents the problem Hamiltonian $\hat{H} = \sum_{ij} G_{ij} \hat{N}_i \hat{N}_j$ defined in Eq. (3), with the restriction to the kernel of some operator $\hat{S}_q$ (or to a subspace within that kernel), according to the constraint matrix A for which $F = A^\dagger G A$. The reduction in the number of operators $\hat{N}_i$ in the reduced problem Hamiltonian results in a substantial reduction in the resources needed for searching for low-excited states of the Hamiltonian in any practical implementation. This method is now benchmarked with the variational quantum eigensolver algorithm [31].

A. The variational quantum eigensolver for the problem hamiltonian

The VQE is a hybrid quantum-classical algorithm. Its input is some Hamiltonian $\hat{H}$ and its output is a quantum state $|\Psi\rangle$ that is highly probable to be a low-excited state of the Hamiltonian $\hat{H}$ [40].

The quantum mechanical component of the algorithm is the preparation of a parametrized quantum state $|\Psi\rangle$ and a measurement scheme that allows for the evaluation of the expectation value $\langle \Psi | \hat{H} | \Psi \rangle$ of the problem Hamiltonian $\hat{H}$ with respect to the prepared quantum state $|\Psi\rangle$. The classical part consists of a variational analysis over the parameters of the quantum state $|\Psi\rangle$ with the goal of minimizing the expectation value $\langle \Psi | \hat{H} | \Psi \rangle$.

In any practical implementation, the states $|\Psi\rangle$ are realized with registers of qubits, so that the problem Hamiltonians given in Eqs. (3) and (10) need to be defined in terms of qubit operators. With the construction

$$\hat{N}_i = -2^{K-1} + \sum_{j=0}^{K-1} \hat{Z}_{ij} 2^j \quad (26)$$

in terms of the Pauli-Z operator for K different qubits [19], the operator $\hat{N}_i$ has an integer spectrum ranging from -2^{K-1} to $2^{K-1} - 1$. With d registers of K qubits each, one can thus realize a problem Hamiltonian defined in Eq. (3) for a d -dimensional lattice or a reduced problem Hamiltonian as defined in Eq. (10) with a constraint matrix of size $(N \times d)$ for a lattice dimension $N > d$.

A Hamiltonian of the form

$$\hat{H} = \sum_{ij} B_{ij} \hat{N}_i \hat{N}_j \quad (27a)$$

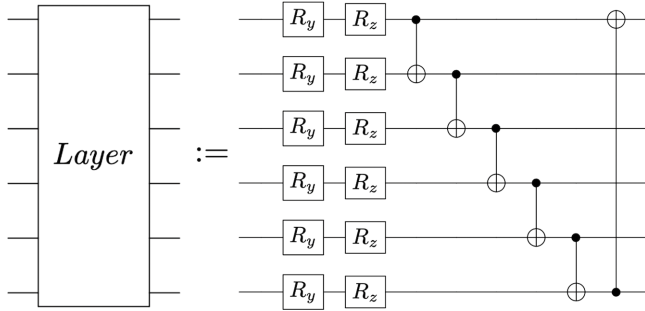


FIG. 5. One layer of the variational quantum circuit for circuits with six qubits. The layer contains applications of the ry and rz single-qubit gates on all qubits, followed by circular ladder of entangling CNOT gates.

can therefore be explicitly realized in terms of qubit operators with

$$\hat{H} = \sum_{ij} B_{ij} \left(2^K + \sum_{pq} 2^{p+q} \hat{Z}_{ip} \hat{Z}_{jq} - 2^{K-1} \sum_p (\hat{Z}_{ip} + \hat{Z}_{jp}) 2^p \right). \quad (27b)$$

In order to avoid the convergence of the VQE to the zero state $|\vec{0}\rangle$ that is the trivial ground state of Hamiltonians of the form in Eqs. (3) and (10), an additional penalty term, $G_{00} |\vec{0}\rangle \langle \vec{0}|$, is added to the Hamiltonian. Thus, the eigenvalue corresponding to the zero state $|\vec{0}\rangle$ are the G_{00} component of the Gram matrix instead of the trivial ground state eigenvalue 0.

B. Numerical methods

The applications of the VQE for the search for low-excited states of problem Hamiltonians [Eq. (3)] and the corresponding reduced problem Hamiltonians [Eq. (10)] are compared for 200 six-dimensional negacyclic lattices. The implementations for the problem Hamiltonians contain six quantum registers with three qubits each. For the reduced problem Hamiltonians, d registers of three qubits are used, such that $d < N$ and is determined according to the associated constraint matrix A with dimensions $(N \times d)$. The analysis is made such that the spectrum of the number operators in both implementations is equal.

The explicit quantum circuits for both implementations are chosen to be standard three-layer circuits followed by measurements. A scheme of one layer for a quantum circuit with six qubits is depicted in Fig. 5. Each layer consists of parametrized ry and rz gates applied to all qubits, followed by a circular ladder of CNOT gates [40]. The algorithms are emulated with the noiseless quantum simulator *default.qubit* of the PENNYLANE package [41].

C. Examples of reduced qubit count and circuit depth

In order to consolidate the understanding of the proposed framework, consider two specific six-dimensional negacyclic

lattices with bases B and C , which are generated from the two normalized lattice vectors

$$\vec{b} = \begin{bmatrix} 0.010 \\ -0.45 \\ -0.50 \\ -0.67 \\ -0.36 \\ -0.18 \end{bmatrix}, \quad \vec{c} = \begin{bmatrix} -0.12 \\ -0.34 \\ 0.087 \\ 0.51 \\ 0.56 \\ 0.53 \end{bmatrix}, \quad (28a)$$

respectively, represented with two significant digits. That is, the basis vectors of B (C) are given by $\{\vec{b}, \Gamma\vec{b}, \dots, \Gamma^5\vec{b}\}$ ($\{\vec{c}, \Gamma\vec{c}, \dots, \Gamma^5\vec{c}\}$). The largest eigenvalue of the Gram matrix G for both lattices is the zeroth eigenvalue g_0 . Therefore, the corresponding operator $\hat{S}_0^{(n)}$ is the principal operator, and the search for low-excited states is limited to a subspace within its kernel.

The subspace within the kernel of the operator $\hat{S}_0^{(n)}$ is characterized according to case (II) in Sec. VB 2 since the greatest common divisor of $2N$ and $2q + 1$ equals unity (and 6 is not a power of 2). The corresponding constraints matrices are given by Eq. (23), and because 3 is the only prime factor greater than 2 of $N = 6$, only one class of states spans the kernel (there is only one constraint matrix). This class of states is explicitly given by $|m_0, m_1, -m_0, -m_1, m_0, m_1\rangle$, with the free integer coefficients m_0, m_1 .

The explicit constraint matrix A that relates the free integer vector $\vec{m} = (m_0, m_1)^T$ to the six-dimensional integer coefficient vector $\vec{n}$ with $\vec{n} = A\vec{m}$ is explicitly given by

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ -1 & 0 \\ 0 & -1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad (29)$$

This results in the 2×2 matrix $F = A^\dagger G A$ according to Eq. (9b). Therefore, the corresponding eigenvalue of a lattice state in the kernel of $\hat{S}_0^{(n)}$ (equivalently the length of the corresponding lattice vector) is given by

$$\sum_{ij=0}^1 F_{ij} m_i m_j + G_{00} \delta_{0,m_i} \delta_{0,m_j}, \quad (30)$$

including the penalty term for the zero state.

One layer of the quantum circuit used in the VQE for the reduced problem Hamiltonian is depicted in Fig. 5. The full circuit contains three layers followed by a measurement of all qubits. Because there are only two degrees of freedom (the constraint matrix has only two columns), the circuit contains only two quantum registers with three qubits each. The top three qubits form one register, as well as the bottom three, and upon measurement of their values, the integer coefficients m_0 and m_1 are determined, respectively.

The output of the VQE for the reduced problem Hamiltonian for the lattice given by the basis B is the quantum state $|1, 0\rangle$ and the corresponding eigenvalue (lattice vector length) is 0.21. The output of the VQE for the problem Hamiltonian, however, which uses a quantum circuit with the same structure

as in Fig. 5 but with 18 qubits, results in the lattice state $|2, -1, -1, 1, 0, 1\rangle$ with the corresponding eigenvalue 0.86.

The ratio between the vector lengths resultant from the VQE for the reduced problem Hamiltonian and the problem Hamiltonian is denoted by λ . A value of $\lambda < 1$ represents a lattice for which the VQE for the reduced problem Hamiltonian results in a lower excited state than the VQE for the problem Hamiltonian. This is the case for the lattice given by the basis B , with a value of $\lambda = 0.24$.

For the lattice given by the basis C , the VQE for the reduced problem Hamiltonian results in the state $|0, 1\rangle$ with a corresponding vector length of 0.70, and the VQE for the problem Hamiltonian results in the lattice state $|1, -1, 1, 0, -1, 1\rangle$ with the corresponding vector length of 0.91. The value of λ for this lattice is thus 0.77, which is smaller than unity as well, indicating that the VQE for the reduced problem Hamiltonian results in a shorter lattice vector.

For both lattices, the VQE for the reduced problem Hamiltonian results in lower excited states than the one for the problem Hamiltonian, even though the search space of the former is restricted to the kernel of $\hat{S}_0^{(n)}$, while for the latter the search space consists of all lattice states. This is possibly an outcome of a more complex optimization landscape in the case of the full problem Hamiltonian compared to the case of the reduced problem Hamiltonian. The more complicated optimization landscape might increase the risk of the classical optimization to get stuck in a local optima rather than converging to the global minimum.

The use of only six qubits for the reduced problem Hamiltonian implementation instead of 18 for the problem Hamiltonian with a shorter circuit depth (24 instead of 60), while resulting lower excited states, encapsulates the key benefits of our work. That is, the framework eases the search of the algorithm by restricting it to a small subspace that is very likely to contain a low-excited state that corresponds to a short lattice vector, and as a consequence, the quantum algorithm benefits from a significant reduction in qubit count and circuit depth.

D. Statistics of the results

A histogram that summarizes the ratio between the length of the output states of the VQE for the reduced problem Hamiltonians and for the problem Hamiltonians, i.e., the values of λ , for all lattices examined is presented in Fig. 6. All bars to the left of the dashed black line indicate cases where the ratio is smaller than unity. This is the case for 130 out of the 200 lattices, where the median value of λ is 0.63. That is, for the majority of lattices, the VQE for the reduced problem Hamiltonian results in shorter vectors than the VQE for the full problem Hamiltonian. As argued earlier (Sec. VIC), the main reason for this is likely a better behaved optimization landscape that allows the former case to converge to a global minimum more easily.

The number of qubits used for the VQE implementation of the problem Hamiltonians is 18, for all lattices, while the number of qubits for the implementations of the reduced problem Hamiltonians depends on the index q of the operator $\hat{S}_q^{(n)}$. For example, in the two cases examined in Sec. VIC, the search is

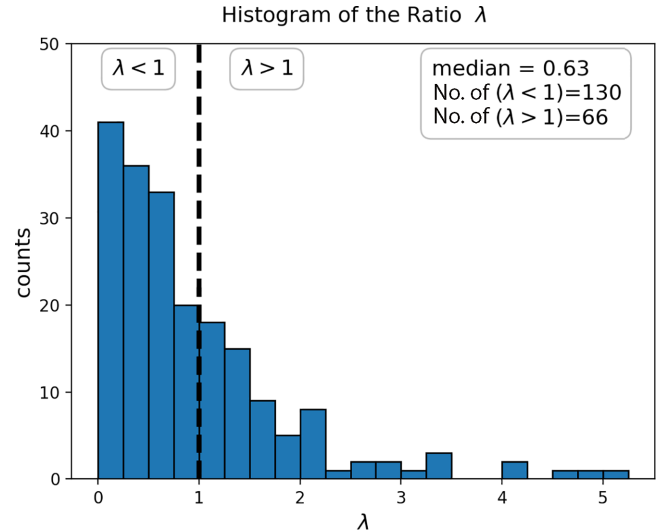


FIG. 6. Histogram of the ratio between the energy values of the outputs of the VQE algorithms for the reduced problem Hamiltonians and the full problem Hamiltonians. Two hundred lattices are examined. Bars to the left of the dashed black line indicate lattices for which the VQE for the reduced problem Hamiltonian results in a lower excited state than the VQE for the full problem Hamiltonian. This is the case for 130 out of the 200 lattices.

restricted to a subspace within the kernel of the operator $\hat{S}_0^{(n)}$, and six qubits are used for the implementation of the VQE for the reduced problem Hamiltonians. The average number of qubits used for the implementations of the reduced problem Hamiltonians is 7.74. It requires on average 2.33 times fewer qubits than the VQE for the problem Hamiltonian. Overall, the application of our framework to the VQE for the search of short lattice vectors results in shorter vectors compared to the original implementation with fewer qubit counts.

VII. OUTLOOK

While symmetries are routinely exploited in physics to simplify computational problems, there is the common belief that symmetries of lattices are not beneficial for the shortest-vector problem and its variants. This might be true even with access to ideal quantum hardware that allows for unlimited scaling of qubit and gate counts. As long as an increase in quantum resources is an actual bottleneck, however, the present work shows that the exploitation of symmetries can provide a gain in efficiency that ultimately makes a problem solvable.

The ability to break down an original SVP problem into several smaller SVP problems is independent of whether solutions are sought by classical or quantum mechanical means. The techniques derived in this paper can thus find applications in a broad range of classical lattice-reduction algorithms, such as the Lenstra-Lenstra-Lovász algorithm [42] and its variants. Because the proposed framework can be incorporated into both quantum and classical algorithms, it appears particularly promising for hybrid schemes that integrate quantum and classical components.

The availability of fault-tolerant application-scale quantum devices [43] will open a new frontier in scientific computation.

Efficient encoding of lattice-based models into Hamiltonians is therefore expected to play a central role in quantum numerical methods. We believe our method applies to lattice-based physical models with cyclic (negacyclic) translational symmetry, whose interaction matrix is diagonalized by the Fourier transform [Eq. (1)]. This is the case, for example, in a classical lattice Coulomb gas of integer charges. This model is dual to the Villain form of the two-dimensional XY model—a non-trivial model exhibiting topological defects [44,45]. Finding further physical models that can benefit from our method is a promising direction for future work.

ACKNOWLEDGMENT

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC), Grant No. EP/Y004477/1.

APPENDIX A: EXTENSION OF THE CHARACTERIZATION OF THE KERNELS

In Sec. VA, the exact characterization of the kernels is given, for the case of cyclic lattices where the greatest common divisor of the lattice dimension N and the index q , denoted by K [i.e., $K := \gcd(N, q)$] is unity. In the following, the extensions of this characterization for further cyclic and negacyclic cases are described. First, the extension to cyclic cases with $K > 1$ is given, followed by the extension to the negacyclic cases with the index $q > 0$.

For lattices with cyclic symmetry, the kernel of the corresponding operator $\hat{S}_q^{(c)}$ is spanned by all lattice states $|\vec{n}\rangle$ with integer coefficients n_p that satisfy

$$\sum_{p=0}^{N-1} n_p \exp\left(-i\frac{2\pi}{N}qp\right) = 0, \quad (\text{A1})$$

a special case of Eq. (7).

For cases with $K > 1$, an effective dimension is defined as $\tilde{N} = \frac{N}{K}$ and an effective coefficient as $\tilde{q} = \frac{q}{K}$ such that $\gcd(\tilde{N}, \tilde{q}) = 1$ by definition. Equation (A1) reduces to

$$\sum_{l=0}^{\tilde{N}-1} y_l \exp\left(-i\frac{2\pi}{\tilde{N}}\tilde{q}l\right) = 0, \quad (\text{A2a})$$

where

$$y_l := \sum_{k=0}^{K-1} n_{l+k\tilde{N}}. \quad (\text{A2b})$$

The solution in terms of the coefficients y_l is given by the method described in Sec. VA, and a direct substitution of the integers n_p gives the solution that can be expressed in terms of a constraint matrix.

For lattices with negacyclic symmetry, since the rank is $\varphi(2N)$, we rewrite the exponential terms in Eq. (15) as

$$\begin{pmatrix} 1 \\ e^{-i\frac{2\pi}{2N}(2q+1)} \\ \vdots \\ e^{-i\frac{2\pi}{2N}(N-1)(2q+1)} \end{pmatrix} = D \begin{pmatrix} 1 \\ e^{-i\frac{2\pi}{2N}} \\ \vdots \\ e^{-i\frac{2\pi}{2N}(\varphi(2N)-1)} \end{pmatrix}, \quad (\text{A3})$$

with the matrix D being an integer matrix of size $N \times \varphi(2N)$. Note that D^T is the counterpart of $(I | C^T)$ in Eq. (13b). Then, we can apply the same procedure to find the Hermite normal form, and hence the kernel. Now, the kernel has dimension $\geq N - \varphi(2N)$.

APPENDIX B: EXPLICIT CHARACTERIZATION OF SUBSPACES WITHIN THE KERNELS

In the following, the explicit characterizations of subspaces within the kernels of the operators $\hat{S}_q$, as described in Sec. VB, are proven. Due to dependencies between the proofs, first the proofs for the cyclic cases (1), (2), and (4) are given, then for the negacyclic cases (I), (II), and (III), and then for the rest of cyclic and negacyclic cases.

1. Cyclic cases (1), (2), and (4)

The following theorems refer to lattices with cyclic symmetry. The lattice states $|\vec{n}\rangle$ that span the kernel are all states with integer vectors $\vec{n} = A\vec{m}$ with a corresponding constraint matrix A . The constraint matrix represents the solutions to Eq. (A1). The greatest common divisor of N and q is denoted by K .

Theorem B1. For $q = 0$, the constraint matrix associated with the kernel of $\hat{S}_0^{(c)}$ is $(N \times N - 1)$ dimensional with elements $A_{ij}^1 = \delta_{i,j} - \delta_{i,N-1}$.

Proof. For $q = 0$, Eq. (A1) reads $\sum_{p=0}^{N-1} n_p = 0$ with the solution $n_{N-1} = -\sum_{p=0}^{N-2} n_p$. Thus, any N -dimensional vector $\vec{n}$ such that $\vec{n} = A\vec{m}$ is a solution to Eq. (A1), for the $(N \times N - 1)$ -dimensional matrix A with elements $A_{ij} = \delta_{i,j} - \delta_{i,N-1}$, and for any $(N - 1)$ -dimensional vector of integers $\vec{m}$. ■

Lemma B1. For a prime number p , the p th cyclotomic polynomial is given by $f = 1 + \omega + \omega^2 + \dots + \omega^{p-1}$ and is irreducible over the rational numbers [46].

Theorem B2. If N is a prime number, the only solution to Eq. (A1) is $n_p = n_0$ for all p .

Proof. For a prime number N , there are N distinct roots of unity given by the equation

$$\omega^N = 1 \iff \omega^N - 1 = 0. \quad (\text{B1a})$$

The right-hand side can be factored into product of two polynomials such that

$$(1 + \omega + \omega^2 + \dots + \omega^{N-1})(\omega - 1) = 0. \quad (\text{B1b})$$

The first polynomial of the product,

$$f(\omega) := \sum_{p=0}^{N-1} \omega^p, \quad (\text{B2})$$

is irreducible over the rational (and integer) numbers as given by Lemma B1. Thus, the roots of the equation $f = 0$ are linearly independent over the field of rational numbers $\mathbb{Q}$; i.e., the unique way to express each one of the roots $\{1, e^{-i\frac{2\pi}{N}q}, e^{-i\frac{2\pi}{N}q^2}, \dots, e^{-i\frac{2\pi}{N}q(p-1)}\}$ as a function of all other roots is given by the equation $f = 0$. Hence, up to a multiplication with any integer, these roots of unity can sum up to

zero only with all their coefficients being 1. Hence, for any prime N ,

$$\sum_{p=0}^{N-1} n_p e^{-i\frac{2\pi}{N}p} = 0 \iff n_p = n_0, \quad \forall p \in [1, N-1]. \quad (\text{B3a})$$

In addition, for a prime number N , the roots $e^{-i\frac{2\pi}{N}m}$ with any $m = 0, 1, \dots, N-1$ are primitive roots. That is, the set of taking all the powers of the root from 0 to $N-1$ generates N distinct roots of unity. Hence, for any $q \in [0, p-1]$ the set $\{e^{-i\frac{2\pi}{N}qp}\}_{p=0}^{N-1}$ is equivalent to the set $\{1, e^{-i\frac{2\pi}{N}q}, e^{-i\frac{2\pi}{N}2q}, \dots, e^{-i\frac{2\pi}{N}(N-1)q}\}$, so the same argument as above holds. Thus, for any $q \in [0, N-1]$ the following relation holds:

$$\sum_{p=0}^{N-1} n_p e^{-i\frac{2\pi}{N}qp} = 0 \iff n_0 = n_p, \quad \forall p \in [1, N-1]. \quad (\text{B3b})$$

Theorem B3. For $K = 1$, each prime factor p of the dimension N has an associated class of states $|\vec{n}\rangle$ that are within the kernel of $\hat{S}_q^{(c)}$. The class of states is defined according to Eq. (8), with the $(N \times \frac{N}{p})$ -dimensional constraint matrix $A^{2,p}$ with elements $A_{ij}^{2,p} = \delta_{i \in \frac{N}{p}, j}$.

Proof. For every prime coefficient p of N , Eq. (A1) can be explicitly written as

$$\sum_{l=0}^{\frac{N}{p}-1} e^{-i\frac{2\pi}{N}ql} f_l(e^{-i\frac{2\pi}{p}q}) = 0, \quad (\text{B4a})$$

with

$$f_l(\omega) := \sum_{m=0}^{p-1} n_{l+m\frac{N}{p}} \omega^m. \quad (\text{B4b})$$

The polynomial $f_l(\omega)$ follows Theorem B2 for prime dimensions. Thus, Eq. (B4) can be solved if all the integer coefficients $n_{l+m\frac{N}{p}}$ for each polynomial f_l are equal.

This results in $\frac{N}{p}$ degrees of freedom, where all states of the form $|n_0, \dots, n_{\frac{N}{p}-1}, n_0, \dots, n_{\frac{N}{p}-1}, n_0, \dots\rangle$ are within the kernel of $\hat{S}_q^{(c)}$. Therefore, all lattice states $|\vec{n}\rangle$ with $\vec{n} = A^{2,p}\vec{m}$ for an $\frac{N}{p}$ -dimensional vector $\vec{m}$ and an $(N \times \frac{N}{p})$ -dimensional matrix $A^{2,p}$ with elements $A_{ij}^{2,p} = \delta_{i \in \frac{N}{p}, j}$ are within the kernel of $\hat{S}_q^{(c)}$ for $K = 1$. ■

Theorem B4. For $K > 1$, for any prime factor p of $\frac{N}{K}$ there is a class of states $|\vec{n}\rangle$ that are within the kernel of $\hat{S}_q^{(c)}$. This class is defined according to Eq. (8) with the constraint matrix $A^{4,p}$ with dimensions $(N \times (N - \frac{N}{Kp}(p-1)))$ and with elements defined in Eq. (20).

Proof. For $K > 1$, an effective dimension is defined as $\tilde{N} = \frac{N}{K}$ and an effective coefficient as $\tilde{q} = \frac{q}{K}$ such that $\gcd(\tilde{N}, \tilde{q}) = 1$. Equation (A1) reduces to

$$\sum_{l=0}^{\tilde{N}-1} y_l \exp\left(-i\frac{2\pi}{\tilde{N}}\tilde{q}l\right) = 0, \quad (\text{B5a})$$

where

$$y_l := \sum_{k=0}^{K-1} n_{l+k\tilde{N}}. \quad (\text{B5b})$$

The solution in terms of the coefficients y_l is given by Theorem B3 such that for each prime factor p of $\tilde{N}$, the solution has $\frac{\tilde{N}}{p}$ free integer coefficients and it reads

$$y_l = y_{[l]}, \quad (\text{B6a})$$

with $[l]$ denoting $l \bmod \frac{\tilde{N}}{p}$.

Substituting Eq. (B5b) into Eq. (B6a) leads to the solution

$$n_j = n_{[j]} + \sum_{k=1}^{K-1} n_{[k\frac{\tilde{N}}{p}+j]} - n_{k\frac{\tilde{N}}{p}+j-N}. \quad (\text{B6b})$$

For each prime factor p of $\tilde{N}$, there are $\tilde{N} - \frac{\tilde{N}}{p}$ constraints and $N - \tilde{N} - \frac{\tilde{N}}{p}$ free modes. These are encapsulated by the constraint matrix $A^{4,p}$ with dimensions $(N \times (N - \frac{N}{Kp}(p-1)))$, and with elements defined in Eq. (20). ■

2. Negacyclic cases (I), (II), and (III)

The following theorems refer to lattices with negacyclic symmetry. The lattice states that span the kernel are all states with integer coefficients that solve Eq. (15). The greatest common divisor of $2N$ and $2q+1$ is denoted by L .

Lemma B2. The n th primitive root of unity ζ_n is a root of a given polynomial $f(\zeta_n) = 0$ iff the n th cyclotomic polynomial $\Phi_n(\omega)$ divides the polynomial f , that is, $\Phi_n(\omega)|f(\omega)$ [46].

Theorem B5. If $N = 2^m$ for some non-negative integer m , the kernel of $\hat{S}_q^{(n)}$ is spanned by the zero state $|\vec{0}\rangle$.

Proof. For the case of $q = 0$, Eq. (15) reduces to $f(\omega) = 0$, with $\omega = \exp(-i\frac{2\pi}{2N})$ and

$$f(\omega) := \sum_{l=0}^{N-1} n_l \omega^l. \quad (\text{B7})$$

The $2N$ th cyclotomic polynomial is given by $\Phi_{2N}(\omega) = \omega^N + 1$. The degree of the cyclotomic polynomial is N , while the degree of the polynomial $f(\omega)$ is $N-1$. Hence, the cyclotomic polynomial cannot divide $f(\omega)$, and according to Lemma B2 there are no primitive roots for the dimension $2N$ that are roots of the polynomial f , specifically $\omega = \exp(-i\frac{2\pi}{2N})$. That is, there is no solution to the equation $f(\exp(-i\frac{2\pi}{2N})) = 0$ unless all the coefficients n_l are zero, i.e., the trivial solution.

For other cases $q > 0$, the same argument applies, since ω^{2q+1} ($1 \leq q \leq N-1$) are exactly the other roots of the cyclotomic polynomial $\Phi_{2N}(\omega)$.

Theorem B6. If N is a prime number, the only nontrivial solution for Eq. (15) is $n_0 = -n_1 = n_2 = \dots = -n_{N-2} = n_{N-1}$. ■

Proof. By adding π radians to the phase of each odd-indexed integer coefficient n_l (i.e., l is odd), Eq. (15) can be rewritten as

$$\sum_{l=0}^{N-1} y_l \exp\left(-i\frac{2\pi}{N}(2q+1)l\right), \quad (\text{B8a})$$

with

$$y_l = \begin{cases} n_{2l}, & \text{if } l \leq \frac{N-1}{2} \\ -n_{2l-N}, & \text{if } l \geq \frac{N+1}{2}. \end{cases} \quad (\text{B8b})$$

The solution is given by Theorem B2 in terms of the integer coefficients y_l . Substituting the original coefficients leads to the only solution $n_0 = -n_1 = n_2 = \dots = -n_{N-2} = n_{N-1}$. ■

Theorem B7. If $L = 1$ and N is not some power of 2, for each prime factor p of the dimension N , all states $|\vec{n}\rangle$ defined according to Eq. (8) with the constraint matrix $A^{II,p}$ are within the kernel of $\hat{S}_q^{(n)}$. The constraint matrix $A^{II,p}$ is $(N \times \frac{N}{p})$ dimensional and its elements are defined according to Eq. (23).

Proof. Following the proof of Theorem B3, for every prime factor $p > 2$ of N , Eq. (15) can be decomposed to $\frac{N}{p}$ polynomials [as in Eq. (B4)]:

$$\sum_{l=0}^{\frac{N}{p}-1} e^{-i\frac{2\pi}{2N}(2q+1)l} f_l(e^{-i\frac{2\pi}{2p}(2q+1)}) = 0, \quad (\text{B9a})$$

where the polynomial $f_l(\omega)$ is defined in Eq. (B4b). The integer coefficients of each polynomial must have the form defined in Theorem B6 in order for the equation to be solved.

Thus, for each prime factor p of N , all states of the form $|n_0, \dots, n_{\frac{N}{p}-1}, -n_0, \dots, -n_{\frac{N}{p}-1}, n_0, \dots\rangle$ span a subspace within the kernel of $\hat{S}_q^{(n)}$. These are represented by the constraint matrix $A^{II,p}$ with elements defined in Eq. (23). ■

Theorem B8. If $L > 1$ and $N = 2^m L$ for some positive integer m , all states $|\vec{n}\rangle$ defined according to Eq. (8) with the constraint matrix A^{III} are within the kernel of $\hat{S}_q^{(n)}$. The constraint matrix A^{III} is $(N \times (N - \frac{N}{L}))$ dimensional and its elements are defined according to Eq. (24).

Proof. By defining an effective dimension $\tilde{N} := \frac{2N}{L}$ and an effective index $\tilde{q} := \frac{2q+1}{L}$, Eq. (15) reduces to

$$\sum_{l=0}^{\tilde{N}-1} y_l \exp\left(-i\frac{2\pi}{\tilde{N}}\tilde{q}l\right) = 0, \quad (\text{B10a})$$

with

$$y_l := \sum_{k:[k]=l} n_k, \quad (\text{B10b})$$

where $[k]$ is a shorthand notation for $k \bmod \tilde{N}$. Because the effective dimension is some power of 2 and $\tilde{K} := \gcd(\tilde{N}, \tilde{q}) = 1$, the solution is given by Theorem B3 in terms of the integers y_l .

The substitution by the original integer coefficients n_l , alongside the fact that 2 is the only prime factor of $\tilde{N}$, leads to $\frac{N}{L}$ constraints that are encapsulated by the $(N \times (N - \frac{N}{L}))$ -dimensional constraint matrix A^{III} with elements defined in Eq. (24). ■

3. Cyclic cases (3) and (5)

Theorem B9. For any K such that $\frac{N}{K}$ is even and is not some power of 2, each prime factor p of $\frac{N}{2K}$ has an associated class of states $|\vec{n}\rangle$ that are within the kernel of $\hat{S}_q^{(c)}$. The class of

states is defined by the $(N \times (N - \frac{N}{2Kp}(p-1)))$ -dimensional constraint matrix $A^{3,p}$ with elements defined in Eq. (19).

Proof. Equation (A1) can be written as

$$\sum_{l=0}^{\tilde{N}-1} y_l \exp\left(-i\frac{2\pi}{\tilde{N}}\tilde{q}l\right) = 0, \quad (\text{B11a})$$

with $\tilde{N} = \frac{N}{K}$, $\tilde{q} = \frac{q}{K}$, and $y_l = \sum_k n_{l+k\tilde{N}}$. Because $\tilde{N}$ is even and the greatest common divisor $\gcd(\tilde{N}, \tilde{q})$ equals unity by definition, $\tilde{q}$ is odd. Thus, the equation can be rewritten as

$$\sum_{l=0}^{\frac{\tilde{N}}{2}-1} z_l \exp\left(-i\frac{2\pi}{2\frac{\tilde{N}}{2}}(2q'+1)l\right) = 0, \quad (\text{B11b})$$

with $z_l = y_l - y_{l+\tilde{N}/2}$ and $\tilde{q} = 2q' + 1$. The last equation can be recognized as the defining equation for the negacyclic symmetry, i.e., Eq. (15), with $L = 1$ and N , which is not some power of 2 [i.e., case (II) for negacyclic lattices].

Hence, according to Theorem B7 each prime factor p of $\frac{\tilde{N}}{2}$ has an associated class of states that lies within the kernel of $\hat{S}_q^{(c)}$. Expressing the integer coefficients z_l in terms of the original integer coefficients n_l leads to the symmetry classes being defined in terms of the constraint matrix $A^{3,p}$ for each prime factor p of $\frac{N}{2K}$ with elements defined in Eq. (19). ■

4. Negacyclic case (IV)

Theorem B10. If $L > 1$ and $N \neq 2^m L$ for any positive integer m , a subspace within the kernel of $\hat{S}_q^{(n)}$ is spanned by all states $|\vec{n}\rangle$ that obey the relation $\vec{n} = A^{IV,p}\vec{m}$ or $\vec{n} = A^{V,q}\vec{m}$ for an arbitrary vector of integers $\vec{m}$, for all prime factors p of $\frac{2N}{L}$ and all prime factors q of $\frac{N}{L}$.

Proof. By defining the effective dimension as $\tilde{N} = \frac{2N}{L}$ and the effective index as $\tilde{q} = \frac{2q+1}{L}$, Eq. (15) reduces to

$$\sum_{l=0}^{\tilde{N}-1} y_l \exp\left(-i\frac{2\pi}{\tilde{N}}\tilde{q}l\right) = 0, \quad (\text{B12a})$$

with

$$y_l = \sum_{[k]=l} n_k, \quad (\text{B12b})$$

where $[k]$ is a shorthand notation for $k \bmod \tilde{N}$. Because the greater common divisor of $\tilde{N}$ and $\tilde{q}$ is unity by definition [i.e., $\tilde{K} := \gcd(\tilde{N}, \tilde{q}) = 1$] and $\tilde{N}$ is even but not some power of 2, the solutions to the above equation are given by cyclic case (3) in terms of the integer coefficients y_l . Substituting the original coefficients n_l and expressing the solution in terms of constraints matrices results in the two types of constraints matrices.

First, for every prime factor p of $\frac{2N}{L}$, the $(N \times (\frac{2N}{L} - \frac{2N}{Lp}))$ -dimensional constraint matrix $A^{IV,p}$ is given explicitly by Eq. (25a). Second, for each prime factor $q > 2$ of $\frac{N}{L}$ the constraint matrix $A^{V,q}$ with dimensions $(N \times (\frac{N}{L} - \frac{N}{Lq}))$ is given by Eq. (25b). A subspace within the kernel of $\hat{S}_q^{(n)}$ is spanned by all states $|\vec{n}\rangle$ that obey the relation $\vec{n} = A^{IV,p}\vec{m}$ or $\vec{n} = A^{V,q}\vec{m}$ for an arbitrary vector of integers $\vec{m}$. ■

- [1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21**, 120 (1978).
- [2] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, Transitioning organizations to post-quantum cryptography, *Nature (London)* **605**, 237 (2022).
- [3] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (Santa Fe, NM, USA, 1994), pp. 124–134.
- [4] A. Katabarwa, K. Gratsea, A. Caesura, and P. D. Johnson, Early fault-tolerant quantum computing, *PRX Quantum* **5**, 020101 (2024).
- [5] Y.-K. Liu and D. Moody, Post-quantum cryptography and the quantum future of cybersecurity, *Phys. Rev. Appl.* **21**, 040501 (2024).
- [6] D. Moody, R. Perlner, A. Regenscheid, A. Robinson, and D. Cooper, Transition to post-quantum cryptography standards, Technical Report NIST IR 8547 (ipd), NIST, 2024.
- [7] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography* (Springer, Berlin, 2009), pp. 1–14.
- [8] C. Peikert, A decade of lattice cryptography, *Found. Trends Theor. Comput. Sci.* **10**, 283 (2016).
- [9] R. Cramer, L. Ducas, and B. Wesolowski, Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time, *J. ACM* **68**, 1 (2021).
- [10] K. de Boer and W. van Woerden, Lattice-based cryptography: A survey on the security of the lattice-based (NIST) finalists, Cryptology ePrint Archive, Report 2025/304, 2025, <https://eprint.iacr.org/2025/304>.
- [11] F. Verstraete, V. Murg, and J. I. Cirac, Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems, *Adv. Phys. (NY)* **57**, 143 (2008).
- [12] R. Orús, Tensor networks in many-body physics, *Nat. Rev. Phys.* **1**, 538 (2019).
- [13] M. C. Bañuls, Tensor network algorithms: A route map, *Annu. Rev. Condens. Matter Phys.* **14**, 173 (2023).
- [14] N. Nakatani and G. K.-L. Chan, Efficient tree tensor network states (TTNS) for quantum chemistry, *J. Chem. Phys.* **138**, 134113 (2013).
- [15] A. Berezutskii, M. Liu, A. Acharya, *et al.*, Tensor networks for quantum computing, *Nat. Rev. Phys.* **7**, 581 (2025).
- [16] B. Fauseweh, Quantum many-body simulations on digital quantum computers: State-of-the-art and future challenges, *Nat. Commun.* **15**, 2123 (2024).
- [17] E. Altman, K. R. Brown, G. Carleo, *et al.*, Quantum simulators: Architectures and opportunities, *PRX Quantum* **2**, 017003 (2021).
- [18] A. J. Daley, I. Bloch, C. Kokail, S. Flannigan, N. Pearson, M. Troyer, and P. Zoller, Practical quantum advantage in quantum simulation, *Nature (London)* **607**, 667 (2022).
- [19] D. Joseph, A. Callison, C. Ling, and F. Mintert, Two quantum Ising algorithms for the shortest-vector problem, *Phys. Rev. A* **103**, 032433 (2021).
- [20] Y. R. Zhu, D. Joseph, C. Ling, and F. Mintert, Iterative quantum optimization with an adaptive problem Hamiltonian for the shortest vector problem, *Phys. Rev. A* **106**, 022435 (2022).
- [21] J. Barberà-Rodríguez, N. Gama, A. K. Narayanan, and D. Joseph, Finding dense sublattices as low energy states of a Hamiltonian, *Phys. Rev. Res.* **6**, 043279 (2024).
- [22] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden, Variational quantum solutions to the shortest vector problem, *Quantum* **7**, 933 (2023).
- [23] Y. Chen, K.-M. Chung, and C.-Y. Lai, Space-efficient classical and quantum algorithms for the shortest vector problem, *Quantum Inf. Comput.* **18**, 285 (2018).
- [24] Y. Chen, Quantum algorithms for lattice problems, Cryptology ePrint Archive, Report 2024/555, 2024, <https://eprint.iacr.org/2024/555>.
- [25] L. Eldar and S. Hallgren, An efficient quantum algorithm for lattice problems achieving subexponential approximation factor, *arXiv:2201.13450*.
- [26] K. Mizuno and S. Watabe, Quantum algorithm for shortest vector problems with folded spectrum method, *arXiv:2408.16062*.
- [27] L. Engelberts, Y. Chen, A. S. Gilani, M.-I. van Hoof, S. Jeffery, and R. de Wolf, An improved quantum algorithm for 3-tuple lattice sieving, *Adv. Cryptol.* **16802**, 429 (2026).
- [28] M. Zheng, J. Zeng, W. Yang, P.-J. Chang, Q. Lu, B. Yan, H. Zhang, M. Wang, S. Wei, and G.-L. Long, Quantum-classical hybrid algorithm for solving the learning-with-errors problem on NISQ devices, *Commun. Phys.* **8**, 208 (2025).
- [29] X. Hou, G. Zhou, S. Jin, Y. Li, W. Huang, A. Sun, X. Wang, and B. Xu, Efficient variational quantum Korkin-Zolotarev algorithm for solving shortest-vector problems, *Phys. Rev. A* **113**, 042611 (2026).
- [30] Z.-W. Huang, X.-H. Ni, J.-C. Fan, S.-J. Qin, W. Huang, B.-J. Xu, and F. Gao, Iterative partition-search variational quantum algorithm for solving the shortest-vector problem, *Phys. Rev. A* **113**, 032601 (2026).
- [31] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O’Brien, A variational eigenvalue solver on a photonic quantum processor, *Nat. Commun.* **5**, 4213 (2014).
- [32] J. Hoffstein, J. Pipher, and J. H. Silverman, NTRU: A ring-based public key cryptosystem, in *Algorithmic Number Theory (ANTS)*, edited by J. P. Buhler, Lecture Notes in Computer Science Vol. 1423 (Springer, Berlin, Heidelberg, 1998), pp. 267–288.
- [33] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions, *Comput. Complex.* **16**, 365 (2007).
- [34] L. Fukshansky and X. Sun, On the geometry of cyclic lattices, *Discrete Comput. Geom.* **52**, 240 (2014).
- [35] G. Alagic, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and D. Apon, Status report on the third round of the NIST post-quantum cryptography standardization process, Technical Report: NIST-IR.8413 (NIST, Gaithersburg, MD, 2026), doi: [10.6028/NIST.IR.8413](https://doi.org/10.6028/NIST.IR.8413).
- [36] V. Lyubashevsky, C. Peikert, and O. Regev, On ideal lattices and learning with errors over rings, *J. ACM* **60**, 1 (2013).
- [37] D. A. Marcus, *Number Fields*, Universitext (Springer, New York, 1977).
- [38] W. Bosma, Canonical bases for cyclotomic fields, *Appl. Algebra Eng. Commun. Comput.* **1**, 125 (1990).

- [39] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics Vol. 138 (Springer, Berlin, 1993).
- [40] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles, Variational quantum algorithms, *Nat. Rev. Phys.* **3**, 625 (2021).
- [41] V. Bergholm *et al.*, PennyLane: Automatic differentiation of hybrid quantum-classical computations, [arXiv:1811.04968](https://arxiv.org/abs/1811.04968).
- [42] A. K. Lenstra, H. W. Lenstra, and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261**, 515 (1982).
- [43] J. Eisert and J. Preskill, Mind the gaps: The fraught road to quantum advantage, [arXiv:2510.19928](https://arxiv.org/abs/2510.19928).
- [44] J. Villain, Theory of one- and two-dimensional magnets with an easy magnetization plane. II. The planar, classical, two-dimensional magnet, *J. Phys. France* **36**, 581 (1975).
- [45] J. V. José, L. P. Kadanoff, S. Kirkpatrick, and D. R. Nelson, Renormalization, vortices, and symmetry-breaking perturbations in the two-dimensional planar model, *Phys. Rev. B* **16**, 1217 (1977).
- [46] P. B. Garrett, *Abstract Algebra* (Chapman and Hall/CRC Press, New York, 2007).