SVP_∞ Is NP-Hard for Power-of-two Cyclotomic Ideals

Yansong Feng, Jiaqi Liu, Hengyi Luo, and Yanbin Pan

Academy of Mathematics and Systems Science, Chinese Academy of Sciences
{fengyansong,ljqi,luohengyi,panyanbin}@amss.ac.cn

Abstract. We prove that exact decision-SVP in the coefficient ℓ_∞-norm is NP-complete for principal ideals and free modules of rank two over the cyclotomic rings $R_n = \mathbb{Z}[X]/(X^n + 1)$, where n ranges over powers of two. For each case, we give a deterministic polynomial-time many-one reduction from the Subset Sum problem. For an instance with s positive input integers, the output lattice has dimension $O(s)$. A solution to the original Subset Sum instance can be recovered in polynomial time from any nonzero output lattice vector of norm at most the specified bound.
We also transfer these reductions from R_n to the power-of-two cyclic rings $S_{2n} = \mathbb{Z}[X]/(X^{2n} - 1)$. This gives NP-completeness of decision-SVP in the coefficient ℓ_∞-norm for principal ideals and free modules of any fixed positive rank over these rings.

1 Introduction

A lattice $\mathcal{L} \subseteq \mathbb{R}^m$ is the set of all integer linear combinations of linearly independent vectors in $\mathbb{R}^m$. Given a basis of $\mathcal{L}$ and a threshold $T > 0$, the decision shortest vector problem (SVP) asks whether $\mathcal{L}$ contains a nonzero vector of norm at most T. For general integer lattices, van Emde Boas proved deterministic NP-hardness of SVP in the ℓ_∞-norm [vEB81]. Dinur later proved NP-hardness of approximating SVP in the ℓ_∞-norm within almost-polynomial factors [Din02]. In the ℓ_2-norm, Ajtai proved randomized NP-hardness [Ajt98], and Micciancio obtained randomized hardness of approximation within constant factors below $\sqrt{2}$ [Mic01]. Khot extended this randomized NP-hardness to approximation within any fixed constant factor [Kho05]. Wan later proved deterministic NP-hardness of approximation within any constant factor greater than 1 [Wan26a].

The worst-case hardness of SVP also provides a basis for lattice-based cryptography. Worst-case-to-average-case reductions connect lattice approximation problems to the average-case learning with errors (LWE) problem. Regev [Reg09] gave quantum reductions from worst-case GapSVP (the gap decision version of SVP) and the shortest independent vectors problem (SIVP) to LWE. Both source problems have polynomial approximation factors in the ℓ_2-norm. Peikert [Pei08] extended these quantum reductions to GapSVP and SIVP in the ℓ_∞-norm. Peikert [Pei09] also gave a classical reduction from GapSVP in the ℓ_∞-norm to LWE for exponentially large moduli. Brakerski et al. [BLP+13] later gave a classical reduction from worst-case GapSVP in the ℓ_2-norm to LWE with polynomially large moduli, at the cost of increasing the dimension.

Cryptographic schemes often use lattices with additional algebraic structure. Under the coefficient embedding, ideals and modules over cyclotomic rings give ideal and module lattices that are closed under multiplication by ring elements. The ring structure supports compact descriptions and fast polynomial arithmetic. Early constructions of collision-resistant hash functions were based on worst-case approximation assumptions for ideal lattices [LM06] and cyclic lattices [PR06]. Worst-case approximation problems on ideal and module lattices over cyclotomic rings also admit reductions to Ring-LWE [LPR10] and Module-LWE [LS15], respectively. The security of ML-KEM, standardized by NIST in FIPS 203, is based on the hardness of Module-LWE over a power-of-two cyclotomic ring [Nat24].

Several recent works have established hardness of SVP in structured settings. Martin gives dimension-preserving reductions from general Euclidean lattice problems to the canonical embeddings of invertible ideals in totally real monogenic orders [Mar26]. Wan proves deterministic NP-hardness of coefficient Euclidean SVP on full-rank ideals of $\mathbb{Z}[X]/(X^N - 1)$, where $N = q - 1$ for an odd prime q [Wan26b]. Liu, Feng, and Pan prove deterministic NP-completeness of canonical Euclidean SVP on free modules of rank two over prime-cyclotomic rings with prime conductor $q \equiv 3 \pmod 4$ [LFP26b].

We ask the following two questions.

(i) *Is* SVP *in the coefficient ℓ_∞-norm* NP*-complete for principal ideals and free modules over power-of-two cyclotomic rings?*

(ii) *Is* SVP *in the coefficient ℓ_∞-norm* NP*-complete for principal ideals and free modules over power-of-two cyclic rings?*

1.1 Our results

We give deterministic polynomial-time many-one reductions from the Subset Sum problem to exact SVP in the coefficient ℓ_∞-norm over the cyclotomic rings

$$R_n = \mathbb{Z}[X]/(X^n + 1)$$

and the cyclic rings $S_{2n} = \mathbb{Z}[X]/(X^{2n} - 1)$, where n ranges over powers of two.

Theorem 1.1 (Informal). SVP *in the coefficient ℓ_∞-norm is* NP*-complete for free modules of rank two and for principal ideals over R_n, where n ranges over powers of two.*

The principal-ideal reduction also gives NP-completeness for free modules of any fixed positive rank over R_n. The separate rank-two construction has smaller lattice dimension and gives a direct polynomial encoding of Subset Sum. Its two-coordinate subset-sum check motivates the principal-ideal construction.

We also extend the cyclotomic-to-cyclic construction of Liu, Feng, and Pan [LFP26a] to free modules of arbitrary fixed rank, obtaining an exact relation between the first minima in the coefficient ℓ_∞-norm.

Theorem 1.2 (Informal). SVP *in the coefficient ℓ_∞-norm is* NP*-complete for principal ideals and free modules of any fixed positive rank over S_{2n}, where n ranges over powers of two.*

For a Subset Sum instance with s positive input integers, the two cyclotomic reductions for principal ideals and free rank-two modules over R_n each produce a lattice of dimension $O(s)$. In either reduction, a solution to the Subset Sum instance can be recovered in deterministic polynomial time from any nonzero vector in the constructed lattice whose ℓ_∞-norm is at most the specified bound. The corresponding search problems are therefore NP-hard under polynomial-time Turing reductions. The cyclic transfer gives the same $O(s)$ dimension bound and search hardness for every fixed module rank over S_{2n}.

1.2 Technical overview

Our reductions start from the Subset Sum problem, whose input consists of positive integers $w_1, \ldots, w_s$ and a nonnegative integer target B. The problem asks whether there are Boolean choices $\xi_j \in \{0, 1\}$ satisfying $\sum_{j=1}^{s} w_j \xi_j = B$. To encode this condition, each reduction constructs a lattice $\mathcal{L}$ and a positive integer T such that

$$\exists\, \boldsymbol{\xi} \in \{0,1\}^s : \sum_{j=1}^{s} w_j \xi_j = B \quad \Longleftrightarrow \quad \exists\, \mathbf{0} \neq \mathbf{y} \in \mathcal{L} : \ \|\mathbf{y}\|_\infty \leq T.$$

We begin with an integer lattice, adapt its encoding to rank-two modules and principal ideals over R_n, and then transfer the constructions to cyclic rings.

Warm-up: ℓ_∞-norm NP-hardness in general lattices. We first recall a reduction from the Subset Sum problem [Kar72] to SVP in general lattices, illustrating the classical NP-hardness result for the ℓ_∞-norm [vEB81]. To encode the Boolean restriction, we represent ξ_j by an integer variable a_j and require $|2a_j - 1| \leq 1$, which is equivalent to $a_j \in \{0, 1\}$. To encode this condition in a lattice, we replace the fixed constant 1 in $2a_j - 1$ by an integer variable b. This replacement gives the linear coordinate $2a_j - b$, which agrees with $2a_j - 1$ when $b = 1$. We will force nonzero vectors of ℓ_∞-norm at most 1 to have $b = \pm 1$, and then take $b = 1$ by negating the vector if necessary.

Put $W := \sum_{j=1}^{s} w_j$. To test the subset-sum equation, we add the coordinate $\sum_{j=1}^{s} w_j a_j - Bb$. We multiply it by 2 so that an ℓ_∞-norm bound of 1 forces it to be zero. To obtain a full-rank lattice, we introduce an integer variable c and add Cc to this coordinate, where $C := 2(W + B + 1)$. The even

value of C preserves this parity condition, and its size will force $c = 0$ for short vectors. Together with the coordinates $2a_j - b$ and b, this gives the lattice

$$\left\{ \begin{pmatrix} 2\mathbf{a} - b\mathbf{1} \\ b \\ 2\big(\sum_{j=1}^{s} w_j a_j - Bb\big) + Cc \end{pmatrix} : \mathbf{a} \in \mathbb{Z}^s,\ b, c \in \mathbb{Z} \right\} \subseteq \mathbb{Z}^{s+2}, \tag{1.1}$$

where $\mathbf{1} \coloneqq (1, \ldots, 1)^\mathsf{T} \in \mathbb{Z}^s$.

A solution $\boldsymbol{\xi}$ to the Subset Sum instance gives a nonzero vector of ℓ_∞-norm 1 in (1.1) by taking $\mathbf{a} = \boldsymbol{\xi}$, $b = 1$, and $c = 0$. Conversely, for a nonzero vector in (1.1) of ℓ_∞-norm at most 1, the second coordinate gives $b \in \{0, \pm 1\}$. The case $b = 0$ would force $\mathbf{a} = \mathbf{0}$ in the first block and $c = 0$ in the last coordinate, giving the zero vector. Thus $b = \pm 1$, and after negating the vector if necessary we may assume $b = 1$. The first block then gives $a_j \in \{0, 1\}$.

With these Boolean choices, the last coordinate tests the subset-sum equation. It is even and has absolute value at most 1, so $2(\sum_{j=1}^{s} w_j a_j - B) + Cc = 0$. The Boolean conditions give $0 \le \sum_{j=1}^{s} w_j a_j \le W$. Since

$$|Cc| = \left| 2 \left(\sum_{j=1}^{s} w_j a_j - B \right) \right| \le 2(W + B) < C,$$

and $c \in \mathbb{Z}$, we obtain $c = 0$ and $\sum_{j=1}^{s} w_j a_j = B$. Thus the lattice in (1.1) contains a nonzero vector of ℓ_∞-norm at most 1 if and only if the Subset Sum instance has a solution.

Encoding Subset Sum in rank-two modules. The lattice in (1.1) encodes the subset-sum equation using integer variables. Similarly, we construct a rank-two module over the cyclotomic ring $R_n \coloneqq \mathbb{Z}[X]/(X^n + 1)$, where n is a power of two. We store the Boolean choices in the coefficients of a polynomial $a \in R_n$. The integer variable b is likewise replaced by a polynomial $b \in R_n$. However, $\|b\|_\infty \le 1$ allows many nonzero terms (for example, $b = 1 + X + \cdots + X^{n-1}$), so this bound alone does not give the normalization to $b = 1$ used in the integer construction. We therefore need an additional constraint forcing a nonzero b to be a signed monomial $b = \pm X^\ell$. Multiplication by b^{-1} then preserves the coefficient ℓ_∞-norm and reduces to $b = 1$.

Step 1. Encoding Boolean choices. We assume $0 \le B \le W$. Let $n \coloneqq 2m$ with $m > s$ a power of two and put $u \coloneqq \sum_{j=1}^{s} X^{j-1}$. Here u plays the role of the all-ones vector $\mathbf{1}$, so $z \coloneqq 2a - ub$ is the polynomial counterpart of the first lattice block $2\mathbf{a} - b\mathbf{1}$ in (1.1). We first choose the second module coordinate to be Mz and the ℓ_∞-norm threshold to be M, where M is a positive integer to be fixed later. Every vector of ℓ_∞-norm at most M then satisfies $\|z\|_\infty \le 1$. If $b = 0$, then $z = 2a$, and the second-coordinate bound gives $\|2a\|_\infty \le 1$, forcing $a = 0$ by integrality. Thus every nonzero vector in this norm range has $b \neq 0$, as in the integer construction (1.1).

We first describe the Boolean and subset-sum checks for the normalized case $b = 1$. In this case, the second-coordinate bound becomes $\|2a - u\|_\infty \le 1$ and forces a to have Boolean coefficients, with $a = \sum_{j=1}^{s} \xi_j X^{j-1}$ and $\xi_j \in \{0, 1\}$.

Step 2. Checking the subset-sum equation. For $b = 1$, we encode the weights in the Subset Sum instance by setting $\tilde{h} \coloneqq \sum_{j=1}^{s} w_j X^{-(j-1)}$. The opposite exponents make the constant coefficient of $\tilde{h}z$, denoted by $[\tilde{h}z]_0$, equal to $2\sum_{j=1}^{s} w_j \xi_j - W$. To compare $\sum_{j=1}^{s} w_j \xi_j$ with the target B, we need to compare this constant coefficient with $2B - W$.

We choose the first coordinate of the module lattice so that a nonzero difference $[\tilde{h}z]_0 - (2B - W)$ makes at least one of its coefficients exceed M in absolute value. To achieve this goal, we give the constant and X^m coefficients the values $-M$ plus and minus this difference, respectively. Since $s < m$, the coefficient of X^m in $\tilde{h}z$ is zero. Multiplying $\tilde{h}z - (2B - W)$ by $1 - X^m$ then keeps this difference in the constant coefficient and shifts its negative to the coefficient of X^m. We therefore set

$$h \coloneqq (1 - X^m)\tilde{h}, \qquad v \coloneqq (2B - W)(1 - X^m).$$

Subtracting $M(1 + X^m)$ from $hz - v$ gives the constant and X^m coefficients

$$-M + \big([\tilde{h}z]_0 - (2B - W)\big), \qquad -M - \big([\tilde{h}z]_0 - (2B - W)\big).$$

The two coefficients are symmetric about $-M$. If $[\tilde{h}z]_0 \neq 2B - W$, either the constant coefficient or the coefficient of X^m is less than $-M$ and therefore has absolute value greater than M. Thus a vector of ℓ_∞-norm at most M must satisfy the subset-sum equation.

Step 3. Restricting b to a signed monomial. We now return to general b and first take $hz - (Md + v)b$ as the first coordinate, where $d \coloneqq 1 + X^m$. A vector of ℓ_∞-norm at most M then satisfies $\|hz - (Md + v)b\|_\infty \leq M$. Multiplication by d replaces the coefficients of b at indices $j, j + m$ by their difference and sum, whose maximum absolute value equals the sum of the original absolute values. Together with $\|z\|_\infty \leq 1$, this first-coordinate bound forces $\|db\|_\infty = 1$ for $b \neq 0$ when M is sufficiently large. Consequently, for each $0 \leq j < m$, at most one of the coefficients of X^j and X^{j+m} in b is nonzero, and any nonzero coefficient equals 1 or -1. Every nonzero coefficient of Mdb therefore has absolute value M. However, the condition $\|db\|_\infty = 1$ still allows b to have several nonzero coefficients (for example, $b = 1 + X$), so an additional constraint is needed to force b to be a signed monomial.

To exclude these remaining possibilities, we set $q \coloneqq Md + Ldk$, with $k \in R_n$ and a positive integer L. The completed construction gives a free module of rank two whose vectors have the following form with $a, b \in R_n$

$$\begin{pmatrix} hz - (q + v)b \\ Mz \end{pmatrix}.$$

For sufficiently large M, every nonzero vector of this module with ℓ_∞-norm at most M satisfies $\|db\|_\infty = 1$. The polynomial k is designed so that, if $\|db\|_\infty = 1$ and b has more than one nonzero term, adding $Ldkb$ to Mdb increases the absolute value of at least one coefficient from M to at least $M + L$. The remaining term satisfies $\|hz - vb\|_\infty \leq 4W$. Choosing $L > 4W$ therefore makes the first coordinate have ℓ_∞-norm greater than M (Lemma 3.5).

Thus every nonzero vector of ℓ_∞-norm at most M has $b = \pm X^\ell$. Multiplication by b^{-1} preserves this norm and reduces to $b = 1$. The constant and X^m coefficients of Ldk are zero, so the constant coefficient and the coefficient of X^m in q both equal M. The second-coordinate bound then gives the Boolean coefficients of a, and the first-coordinate bound forces $\sum_{j=1}^{s} w_j \xi_j = B$. Conversely, a solution to the Subset Sum instance gives a vector of ℓ_∞-norm M, since the constant and X^m coefficients of the first coordinate are $-M$, its other coefficients have absolute value less than M, and $\|Mz\|_\infty = M$.

Encoding Subset Sum in principal ideals. In the rank-two construction, a stores the Boolean choices, while a signed monomial b is normalized to 1 for the subset-sum check. A vector in a principal ideal has the form $f\sigma$, so the same polynomial $\sigma \in R_n$ must encode the Boolean choices and at the same time allow us to check the subset-sum equation.

Step 1. Encoding Boolean choices. Let m be a sufficiently large power of two and set $n \coloneqq 2m$. We encode each Boolean choice ξ_j by the position of a nonzero coefficient of σ in the three-element set $\{8j - 1, 8j, 8j + 1\}$. The center $8j$ represents $\xi_j = 0$, and either $8j - 1$ or $8j + 1$ represents $\xi_j = 1$. To construct a polynomial from given Boolean choices $\boldsymbol{\xi} \in \{0, 1\}^s$, we take the index $8j + \xi_j$ and add the constant term 1, giving

$$\sigma \coloneqq 1 + \sum_{j=1}^{s} X^{8j+\xi_j}.$$

The constant term fixes $\sigma_0 = 1$, allowing the target B to enter the subset-sum check as a fixed subtraction.

Step 2. Checking the subset-sum equation. We retain the module construction's subset-sum check, in which the difference enters two ordinary coefficients with opposite signs. In the ring setting, write $\mathrm{i} = X^m$ and group the ordinary coefficients at ℓ and $\ell + m$ into the complex coefficient $\sigma_\ell = [\sigma]_\ell + \mathrm{i}[\sigma]_{\ell+m}$ for $0 \leq \ell < m$. Write $Z \coloneqq \sum_{j=1}^{s} w_j \xi_j - B$ for the subset-sum error associated with the Boolean choices $\boldsymbol{\xi}$. Let $T > 0$ be the ℓ_∞-norm bound. We first seek a polynomial $v \in R_n$ for which $(v\sigma)_0 = \mathrm{i}Z$. Therefore, for the generator $(T - v)d$ with $d = 1 + \mathrm{i}$, we have

$$\big((T - v)d\sigma\big)_0 = (1 + \mathrm{i})(T - \mathrm{i}Z) = (T + Z) + \mathrm{i}(T - Z).$$

The larger absolute value of these two ordinary coefficients is $T + |Z|$, so the ℓ_∞-norm bound T enforces $Z = 0$.

Just as $\tilde{h}$ reads the coefficients of z through the constant coefficient of $\tilde{h}z$, we construct a polynomial v to read the choices encoded in σ through the complex coefficient $(v\sigma)_0$. Multiplication by X^{-r} makes σ_r contribute to the complex coefficient at 0. To guarantee that each set $\{8j - 1, 8j, 8j + 1\}$

with $1 \le j \le s$ contains a nonzero complex coefficient of σ under the norm bound, we introduce a common offset $H := W + 1$. We assign the value H to the center $8j$ and $H + w_j$ to the two adjacent indices $8j - 1$ and $8j + 1$. Since $H > W$, omitting an entire set loses more than all the input weights can supply.

For the polynomial σ constructed in Step 1, subtracting $sH + B$ from $sH + \sum_{j=1}^{s} w_j \xi_j$ gives Z. We want the ordinary coefficients at indices 0 and m to form the pair $(T + Z, T - Z)$. To obtain these coefficients after multiplication by d, we place Z in the imaginary part of $(v\sigma)_0$ by defining

$$v := \mathrm{i}\left(\sum_{j=1}^{s}\left[HX^{-8j} + (H + w_j)\left(X^{-(8j-1)} + X^{-(8j+1)}\right)\right] - (sH + B)\right).$$

Thus $(v\sigma)_0 = \mathrm{i}Z$.

Step 3. Correcting the generator. However, the vector $(T - v)d\sigma$ violates the norm bound in the ordinary coefficient pair at indices p_s and $p_s + m$, where $p_s := 8s + \xi_s$ is the index of the last nonzero complex coefficient of σ. The terms containing negative powers of X in the definition of v contribute zero at p_s, so $(v\sigma)_{p_s} = -\mathrm{i}(sH + B)$. The ordinary coefficients at p_s and $p_s + m$ consequently have maximum absolute value $T + sH + B > T$, even when $Z = 0$. For σ constructed in Step 1, we design the correction $(g - v)\sigma$ to have real coefficient C at index 0 and real coefficients at least $2C$ at the other indices where σ has a nonzero complex coefficient, including p_s. We choose $C := \|v\|_1 + 1$ and raise the main term to $(T + C)d\sigma$. The correction is designed to bring both ordinary coefficients of $f\sigma$ below T in absolute value at every other nonzero complex position of σ. Thus $(g\sigma)_0 = C + \mathrm{i}Z$, and $(T + C - g)\sigma$ has complex coefficient $T - \mathrm{i}Z$ at 0. We therefore take the generator $f := (T + C - g)d$. Multiplication by d gives

$$d(T - \mathrm{i}Z) = (T + Z) + \mathrm{i}(T - Z).$$

Step 4. Enforcing the encoding. It remains to control the positions and complex coefficients of σ for every nonzero vector $f\sigma$ of ℓ_∞-norm at most T. To enforce the intended encoding, we take g to be of the form

$$g := 10Ca_E + t_0 + v. \tag{1.2}$$

With $T := 3\|g\|_1 + 1$, we can prove that every nonzero vector $f\sigma$ of ℓ_∞-norm at most T satisfies $\|d\sigma\|_\infty = 1$. Hence the complex coefficients of σ lie in $\{0, \pm 1, \pm \mathrm{i}\}$. We explain the roles of the three terms under this norm bound.

Multiplication by a power of X preserves $\|f\sigma\|_\infty$. We therefore use the dominant term $10Ca_E$ to constrain the pairwise cyclic distances between the indices of nonzero complex coefficients instead of their absolute positions. We build a_E from differences $X^\delta - X^{-\delta}$ for distances outside $E := \bigcup_{j=1}^{s}\{8j - 1, 8j, 8j + 1\}$. The norm bound forces all pairwise cyclic distances to belong to E and $(a_E\sigma)_\ell = 0$ whenever $\sigma_\ell \neq 0$ (Lemma 4.3). After multiplying by a suitable power of X, we may assume $\sigma_0 = 1$. Every other nonzero complex coefficient then has its index in one of the three-element sets, with at most one such index in each set.

The term v, defined above, uses the common offset $H > W$ to ensure that each set $\{8j-1, 8j, 8j+1\}$ contains a nonzero complex coefficient of σ. A missing copy of H cannot be compensated by the remaining input weights. Together with the distance restrictions from a_E, the norm bound gives exactly one nonzero complex coefficient in each set $\{8j - 1, 8j, 8j + 1\}$. For the polynomial constructed in Step 1, t_0 supplies the correction described in Step 3. With t_0, the norm bound then forces all nonzero complex coefficients of σ to equal 1 (Lemma 4.5).

Reading the Boolean choices from the nonzero positions of σ as in Step 1, we obtain $(v\sigma)_0 = \mathrm{i}Z$. Combining this with $(a_E\sigma)_0 = 0$ and $(t_0\sigma)_0 = C$ gives $(g\sigma)_0 = C + \mathrm{i}Z$. The ordinary coefficients of $f\sigma$ at 0 and m are therefore $T + Z$ and $T - Z$, so the norm bound forces $Z = 0$. Conversely, a solution gives a polynomial σ of the displayed form for which every ordinary coefficient of $f\sigma$ has absolute value at most T, with equality at indices 0 and m. The first minimum is therefore T on YES instances and at least $T + 1$ on NO instances by integrality.

Transfer to cyclic rings. The preceding reductions use $R_n = \mathbb{Z}[X]/(X^n + 1)$, where n is a power of two. Multiplication by X gives a negacyclic shift in R_n and a cyclic shift in $S_{2n} = \mathbb{Z}[X]/(X^{2n} - 1)$. The $\mathbb{Z}$-linear embedding $p \mapsto (1 - X^n)p$ sends the coefficient vector $\mathbf{p} \in \mathbb{Z}^n$ of p to $(\mathbf{p}, -\mathbf{p})$. The identity $(1 - X^n)(X^n + 1) = 0$ in S_{2n} ensures that multiplication by X in S_{2n} gives the required

negacyclic shift on the first block. We therefore seek a principal ideal of S_{2n} whose shortest vectors have the form $(\mathbf{w}, -\mathbf{w})$ with $\mathbf{w} \in \mathbb{Z}^n$.

We take $r = 1$ for example. We follow the construction of Liu, Feng, and Pan [LFP26a]. Given $0 \neq f \in R_n$, represented by a polynomial of degree less than n, take $C := 2\|f\|_\infty + 1$ and define

$$\widehat{f} := (1 - X^n)f + C(1 + X^n) \in S_{2n}.$$

To analyze the coefficients of $\widehat{f}u$, write $u = a + X^n b \in S_{2n}$ with $a, b \in \mathbb{Z}[X]$ of degree less than n. Let y be the representative of $f(a - b) \in R_n$ of degree less than n. Then

$$\widehat{f}u = \big(y + C(a + b)\big) + X^n\big(-y + C(a + b)\big).$$

The same polynomial $C(a + b)$ occurs in both blocks, and y occurs with opposite signs. A nonzero coefficient of $C(a+b)$ cannot be canceled in both blocks, so $a+b \neq 0$ forces $\left\|\widehat{f}u\right\|_\infty \geq C$. On the other hand, $\widehat{f}(1 - X^n) = 2(1 - X^n)f$ has norm $2\|f\|_\infty < C$. Every shortest output vector must therefore have $b = -a$. With $b = -a$, the two output blocks are $2fa$ and $-2fa$, where fa is reduced modulo X^n+1. Every vector $fa \in (f)$ has such an image by taking $u = a-X^n a$. Thus $\lambda_{1,\infty}((\widehat{f})) = 2\lambda_{1,\infty}((f))$.

Section 5 proves that the output module is free and extends this construction to polynomial matrices. It gives a deterministic polynomial-time reduction from SVP on free rank-r modules over R_n to the same problem over S_{2n}, for every fixed $r \geq 1$.

1.3 Organization

Section 2 establishes the algebraic preliminaries, coefficient norms, input representations, and complex coefficient representation. Section 3 presents the rank-two module reduction. Section 4 presents the principal-ideal reduction. Section 5 transfers both reductions to cyclic polynomial rings, and Section 6 concludes. A Lean formalization of our results is available at https://github.com/fffmath/pow2-cyclotomic-svp.

2 Preliminaries

Notation. We write $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ for the integers, rationals, reals, and complex numbers, respectively. Polynomials are denoted by lowercase italic letters, vectors by bold lowercase letters, and matrices by bold uppercase letters. The superscript T denotes transpose. For $z \in \mathbb{C}$, $\overline{z}$, $\Re z$, and $\Im z$ denote its complex conjugate, real part, and imaginary part, respectively. Logarithms are to base two.

2.1 Lattices

Let $1 \leq d \leq N$ and let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d) \in \mathbb{R}^{N\times d}$ have linearly independent columns. The *lattice* generated by $\mathbf{B}$ is

$$\mathcal{L} := \mathbf{B}\mathbb{Z}^d = \left\{ \sum_{j=1}^{d} u_j \mathbf{b}_j : u_1, \ldots, u_d \in \mathbb{Z} \right\}.$$

We call the columns of $\mathbf{B}$ a *basis* of $\mathcal{L}$ and d the *rank* of $\mathcal{L}$ [Mic01]. We call $\mathcal{L}$ *full-rank* if $d = N$.

For $\mathbf{x} = (x_1, \ldots, x_N)^\mathsf{T} \in \mathbb{R}^N$, define its ℓ_∞*-norm* by $\|\mathbf{x}\|_\infty := \max_{1\leq j\leq N} |x_j|$. We define the *first minimum* of $\mathcal{L}$ in this norm by

$$\lambda_{1,\infty}(\mathcal{L}) := \min_{\mathbf{0}\neq\mathbf{x}\in\mathcal{L}} \|\mathbf{x}\|_\infty .$$

Given an integer basis of a lattice $\mathcal{L}$ and a positive integer T, the *decision shortest vector problem* in the ℓ_∞-norm asks whether $\lambda_{1,\infty}(\mathcal{L}) \leq T$. Given an integer basis of $\mathcal{L}$, *search*-SVP in the ℓ_∞-norm asks for $\mathbf{0} \neq \mathbf{x} \in \mathcal{L}$ with $\|\mathbf{x}\|_\infty = \lambda_{1,\infty}(\mathcal{L})$.

2.2 Cyclotomic ring

Let $n \geq 1$ be a power of two and set

$$R_n \coloneqq \mathbb{Z}[X]/(X^n + 1).$$

Let $\zeta \coloneqq e^{\pi \mathrm{i}/n}$ be a primitive $2n$-th root of unity. Since $X^n + 1$ is the $2n$-th cyclotomic polynomial, evaluation at ζ induces the isomorphism $R_n \cong \mathbb{Z}[\zeta]$ sending X to ζ. The ring $\mathbb{Z}[\zeta]$ is the full ring of integers of the cyclotomic field $\mathbb{Q}(\zeta)$ [Was97]. Hence R_n is an integral domain. We identify each element with its unique representative of degree less than n. For $g \in R_n$ and $0 \leq \ell < n$, $[g]_\ell \in \mathbb{Z}$ denotes the *ordinary coefficient* of X^ℓ in this representative. The *coefficient embedding* with respect to the power basis $1, X, \ldots, X^{n-1}$ maps $g = \sum_{\ell=0}^{n-1} [g]_\ell X^\ell \in R_n$ to $([g]_0, \ldots, [g]_{n-1})^\mathsf{T} \in \mathbb{Z}^n$. We identify g with this vector and represent tuples of polynomials by concatenating their coefficient vectors.

For $g \in R_n$, define its norms by its coefficient vector:

$$\|g\|_1 \coloneqq \sum_{\ell=0}^{n-1} |[g]_\ell|, \qquad \|g\|_\infty \coloneqq \max_{0 \leq \ell < n} |[g]_\ell|.$$

For $\mathbf{z} = (z_1, \ldots, z_r) \in R_n^r$, set $\|\mathbf{z}\|_\infty \coloneqq \max_{1 \leq a \leq r} \|z_a\|_\infty$. For $g, z \in R_n$, we have

$$\|gz\|_\infty \leq \|g\|_1 \, \|z\|_\infty . \tag{2.1}$$

Multiplication by $g \in R_n$ is represented in the power basis by the matrix

$$\mathbf{M}_g \coloneqq \left([X^j g]_\ell\right)_{0 \leq \ell, j < n}. \tag{2.2}$$

Its j-th column is the coefficient vector of $X^j g$ for $0 \leq j < n$. Since $X^n = -1$, multiplication by X permutes coefficients up to sign, and $X^{-1} = -X^{n-1}$.

For $g, z \in R_n$, their *coefficient inner product* is $\langle g, z \rangle \coloneqq \sum_{\ell=0}^{n-1} [g]_\ell [z]_\ell$. For $g \in R_n$, define its *adjoint* by $g^* \coloneqq g(X^{-1})$. Under the identification $R_n \cong \mathbb{Z}[\zeta]$, this operation corresponds to complex conjugation. For $g, z, w \in R_n$, we have

$$\langle gz, w \rangle = \langle z, g^* w \rangle. \tag{2.3}$$

The inner-product identity follows by linearity because multiplication by X^{-1} is the transpose of multiplication by X. A polynomial g is *skew-adjoint* if $g^* = -g$. In this case, $\langle z, gz \rangle = \langle z, g^* z \rangle = -\langle z, gz \rangle$, so $\langle z, gz \rangle = 0$.

2.3 Ideal and module lattices

An *ideal* $\mathcal{I} \subseteq R_n$ is an additive subgroup closed under multiplication by elements of R_n. More generally, for $r \geq 1$, an *R_n-submodule* $\mathcal{M} \subseteq R_n^r$ is an additive subgroup closed under scalar multiplication by elements of R_n. Under the coefficient embedding, a nonzero ideal of R_n gives an integer lattice in $\mathbb{Z}^n$, called an *ideal lattice* [LPR10]. For $0 \neq f \in R_n$, the *principal ideal* $(f) \coloneqq \{fa : a \in R_n\}$ has coefficient lattice $\mathbf{M}_f \mathbb{Z}^n$. A nonzero R_n-submodule of R_n^r similarly gives a *module lattice* in $\mathbb{Z}^{rn}$. We call an R_n-module *free of rank r* if it has an R_n-basis with r elements. We consider free modules $\mathcal{M} \coloneqq \mathbf{G} R_n^r$, where $\mathbf{G} = (g_{ab}) \in R_n^{r \times r}$ and $\det \mathbf{G} \neq 0$. Their coefficient lattices have integer basis $\mathbf{B} \coloneqq (\mathbf{M}_{g_{ab}})_{1 \leq a, b \leq r} \in \mathbb{Z}^{rn \times rn}$.

We consider the following decision versions of SVP in the coefficient ℓ_∞-norm.

Definition 2.1 (Ideal and module SVP). *Given a power of two n, a nonzero ideal $\mathcal{I} \subseteq R_n$, and a positive integer T, the problem* $\mathsf{IdealSVP}_\infty$ *asks whether $\lambda_{1,\infty}(\mathcal{I}) \leq T$.*

Given a power of two n, a free rank-two R_n-module $\mathcal{M} \subseteq R_n^2$, and a positive integer T, the problem $\mathsf{ModuleSVP}_{\infty,2}$ *asks whether $\lambda_{1,\infty}(\mathcal{M}) \leq T$.*

The corresponding *search*-$\mathsf{IdealSVP}_\infty$ and *search*-$\mathsf{ModuleSVP}_{\infty,2}$ problems take $(n, \mathcal{I})$ and $(n, \mathcal{M})$, respectively, and ask for a nonzero vector of minimum coefficient ℓ_∞-norm in the given ideal or module.

In the problems above, the ideal $\mathcal{I}$ is specified by a $\mathbb{Z}$-basis in R_n, and the free module $\mathcal{M}$ by an R_n-basis matrix $\mathbf{G}$. The coefficient embedding represents these basis elements as integer coefficient vectors. We use their ring representations below.

Lemma 2.2. *The problems* $\mathsf{IdealSVP}_\infty$ *and* $\mathsf{ModuleSVP}_{\infty,2}$ *belong to* NP.

Proof. For either problem, let $r := 1$ for ideals and $r := 2$ for modules. A YES certificate is a vector $\mathbf{y} \in \mathbb{Z}^{rn}$ with $1 \le \|\mathbf{y}\|_\infty \le T$. Its bit length is $O(rn \log(T+1))$. The verifier checks the input conditions and norm bound. It tests lattice membership by solving $\mathbf{Bu} = \mathbf{y}$ over $\mathbb{Q}$ and checking $\mathbf{u} \in \mathbb{Z}^{rn}$, using the coefficient vectors of the supplied ideal basis and the block expansion of $\mathbf{G}$ for modules. For an ideal input, it also applies this test to X times each basis vector, since R_n is generated by X over $\mathbb{Z}$. All these checks take polynomial time [Coh93]. □

2.4 The subset sum problem

Definition 2.3 (Subset Sum). *An instance of* Subset Sum *consists of* $s \ge 1$ *positive integer* weights $w_1, \dots, w_s$ *and a nonnegative* target *integer* B. *It is a* YES instance *if there exists a Boolean vector* $\boldsymbol{\xi} = (\xi_1, \dots, \xi_s) \in \{0,1\}^s$ *such that*

$$\sum_{j=1}^{s} w_j \xi_j = B.$$

We write $W := \sum_{j=1}^{s} w_j$ for the *total weight* and set $\beta := \lceil \log_2(2 + \max\{B, w_1, \dots, w_s\}) \rceil$. Subset Sum is NP-complete [Kar72].

2.5 Complex coefficient representation

Let $n = 2m$, where $m \ge 1$ is a power of two. Under the isomorphism $R_n \cong \mathbb{Z}[\zeta]$, the element X^m corresponds to $\zeta^m = \mathrm{i}$. We write $\mathrm{i} = X^m$ in R_n. Since $\mathrm{i}^2 = -1$, every $z \in R_n$ has a unique representation

$$z = \sum_{j=0}^{m-1} z_j X^j, \qquad z_j := [z]_j + \mathrm{i}[z]_{j+m} \in \mathbb{Z}[\mathrm{i}]. \tag{2.4}$$

We call z_j the j-th *complex coefficient* of z. The ordinary coefficient norm satisfies $\|z\|_\infty = \max_{0 \le j < m} \{|\Re z_j|, |\Im z_j|\}$. For $z, w \in R_n$, the coefficient inner product satisfies $\langle z, w \rangle = \Re \sum_{j=0}^{m-1} \overline{z_j} w_j$. The *support* of the coefficient sequence $(z_0, \dots, z_{m-1})$ is $\{j \in \{0, \dots, m-1\} : z_j \ne 0\}$. The units of $\mathbb{Z}[\mathrm{i}]$ are $1, -1, \mathrm{i}, -\mathrm{i}$.

We also extend the complex coefficients to all integer indices by setting

$$z_{j+qm} := \mathrm{i}^{-q} z_j \qquad (0 \le j < m,\ q \in \mathbb{Z}). \tag{2.5}$$

In particular, $z_{j+m} = -\mathrm{i} z_j$, and $(X^a z)_j = z_{j-a}$ for every integer a and $0 \le j < m$.

Set $d := 1 + \mathrm{i} = 1 + X^m$. To describe the nonzero polynomials satisfying $\|db\|_\infty = 1$, define

$$\mathcal{U}_m := \{0 \ne b \in R_n : b_j \in \{0, \pm 1, \pm \mathrm{i}\} \text{ for } 0 \le j < m\}.$$

Thus $\mathcal{U}_m$ consists of nonzero polynomials whose complex coefficients are zero or units of $\mathbb{Z}[\mathrm{i}]$. Multiplication by d gives the following norm formula.

Lemma 2.4. *For every* $b \in R_n$, *we have*

$$\|db\|_\infty = \max_{0 \le j < m} \big(|\Re b_j| + |\Im b_j| \big). \tag{2.6}$$

In particular, a nonzero $b \in R_n$ *satisfies* $\|db\|_\infty = 1$ *if and only if* $b \in \mathcal{U}_m$. *Every other nonzero* b *satisfies* $\|db\|_\infty \ge 2$.

Proof. For $0 \le j < m$, multiplication by $d = 1 + X^m$ gives

$$([db]_j, [db]_{j+m}) = ([b]_j - [b]_{j+m}, [b]_j + [b]_{j+m}).$$

The identity $\max\{|c - e|, |c + e|\} = |c| + |e|$ for real c, e therefore gives

$$\max\{|[db]_j|, |[db]_{j+m}|\} = |[b]_j| + |[b]_{j+m}| = |\Re b_j| + |\Im b_j|.$$

Taking the maximum over $0 \le j < m$ proves (2.6). Since $b_j \in \mathbb{Z}[\mathrm{i}]$, the quantity $|\Re b_j| + |\Im b_j|$ is at most one exactly when $b_j \in \{0, \pm 1, \pm \mathrm{i}\}$. For nonzero b, the maximum is positive, so the remaining claims follow. □

3 Free modules of rank two

In this section, we encode a Subset Sum instance $(w_1, \dots, w_s; B)$ in a free rank-two module over R_n whose nonzero vectors of ℓ_∞-norm at most M determine solutions to the instance. The module vectors are designed to have the form

$$\begin{pmatrix} hz - (q+v)b \\ Mz \end{pmatrix}, \tag{3.1}$$

where $z \coloneqq 2a - ub$ and $a, b \in R_n$. The polynomials u, h, v, q and the positive integer M will be specified in Section 3.2.

A vector of ℓ_∞-norm at most M in the constructed lattice therefore satisfies $\|z\|_\infty \le 1$ and $\|hz - (q+v)b\|_\infty \le M$. We choose these polynomials so that every nonzero such vector has $b = \pm X^\ell$. Multiplication by b^{-1} then preserves the coefficient ℓ_∞-norm and reduces to $b = 1$. With this normalization, the second module coordinate forces a to have Boolean coefficients, and the bounds on two coefficients of the first coordinate force $\sum_{j=1}^{s} w_j [a]_{j-1} = B$.

3.1 A criterion for signed monomials

Let $m \ge 2$ be a power of two and set $n \coloneqq 2m$. We recall that $d = 1 + X^m$ and that the complex coefficients of $b \in R_n$ are $b_j = [b]_j + \mathrm{i}[b]_{j+m}$, as in (2.4). When the vector in (3.1) has ℓ_∞-norm at most M, we first aim to force a nonzero b to have a single nonzero complex coefficient.

For this purpose, define the polynomials

$$\begin{aligned} p^{(0)} &\coloneqq \sum_{\delta=1}^{m-1} (X^\delta - X^{-\delta}) = (1+\mathrm{i}) \sum_{\delta=1}^{m-1} X^\delta, \\ p^{(1)} &\coloneqq \sum_{\delta=1}^{m-1} \delta (X^\delta - X^{-\delta}) = \sum_{\delta=1}^{m-1} \big(\delta + \mathrm{i}(m-\delta)\big) X^\delta. \end{aligned} \tag{3.2}$$

where we used $X^{-\delta} = -\mathrm{i} X^{m-\delta}$. The proof of the next lemma compares the first and last nonzero complex coefficients of b using $p^{(0)}b$ and $p^{(1)}b$.

Lemma 3.1. *Let $0 \ne b \in R_n$. If $(p^{(0)}b)_j = (p^{(1)}b)_j = 0$ for every $0 \le j < m$ with $b_j \ne 0$, then b has exactly one nonzero complex coefficient.*

Proof. Suppose that b has at least two nonzero complex coefficients, and let $j < r$ be the smallest and largest indices of its nonzero complex coefficients. By (3.2) and (2.5),

$$\begin{aligned} 0 = (p^{(0)}b)_j &= \mathrm{i}(1+\mathrm{i}) \sum_{\ell=j+1}^{r} b_\ell, \\ 0 = (p^{(0)}b)_r &= (1+\mathrm{i}) \sum_{\ell=j}^{r-1} b_\ell. \end{aligned} \tag{3.3}$$

Both sums equal zero, and subtracting them gives $b_j = b_r$.

For $j < \ell \le r$, the $X^{m+j-\ell}$ term of $p^{(1)}$, together with $X^{m+j} = \mathrm{i}X^j$, gives the coefficient $-(1+\mathrm{i})(\ell - j) + \mathrm{i}m$ of b_ℓ in $(p^{(1)}b)_j$. For $j \le \ell < r$, the $X^{r-\ell}$ term gives the coefficient $(1-\mathrm{i})(r-\ell) + \mathrm{i}m$ of b_ℓ in $(p^{(1)}b)_r$. The parts of the coefficients independent of ℓ multiply the zero sums in (3.3), giving

$$\begin{aligned} 0 = (p^{(1)}b)_j &= -(1+\mathrm{i}) \sum_{\ell=j+1}^{r} \ell b_\ell, \\ 0 = (p^{(1)}b)_r &= -(1-\mathrm{i}) \sum_{\ell=j}^{r-1} \ell b_\ell. \end{aligned} \tag{3.4}$$

Subtracting the sums in (3.4) gives $jb_j = rb_r$. Together with $b_j = b_r$, this yields $(r-j)b_j = 0$, contradicting $r > j$ and $b_j \ne 0$. □

For $b \in R_n$ with $\|b\|_\infty \le 1$, the ordinary coefficients of $p^{(0)}b$ are uniformly bounded in terms of m. This allows us to choose an integer α so that the two zero-coefficient conditions in Lemma 3.1 can be expressed using a single polynomial. Define $k \in R_n$ by

$$k \coloneqq p^{(0)} + \alpha p^{(1)} = \sum_{\delta=1}^{m-1} (1 + \alpha\delta)(X^\delta - X^{-\delta}), \tag{3.5}$$

where $\alpha \coloneqq 2m + 1$. This choice of α gives the following equivalence.

Lemma 3.2. *Let $b \in R_n$ satisfy $\|b\|_\infty \le 1$. For every $0 \le j < m$, $(kb)_j = 0$ if and only if $(p^{(0)}b)_j = (p^{(1)}b)_j = 0$.*

Proof. If $(p^{(0)}b)_j = (p^{(1)}b)_j = 0$, then $(kb)_j = 0$ by the definition of k. Conversely, suppose that $(kb)_j = 0$. The identity $(p^{(0)}b)_j = -\alpha(p^{(1)}b)_j$ shows that both the real and imaginary parts of $(p^{(0)}b)_j$ are integers divisible by α. Since $\|b\|_\infty \le 1$, inequality (2.1) gives

$$\left\|p^{(0)}b\right\|_\infty \le \left\|p^{(0)}\right\|_1 \|b\|_\infty \le 2(m-1) < \alpha.$$

Both parts must therefore be zero, and hence $(p^{(0)}b)_j = (p^{(1)}b)_j = 0$. □

We next consider $b \in \mathcal{U}_m$, or equivalently $\|db\|_\infty = 1$ by Lemma 2.4. Lemmas 3.1 and 3.2 give the following criterion for signed monomials.

Corollary 3.3. *Let $b \in \mathcal{U}_m$. If $(kb)_j = 0$ for every $0 \le j < m$ with $b_j \ne 0$, then $b = \pm X^\ell$ for some $0 \le \ell < 2m$.*

Proof. Since $b \in \mathcal{U}_m$, we have $\|b\|_\infty = 1$. Lemmas 3.1 and 3.2 therefore show that b has exactly one nonzero complex coefficient. This coefficient belongs to $\{\pm 1, \pm \mathrm{i}\}$, so $\mathrm{i} = X^m$ gives $b = \pm X^\ell$ for some $0 \le \ell < 2m$. □

Equation (3.2) gives $(p^{(0)})^* = -p^{(0)}$ and $(p^{(1)})^* = -p^{(1)}$. By linearity, $k^* = -k$. For the construction in Section 3.2, we also need the following coefficient identities and norm bounds for k and dk.

Lemma 3.4. *The polynomial k satisfies*

(i) $[k]_0 = [k]_m = [dk]_0 = [dk]_m = 0$.
(ii) $\|dk\|_\infty \le \|k\|_1 < 3m^3$.

Proof. Using $X^{-\delta} = -X^{n-\delta}$ in (3.5), we find that the nonzero ordinary coefficients of k occur at indices $1, \dots, m-1$ and $m+1, \dots, n-1$. Thus $[k]_0 = [k]_m = 0$, and the coefficient calculation in Lemma 2.4 gives

$$([dk]_0, [dk]_m) = ([k]_0 - [k]_m, [k]_0 + [k]_m) = (0, 0).$$

Since $\|d\|_\infty = 1$, inequality (2.1) and the distinct ordinary coefficient positions in (3.5) give

$$\|dk\|_\infty \le \|k\|_1 = 2\sum_{\delta=1}^{m-1} (1 + \alpha\delta) = (m-1)(2 + \alpha m) < 3m^3.$$ □

3.2 The rank-two module construction

We now construct an instance $(n, \mathcal{M}, M)$ of $\mathsf{ModuleSVP}_{\infty,2}$ over the ring $R_n = \mathbb{Z}[X]/(X^n + 1)$ from a Subset Sum instance $(w_1, \dots, w_s; B)$ with $s \ge 1$ positive integer weights and a nonnegative integer target B. Set $W \coloneqq \sum_{j=1}^s w_j$. If $B > W$, the Subset Sum instance is a NO instance. In this case, we set $\mathcal{M} \coloneqq 2R_2^2$ with basis $2\mathbf{I}_2$ and output $(2, \mathcal{M}, 1)$.

We assume $0 \le B \le W$ from now on. We choose the least power of two $m > s$ and set $n \coloneqq 2m$.

Step 1. Encoding the instance. We first specify the positions of the Boolean variables using the polynomial $u \coloneqq \sum_{j=1}^s X^{j-1}$, whose coefficients are 1 at indices $0, \dots, s-1$ and 0 elsewhere.

To obtain the weighted sum in the constant coefficient, we define $\tilde{h} \coloneqq \sum_{j=1}^{s} w_j X^{-(j-1)}$, so that $[\tilde{h}a]_0 = \sum_{j=1}^{s} w_j [a]_{j-1}$ for $a \in R_n$. We then set

$$h \coloneqq (1 - X^m)\tilde{h}, \qquad v \coloneqq (2B - W)(1 - X^m). \tag{3.6}$$

For $b = 1$ and $a = \sum_{j=1}^{s} \xi_j X^{j-1}$ with $\xi_j \in \{0, 1\}$ and $z = 2a - u$, the constant coefficient and the coefficient of X^m in $hz - v$ are $2(\sum_{j=1}^{s} w_j \xi_j - B)$ and its negative, respectively.

Step 2. Constructing the module. Since $0 \le B \le W$, we have $\|h\|_1 \le 2\left\|\tilde{h}\right\|_1 = 2W$ and $\|v\|_1 = 2|2B - W| \le 2W$. Recall that $d = 1 + X^m$. We choose L and M and define q by

$$L \coloneqq 4W + 1, \qquad M \coloneqq 2L\|k\|_1 + 6W + 1, \qquad q \coloneqq Md + Ldk. \tag{3.7}$$

We define the generator matrix

$$\mathbf{G} \coloneqq \begin{pmatrix} 2h & -hu - q - v \\ 2M & -Mu \end{pmatrix} \in R_n^{2\times 2}. \tag{3.8}$$

Let $\mathcal{M} \coloneqq \mathbf{G}R_n^2$. With $z \coloneqq 2a - ub$ for $a, b \in R_n$, we have

$$\mathbf{G}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} hz - (q + v)b \\ Mz \end{pmatrix}. \tag{3.9}$$

We output the instance $(n, \mathcal{M}, M)$.

3.3 Proof of the reduction

We first verify the signed-monomial restriction and compute the exact norm for Boolean choices. We then establish the correctness and polynomial running time of the reduction in Section 3.2.

Lemma 3.5. *Let h, v, L, M, q be defined by (3.6) and (3.7), with $0 \le B \le W$. Let $b, z \in R_n$ satisfy $\|z\|_\infty \le 1$ and*

$$\|hz - (q + v)b\|_\infty \le M. \tag{3.10}$$

Then either $b = 0$ or $b = \pm X^\ell$ for some $0 \le \ell < n$.

Proof. Assume $b \neq 0$. To apply Corollary 3.3, we show that $b \in \mathcal{U}_m$ and $(kb)_j = 0$ for every j with $b_j \neq 0$. Set $e \coloneqq vb - hz$ and $t \coloneqq \|db\|_\infty$.

By Lemma 2.4, the condition $b \in \mathcal{U}_m$ is equivalent to $t = 1$. We first compare Mdb with the possible cancellation from $Ldkb + e$ to rule out $t \ge 2$. Equation (2.6) gives $1 \le \|b\|_\infty \le t$. Using (2.1) and the bounds $\|h\|_1, \|v\|_1 \le 2W$, we obtain

$$\|e\|_\infty \le 2W(t + 1), \qquad \|dkb\|_\infty \le \|k\|_1 t.$$

By (3.10) and the definition of q, we have $\|Mdb + Ldkb + e\|_\infty \le M$. If $t \ge 2$, the triangle inequality gives

$$\begin{aligned} \|Mdb + Ldkb + e\|_\infty &\ge Mt - L\|dkb\|_\infty - \|e\|_\infty \\ &\ge (M - L\|k\|_1 - 2W)t - 2W \\ &\ge M + 1. \end{aligned}$$

The last inequality follows from $t \ge 2$ and the definition of M. This contradicts (3.10). Since t is a positive integer, we conclude that $t = 1$. Lemma 2.4 gives $b \in \mathcal{U}_m$, and $\|e\|_\infty \le 4W = L - 1$.

We next use $k^* = -k$ to prove that $(kb)_j = 0$ for every j with $b_j \neq 0$. Fix $0 \le \ell < n$ with $[db]_\ell \neq 0$. Since $\|db\|_\infty = 1$, we have $[db]_\ell \in \{-1, 1\}$. Multiplying the expression inside $|M[db]_\ell + L[dkb]_\ell + [e]_\ell| \le M$ by $[db]_\ell$ and using $[db]_\ell^2 = 1$ gives

$$M + L[db]_\ell[dkb]_\ell + [db]_\ell[e]_\ell \le M.$$

Subtracting M and using $\|e\|_\infty \le L - 1$ yields

$$L[db]_\ell[dkb]_\ell \le -[db]_\ell[e]_\ell \le |[e]_\ell| \le L - 1 < L.$$

By integrality, $[db]_\ell[dkb]_\ell \le 0$. At a position where $[db]_\ell = 0$, the product is zero. Since $k^* = -k$, we also have

$$\sum_{\ell=0}^{n-1} [db]_\ell [dkb]_\ell = \langle db, k(db)\rangle = 0.$$

Every summand is nonpositive, so each is zero. Hence $[dkb]_\ell = 0$ for every ℓ with $[db]_\ell \neq 0$.

For every j with $b_j \neq 0$, we have $b_j \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$. Both the real and imaginary parts of $(1+\mathrm{i})b_j$ are therefore nonzero, so $[db]_j$ and $[db]_{j+m}$ are nonzero. Consequently $[dkb]_j = [dkb]_{j+m} = 0$, and hence $(dkb)_j = (1+\mathrm{i})(kb)_j = 0$. Since $1+\mathrm{i} \neq 0$, we obtain $(kb)_j = 0$ for every j with $b_j \neq 0$. Corollary 3.3 yields $b = \pm X^\ell$. □

The next lemma computes the norm of the vector in (3.9) for $b = 1$ and Boolean choices.

Lemma 3.6. *Let* $\mathbf{G}$ *be given by* (3.8) *with the choices in* (3.6) *and* (3.7)*, where* $0 \le B \le W$*. For* $\boldsymbol{\xi} \in \{0,1\}^s$*, set* $a := \sum_{j=1}^{s} \xi_j X^{j-1}$*. Then*

$$\left\| \mathbf{G} \begin{pmatrix} a \\ 1 \end{pmatrix} \right\|_\infty = \left\| \begin{pmatrix} h(2a-u) - q - v \\ M(2a-u) \end{pmatrix} \right\|_\infty = M + 2\left| \sum_{j=1}^{s} w_j \xi_j - B \right|. \tag{3.11}$$

Proof. Set $A := \sum_{j=1}^{s} w_j \xi_j$ and $z := 2a - u = \sum_{j=1}^{s} (2\xi_j - 1) X^{j-1}$. Then $\|z\|_\infty = 1$. Expanding gives

$$\tilde{h}z = \sum_{j,\ell=1}^{s} w_j (2\xi_\ell - 1) X^{\ell - j}.$$

Every exponent lies in $[-s+1, s-1] \subseteq [-m+1, m-1]$. Thus only the terms with $j = \ell$ contribute to the constant coefficient, and the coefficient of X^m is zero. Hence

$$[\tilde{h}z]_0 = \sum_{j=1}^{s} w_j (2\xi_j - 1) = 2A - W, \qquad [\tilde{h}z]_m = 0.$$

From $h = (1 - X^m)\tilde{h}$ and $v = (2B - W)(1 - X^m)$, we obtain $[hz - v]_0 = 2(A - B)$ and $[hz - v]_m = -2(A - B)$. Also, $q = Md + Ldk$ and Lemma 3.4(i) give $[q]_0 = [q]_m = M$. Therefore

$$\begin{aligned} [hz - q - v]_0 &= -M + 2(A - B), \\ [hz - q - v]_m &= -M - 2(A - B). \end{aligned} \tag{3.12}$$

The two coefficients in (3.12) satisfy

$$\max\{|-M + 2(A-B)|,\ |-M - 2(A-B)|\} = M + 2|A - B| \ge M.$$

At every position $\ell \notin \{0, m\}$, the coefficients of Md and v are zero. Since $\|hz\|_\infty \le 2W$ by (2.1), Lemma 3.4(ii) gives

$$|[hz - q - v]_\ell| \le \|hz\|_\infty + L\,\|dk\|_\infty \le 2W + L\|k\|_1 < M.$$

Thus $\|hz - q - v\|_\infty = M + 2|A - B|$. Since $\|Mz\|_\infty = M$, equation (3.9) gives (3.11). □

We now verify the reduction.

Theorem 3.7. *There exists a deterministic polynomial-time reduction from* Subset Sum *to* $\mathsf{ModuleSVP}_{\infty,2}$ *that maps each instance to an instance* $(n, \mathcal{M}, M)$*, where* $\mathcal{M} = \mathbf{G}R_n^2$ *is a free rank-two module lattice over* R_n*. The first minimum of* $\mathcal{M}$ *is* M *on YES instances and at least* $M + 1$ *on NO instances. Consequently,* $\mathsf{ModuleSVP}_{\infty,2}$ *is* NP*-complete for free rank-two modules over* R_n*, where* n *ranges over powers of two.*

Proof. For $B > W$, the output module $\mathcal{M} = 2R_2^2$ has first minimum 2. Assume $0 \le B \le W$. By Lemma 3.4(i), $[q + v]_0 = M + 2B - W \ge M - W > 0$. Since R_n is an integral domain, $\det \mathbf{G} = 2M(q + v) \neq 0$, so $\mathbf{G}$ defines a free module of rank two.

Every solution to the Subset Sum instance gives a nonzero vector of norm M by Lemma 3.6. Conversely, let $\mathbf{G}\binom{a}{b}$ be a nonzero vector of norm at most M, and put $z \coloneqq 2a - ub$. Equation (3.9) gives $\|z\|_\infty \le 1$ and $\|hz - (q+v)b\|_\infty \le M$, so Lemma 3.5 gives $b = 0$ or $b = \pm X^\ell$. The case $b = 0$ would force $\|2a\|_\infty \le 1$ and hence $a = 0$, contrary to the vector being nonzero. Thus $b = \pm X^\ell$. Multiplying the vector by b^{-1} preserves its coefficient norm, so we may replace a by ab^{-1} and assume $b = 1$.

Now $\|2a - u\|_\infty \le 1$ forces $[a]_j \in \{0,1\}$ for $0 \le j < s$ and $[a]_j = 0$ for $s \le j < n$. Hence

$$a = \sum_{j=1}^{s} \xi_j X^{j-1},$$

where $\boldsymbol{\xi} \in \{0,1\}^s$. Lemma 3.6 gives $M + 2\left|\sum_{j=1}^{s} w_j\xi_j - B\right| \le M$, forcing $\sum_{j=1}^{s} w_j\xi_j = B$ and the vector norm to equal M. Therefore the first minimum is M on a YES instance and at least $M+1$ on a NO instance by integrality.

The choice of m gives $m \le 2s$, so the integer lattice dimension is $2n \le 8s$. Since $L = O(W)$ and $\|k\|_1 = O(m^3)$, we have $M = O(m^3W) = O(s^3W)$. Also, $\|hu\|_\infty \le 2W$ and

$$\|-hu - q - v\|_\infty \le 2W + M + L\|k\|_1 + 2W < 2M.$$

The coefficients of the other entries $2h$, $-Mu$, and $2M$ also have absolute value at most $2M$. Thus the output has $O(s(\log s + \log W))$ bits, and the explicit formulas give a deterministic polynomial-time construction. Membership in NP follows from Lemma 2.2. □

The proof of Theorem 3.7 also gives the following corollary. Comparing the norm of a shortest vector with M decides the source Subset Sum instance, and on a YES instance the proof recovers a solution in polynomial time.

Corollary 3.8. *Search-*ModuleSVP$_{\infty,2}$ *is* NP*-hard for free rank-two modules over R_n under polynomial-time Turing reductions, where n ranges over powers of two.*

4 Principal ideals

In this section, we encode a Subset Sum instance $(w_1, \dots, w_s; B)$ in a principal ideal $(f) \subseteq R_n$ whose nonzero vectors of ℓ_∞-norm at most T determine solutions to the instance. We choose a generator of the form $f = (T + C - g)d$, where $d = 1 + X^m$. The polynomial g and the positive integers T, C will be specified in Section 4.2.

We choose T so that every nonzero vector fb satisfying $\|fb\|_\infty \le T$ has $\|db\|_\infty = 1$, and hence $b \in \mathcal{U}_m$ by Lemma 2.4. The indices j with $b_j \neq 0$ encode the Boolean choices. We construct g so that all nonzero complex coefficients of b become 1 after multiplication by a power of X. Their indices then consist of 0 and one index in each of s separated three-element sets. The position chosen in each set gives a Boolean value $\xi_h \in \{0,1\}$. The bounds on the ordinary coefficients at indices 0 and m then force $\sum_{h=1}^{s} w_h\xi_h = B$.

4.1 Norm identities and support restrictions

Let $m \ge 2$ be a power of two and set $n \coloneqq 2m$. Recall that $d = 1 + \mathrm{i} = 1 + X^m$, and use the complex coefficients in (2.4). We first prove the norm identities with a positive integer M as the main-term coefficient. The construction in Section 4.2 takes $M = T + C$. For $g \in R_n$, define

$$f \coloneqq (M - g)d. \tag{4.1}$$

We first compare $\|fb\|_\infty$ for arbitrary nonzero $b \in R_n$. The triangle inequality and (2.1) give

$$(M - \|g\|_1)\,\|db\|_\infty \le \|fb\|_\infty \le (M + \|g\|_1)\,\|db\|_\infty\,. \tag{4.2}$$

By Lemma 2.4, $\|db\|_\infty = 1$ for $b \in \mathcal{U}_m$, whereas $\|db\|_\infty \ge 2$ for every other nonzero b. In particular, $\|f\sigma\|_\infty \le M + \|g\|_1$ for every $\sigma \in \mathcal{U}_m$. We assume $M > 3\,\|g\|_1$, so that $2(M - \|g\|_1) > M + \|g\|_1$. Thus $f \neq 0$, and every shortest nonzero vector of (f) has the form $f\sigma$ with $\sigma \in \mathcal{U}_m$.

It therefore suffices to determine the coefficient ℓ_∞-norm of $f\sigma$ for $\sigma \in \mathcal{U}_m$. If $\sigma_j \neq 0$, both $[d\sigma]_j$ and $[d\sigma]_{j+m}$ belong to $\{-1, 1\}$, so the corresponding coefficients of $Md\sigma$ have absolute value M. For $\ell \in \{j, j+m\}$, multiplying inside the absolute value by $[d\sigma]_\ell$ gives

$$|[f\sigma]_\ell| = \big|M - [d\sigma]_\ell [dg\sigma]_\ell\big|.$$

For $0 \leq j < m$ with $\sigma_j \neq 0$, define

$$\phi_j^{\pm}(g, \sigma) \coloneqq \Re\big(\overline{\sigma_j}(g\sigma)_j\big) \pm \Im\big(\overline{\sigma_j}(g\sigma)_j\big). \tag{4.3}$$

If $\overline{\sigma_j}(g\sigma)_j = x + \mathrm{i}y$, then the minimum decrease in absolute value of the two ordinary coefficients at j and $j+m$ is $\min\{x - y, x + y\} = x - |y|$ by Lemma 4.1. For fixed σ and j, the maps $g \mapsto \phi_j^{\pm}(g, \sigma)$ take values in $\mathbb{Z}$ and are $\mathbb{Z}$-linear. In particular, $\phi_j^{\pm}(cg + t, \sigma) = c\phi_j^{\pm}(g, \sigma) + \phi_j^{\pm}(t, \sigma)$ for $c \in \mathbb{Z}$ and $g, t \in R_n$. The following lemma expresses the absolute values of the ordinary coefficients of $f\sigma$ at j and $j+m$ as $|M - \phi_j^{\pm}(g, \sigma)|$.

Lemma 4.1. *Let $g \in R_n$ and $\sigma \in \mathcal{U}_m$. For every $0 \leq j < m$ with $\sigma_j \neq 0$,*

$$\big\{[d\sigma]_j [dg\sigma]_j,\ [d\sigma]_{j+m} [dg\sigma]_{j+m}\big\} = \big\{\phi_j^-(g, \sigma),\ \phi_j^+(g, \sigma)\big\}.$$

Moreover, $|\phi_j^{\pm}(g, \sigma)| \leq \|g\|_1$.

Proof. Fix $0 \leq j < m$ with $\sigma_j \neq 0$ and write $\overline{\sigma_j}(g\sigma)_j = x + \mathrm{i}y$ with $x, y \in \mathbb{R}$. By (4.3), $\phi_j^-(g, \sigma) = x - y$ and $\phi_j^+(g, \sigma) = x + y$. Since $\sigma_j \overline{\sigma_j} = 1$, we have $(g\sigma)_j = \sigma_j(x + \mathrm{i}y)$. Multiplication by $d = 1 + \mathrm{i}$ gives

$$d(x + \mathrm{i}y) = x + \mathrm{i}y + \mathrm{i}x - y = (x - y) + \mathrm{i}(x + y).$$

Hence $(d\sigma)_j = \sigma_j(1 + \mathrm{i})$ and $(dg\sigma)_j = \sigma_j\big((x - y) + \mathrm{i}(x + y)\big)$. Computing the ordinary coefficient products yields

$$\big([d\sigma]_j [dg\sigma]_j,\ [d\sigma]_{j+m} [dg\sigma]_{j+m}\big) = \begin{cases} (x - y, x + y), & \sigma_j \in \{1, -1\}, \\ (x + y, x - y), & \sigma_j \in \{\mathrm{i}, -\mathrm{i}\}. \end{cases}$$

In both cases, the unordered pair is $\{\phi_j^-(g, \sigma), \phi_j^+(g, \sigma)\}$, proving the identity.

By Lemma 2.4, $\|d\sigma\|_\infty = 1$. Inequality (2.1) therefore gives

$$\|dg\sigma\|_\infty \leq \|g\|_1 \|d\sigma\|_\infty = \|g\|_1.$$

Since $[d\sigma]_j, [d\sigma]_{j+m} \in \{-1, 1\}$, this also bounds $|\phi_j^{\pm}(g, \sigma)|$. □

For $\sigma \in \mathcal{U}_m$, define the minimum of $\phi_j^{\pm}(g, \sigma)$ over all indices j with $\sigma_j \neq 0$ by

$$\theta_g(\sigma) \coloneqq \min_{\substack{0 \leq j < m \\ \sigma_j \neq 0}} \min\{\phi_j^+(g, \sigma), \phi_j^-(g, \sigma)\}.$$

The following lemma shows how $\theta_g(\sigma)$ determines the coefficient ℓ_∞-norm of $f\sigma$.

Lemma 4.2. *Assume $M > 3\|g\|_1$, and let f be defined by (4.1). For every $\sigma \in \mathcal{U}_m$, we have $\|f\sigma\|_\infty = M - \theta_g(\sigma)$.*

Proof. We compute the absolute values of the ordinary coefficients of $f\sigma$ for $\sigma \in \mathcal{U}_m$. Fix $0 \leq j < m$. If $\sigma_j \neq 0$, equation (4.1) and Lemma 4.1 give $|M - \phi_j^{\pm}(g, \sigma)|$ as the two absolute values at indices j and $j + m$. Since $|\phi_j^{\pm}(g, \sigma)| \leq \|g\|_1 < M$, these equal $M - \phi_j^{\pm}(g, \sigma) \geq M - \|g\|_1$. If $\sigma_j = 0$, both $[d\sigma]_j$ and $[d\sigma]_{j+m}$ are zero, so for $\ell \in \{j, j + m\}$,

$$|[f\sigma]_\ell| = |[dg\sigma]_\ell| \leq \|g\|_1 < M - \|g\|_1.$$

Taking the maximum over all ordinary coefficients therefore gives $\|f\sigma\|_\infty = M - \theta_g(\sigma)$. □

For $\sigma \in \mathcal{U}_m$, Lemma 4.2 shows that $\|f\sigma\|_\infty \le M$ if and only if $\theta_g(\sigma) \ge 0$. Since multiplication by X^ℓ permutes the ordinary coefficients of $f\sigma$ up to sign, $\|f(X^\ell\sigma)\|_\infty = \|f\sigma\|_\infty$ for every integer ℓ. The norm bound therefore cannot distinguish a common cyclic translation of the indices of nonzero complex coefficients. We choose g so that $\theta_g(\sigma) \ge 0$ restricts the cyclic distances between these indices.

The *cyclic distance* between $j, \ell \in \{0, \dots, m-1\}$ is defined as $\min\{|j-\ell|, m-|j-\ell|\}$. This counts the steps along the shorter of the two paths between j and ℓ around the cycle. Let $E \subseteq \{1, \dots, m/2\}$ be the set of allowed nonzero cyclic distances, and order the elements of $\{1, \dots, m/2\} \setminus E$ as $\Delta_0 < \Delta_1 < \cdots < \Delta_{r-1}$, where $r := m/2 - |E|$.

To exclude a cyclic distance $\delta \notin E$ between indices of nonzero complex coefficients, we require $\sigma_{j-\delta} - \sigma_{j+\delta} = 0$ for every j with $\sigma_j \neq 0$. As we will show in Lemma 4.3, if σ_j and $\sigma_{j+\delta}$ were both nonzero, these equalities would force $(\sigma_{j+\nu\delta})_{\nu\in\mathbb{Z}}$ to be nonzero and 2-periodic. For power-of-two m, this contradicts (2.5). The difference $\sigma_{j-\delta} - \sigma_{j+\delta}$ is the j-th complex coefficient of $(X^\delta - X^{-\delta})\sigma$. We combine these differences over the distances outside E and define

$$a_E := \sum_{\nu=0}^{r-1} 5^\nu (X^{\Delta_\nu} - X^{-\Delta_\nu}). \tag{4.4}$$

The powers of 5 separate the coefficient conditions for different distances. For $\sigma \in \mathcal{U}_m$, requiring $(a_E\sigma)_j = 0$ at every index j with $\sigma_j \neq 0$ excludes pairs of nonzero complex coefficients at cyclic distances outside E. The next lemma proves this implication and shows how to choose g so that $\theta_g(\sigma) \ge 0$ forces these zero coefficients.

Lemma 4.3. *Let $\sigma \in \mathcal{U}_m$. Then $(a_E\sigma)_j = 0$ for every j with $\sigma_j \neq 0$ if and only if all pairwise cyclic distances between the positions of the nonzero complex coefficients of σ belong to E. Moreover, let $t \in R_n$, and set $L := \|t\|_1 + 1$ and $g := La_E + t$. If $\theta_g(\sigma) \ge 0$, both conditions hold.*

Proof. We first prove the equivalence. If all pairwise cyclic distances between indices of nonzero complex coefficients belong to E, then $\sigma_{j-\delta} = \sigma_{j+\delta} = 0$ for every j with $\sigma_j \neq 0$ and $\delta \in \{1, \dots, m/2\} \setminus E$, so (4.4) gives $(a_E\sigma)_j = 0$.

Conversely, suppose that $(a_E\sigma)_j = 0$ for every j with $\sigma_j \neq 0$, and fix $0 \le j < m$ with $\sigma_j \neq 0$. Using (2.5), we compute the j-th complex coefficient of $a_E\sigma$ as

$$(a_E\sigma)_j = \sum_{\nu=0}^{r-1} 5^\nu (\sigma_{j-\Delta_\nu} - \sigma_{j+\Delta_\nu}) = 0.$$

For every $0 \le \nu < r$, the real and imaginary parts of $\sigma_{j-\Delta_\nu} - \sigma_{j+\Delta_\nu}$ lie in $\{-2, -1, 0, 1, 2\}$. If $r > 0$, reduction modulo 5 gives $\sigma_{j-\Delta_0} = \sigma_{j+\Delta_0}$. Dividing by 5 and repeating the argument gives

$$\sigma_{j-\delta} = \sigma_{j+\delta}, \tag{4.5}$$

for every $\delta \in \{1, \dots, m/2\} \setminus E$. By (2.5), shifting j by qm for any $q \in \mathbb{Z}$ multiplies both sides of (4.5) by i^{-q}. Thus (4.5) holds for every $j \in \mathbb{Z}$ with $\sigma_j \neq 0$.

Suppose two indices of nonzero complex coefficients have cyclic distance $\delta \notin E$. Choose $j \in \mathbb{Z}$ so that $a_0 := \sigma_j$ and $a_1 := \sigma_{j+\delta}$ are nonzero, and define $a_\nu := \sigma_{j+\nu\delta}$ for every $\nu \in \mathbb{Z}$. If $a_\nu \neq 0$, equation (4.5) gives $a_{\nu-1} = a_{\nu+1}$. Starting from $a_0, a_1 \neq 0$ and inducting in both directions shows that every a_ν is nonzero and $a_{\nu+2} = a_\nu$.

Set $\eta := \gcd(m, \delta)$, $\ell := m/\eta$, and $q := \delta/\eta$. Since m is a power of two and $1 \le \delta \le m/2$, ℓ is even and q is odd. Since $\ell\delta = qm$, the 2-periodicity and (2.5) give

$$a_0 = a_\ell = \sigma_{j+\ell\delta} = \sigma_{j+qm} = \mathrm{i}^{-q} a_0.$$

Since q is odd, $\mathrm{i}^{-q} \in \{\mathrm{i}, -\mathrm{i}\}$. The equality $a_0 = \mathrm{i}^{-q} a_0$ therefore implies $a_0 = 0$, contrary to the choice $a_0 = \sigma_j \neq 0$. Thus all pairwise cyclic distances between the indices of nonzero complex coefficients belong to E.

Finally, assume that $\theta_g(\sigma) \ge 0$. For every $0 \le j < m$ with $\sigma_j \neq 0$, linearity and Lemma 4.1 give

$$0 \le \phi_j^\pm(g, \sigma) = L\phi_j^\pm(a_E, \sigma) + \phi_j^\pm(t, \sigma) \le L\phi_j^\pm(a_E, \sigma) + L - 1.$$

Hence $\phi_j^\pm(a_E, \sigma) > -1$, and integrality gives $\phi_j^\pm(a_E, \sigma) \ge 0$.

By linearity and (4.4), $a_E{}^* = -a_E$. Using (2.3), the complex coefficient representation, and (4.3), we obtain

$$\begin{aligned}\sum_{\substack{0\le j<m\\ \sigma_j\neq 0}} \big(\phi_j^+(a_E,\sigma)+\phi_j^-(a_E,\sigma)\big) &= 2\Re\sum_{j=0}^{m-1}\overline{\sigma_j}(a_E\sigma)_j \\ &= 2\sum_{\ell=0}^{2m-1}[\sigma]_\ell[a_E\sigma]_\ell = 2\langle\sigma, a_E\sigma\rangle = 0.\end{aligned} \tag{4.6}$$

Since each $\phi_j^{\pm}(a_E,\sigma)$ is nonnegative, equation (4.6) gives

$$\phi_j^+(a_E,\sigma)=\phi_j^-(a_E,\sigma)=0$$

for every j with $\sigma_j\neq 0$. Taking the sum and difference in (4.3) gives $\overline{\sigma_j}(a_E\sigma)_j=0$. Since $\sigma_j\neq 0$, we obtain $(a_E\sigma)_j=0$. The distance condition follows from the equivalence. □

4.2 The principal-ideal construction

We now construct an instance $(n,(f),T)$ of $\mathsf{IdealSVP}_\infty$ over $R_n=\mathbb{Z}[X]/(X^n+1)$ from a given Subset Sum instance. Let $(w_1,\dots,w_s;B)$ have $s\ge 1$ positive integer weights and a nonnegative integer target B, and set $W\coloneqq\sum_{h=1}^{s}w_h$.

Step 1. Encoding Boolean choices. We encode the Boolean choices in the indices of the nonzero complex coefficients of σ, using s three-element sets. Set $V\coloneqq 8s+1$ and $m\coloneqq\min\{2^\ell : 2^\ell > 4V\}$, and define

$$E\coloneqq\bigcup_{h=1}^{s}\{8h-1,8h,8h+1\}. \tag{4.7}$$

Here $V=\max E$ is the largest allowed distance. If the indices j with $\sigma_j\neq 0$ for $\sigma\in\mathcal{U}_m$ have pairwise cyclic distances in E, Lemma 4.4 applies. After a common cyclic translation modulo m, each three-element set then contains at most one such index. Set $n\coloneqq 2m$ and form a_E by (4.4).

Step 2. Assigning the weights. Within each three-element set $\{8h-1,8h,8h+1\}$, a nonzero complex coefficient at $8h$ encodes $\xi_h=0$ and does not include w_h in the subset, while one at $8h\pm 1$ encodes $\xi_h=1$ and includes w_h. Set $H\coloneqq W+1$. We assign weight H to position $8h$ and weight $H+w_h$ to each of the positions $8h\pm 1$. The shifts X^{-8h} and $X^{-(8h\pm1)}$ bring the corresponding complex coefficients to index 0. If the h-th set contains no nonzero complex coefficient, its base weight H is missing. Lemma 4.5 uses $H>W$ to rule out empty sets. We define

$$v\coloneqq \mathrm{i}\Big(\sum_{h=1}^{s}\Big[HX^{-8h}+(H+w_h)(X^{-(8h-1)}+X^{-(8h+1)})\Big]-(sH+B)\Big).$$

We use the factor i to place the subset-sum difference in the imaginary part of $(v\sigma)_0$. Multiplication by $d=1+\mathrm{i}$ makes this difference contribute with opposite signs to the ordinary coefficients at indices 0 and m. We will set their common baseline at the norm bound, so a nonzero difference forces at least one absolute value above that bound.

The $3s+1$ integer exponents $0,-8h,-(8h\pm1)$, $1\le h\le s$, are distinct and lie in $[-V,0]$. Since $V<m/4<2m$, these exponents remain distinct modulo $2m$, so their monomials do not combine in R_n. Since multiplication by i permutes ordinary coefficients up to sign, $\|v\|_1=4sH+2W+B$. We choose $C\coloneqq\|v\|_1+1$. By Lemma 4.1, this choice gives $|\phi_j^{\pm}(v,\sigma)|\le C-1$ for $\sigma\in\mathcal{U}_m$ and $0\le j<m$ with $\sigma_j\neq 0$.

Once the indices of nonzero complex coefficients of σ have pairwise cyclic distances in E and every three-element set contains exactly one index j with $\sigma_j\neq 0$, Lemma 4.4 gives gaps in $\{7,8,9\}$ between consecutive indices of nonzero complex coefficients in $[0,V]$. After normalizing σ_0 to 1, we force every other nonzero complex coefficient to equal 1 by comparing coefficients at consecutive nonzero positions. We therefore define $t_0\coloneqq C\sum_{\nu=7}^{9}(2X^\nu+X^{-\nu})$. At a nonzero position between the endpoints, multiplication by t_0 combines the preceding and following complex coefficients with weights $2C$ and C, respectively. With $\theta_g(\sigma)\ge C$, the weights $2C$ and C force consecutive nonzero complex coefficients of σ to agree, as proved in Lemma 4.5.

Step 3. Constructing the ideal. The nonzero ordinary coefficients of t_0 have indices in $[7,9] \cup [2m-9, 2m-7]$, and those of v have indices in $[m-V, m]$. These index sets do not intersect because $9 \le V < m/4$. Hence $\|t_0 + v\|_1 = 9C + (C-1) = 10C - 1$. To apply Lemma 4.3, define

$$g \coloneqq 10Ca_E + t_0 + v. \tag{4.8}$$

With $d = 1 + \mathrm{i} = 1 + X^m$, choose the norm bound $T \coloneqq 3\|g\|_1 + 1$ and set $M \coloneqq T + C$. We define

$$f \coloneqq (T + C - g)d. \tag{4.9}$$

Suppose that σ has complex coefficient 1 at 0 and at one index in each three-element set, and zero elsewhere. Set $Z \coloneqq \sum_{h=1}^{s} w_h \xi_h - B$. Then $(g\sigma)_0 = C + \mathrm{i}Z$, so the ordinary coefficients of $f\sigma$ at 0 and m are $T + Z$ and $T - Z$. A nonzero Z makes one of these coefficients have absolute value greater than T, as proved in Lemma 4.6.

We output the instance $(n, (f), T)$ with the integer basis $\mathbf{M}_f$ from (2.2).

The next lemma describes the indices allowed by the distance condition for E. After a common cyclic translation modulo m, the indices outside the origin lie in distinct three-element sets, with all nonzero offsets from the centers $8h$ having the same sign.

Lemma 4.4. *Let $J \subseteq \{0, \dots, m-1\}$ have $\ell \ge 1$ elements whose pairwise cyclic distances belong to E. There exists $\tau \in \{0, \dots, m-1\}$ such that, after the cyclic translation $j \mapsto j + \tau \pmod m$, the translated indices have least nonnegative representatives ordered as*

$$0 = p_0 < p_1 < \cdots < p_{\ell-1} \le V.$$

Moreover, $p_j = 8\kappa_j + \delta_j$ for $1 \le j < \ell$, where the κ_j are strictly increasing in $\{1, \dots, s\}$, and either all δ_j lie in $\{0, 1\}$ or all lie in $\{-1, 0\}$. In particular, $\ell \le s + 1$.

Proof. We first apply a cyclic translation that sends one element of J to 0 modulo m, preserving all pairwise cyclic distances. Since $E \subseteq [1, V]$, all indices have representatives in $[-V, V]$. The difference between the largest and smallest representatives is at most $2V < m/2$, so it equals their cyclic distance and is at most V. Subtracting the smallest representative gives $0 = p_0 < \cdots < p_{\ell-1} \le V$.

For $1 \le j < \ell$, we have $p_j \le V < m/2$, so the cyclic distance from 0 to p_j is p_j. Each positive p_j belongs to E and has a unique expression $p_j = 8\kappa_j + \delta_j$ with $1 \le \kappa_j \le s$ and $\delta_j \in \{-1, 0, 1\}$. Distinct elements of one three-element set have distance at most 2, whereas $\min E = 7$. Hence the positive indices p_j lie in distinct sets, ordered by their centers $8h$, so the κ_j are strictly increasing. This gives $\ell \le s + 1$, with $\kappa_j = j$ for $1 \le j \le s$ when $\ell = s + 1$.

For $1 \le c < j < \ell$, we have $p_j - p_c = 8(\kappa_j - \kappa_c) + (\delta_j - \delta_c) \in E$. Reducing modulo 8 and using $|\delta_j - \delta_c| \le 2$ gives $\delta_j - \delta_c \in \{-1, 0, 1\}$. Hence 1 and -1 cannot both occur among the δ_j, so all δ_j lie in $\{0, 1\}$ or all lie in $\{-1, 0\}$. □

4.3 Proof of the reduction

For $\sigma \in \mathcal{U}_m$, Lemma 4.2 with $M = T + C$ gives $\|f\sigma\|_\infty \le T$ if and only if $\theta_g(\sigma) \ge C$. Every nonzero $b \in R_n \setminus \mathcal{U}_m$ satisfies $\|fb\|_\infty \ge 2(T + C - \|g\|_1) > T$ by (4.2) and Lemma 2.4, so it suffices to consider $\sigma \in \mathcal{U}_m$. We first determine the positions and values of the nonzero complex coefficients of σ, then test the subset-sum equation.

Lemma 4.5. *For g constructed in Section 4.2, let $\sigma \in \mathcal{U}_m$ satisfy $\theta_g(\sigma) \ge C$. After multiplication by a power of X, σ has the form*

$$\sigma = 1 + \sum_{h=1}^{s} X^{8h + \delta_h},$$

where either all δ_h lie in $\{0, 1\}$ or all lie in $\{-1, 0\}$.

Proof. For every integer ν, we have $X^\nu \sigma \in \mathcal{U}_m$ and $\|f(X^\nu\sigma)\|_\infty = \|f\sigma\|_\infty$, since multiplication by X^ν permutes ordinary coefficients up to sign. Applying the norm identity in Lemma 4.2 with $M = T + C$ to σ and $X^\nu\sigma$ gives $\theta_g(X^\nu\sigma) = \theta_g(\sigma)$.

Since $\theta_g(\sigma) \ge C > 0$ and $\|t_0 + v\|_1 = 10C - 1$, Lemma 4.3 with $t = t_0 + v$ and $L = 10C$ shows that all pairwise cyclic distances between the indices of nonzero complex coefficients of σ belong to E.

By Lemma 4.4, a cyclic translation puts the indices of the nonzero complex coefficients of σ in the form $0 = p_0 < p_1 < \cdots < p_{\ell-1} \le V$, with $p_j = 8\kappa_j + \delta_j$ for $1 \le j < \ell$. Since $\sigma_0 \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$ and $\mathrm{i} = X^m$, multiplying further by a power of X^m gives $\sigma_0 = 1$ and preserves these indices and $\theta_g(\sigma)$. Lemma 4.3 also gives $(a_E\sigma)_{p_j} = 0$ for $0 \le j < \ell$.

We first show that $\ell = s + 1$. For $7 \le \nu \le 9$, we have $m - \nu > V$. Since the nonzero complex coefficients of σ have indices in $[0, V]$, (2.5) gives $\sigma_{-\nu} = \mathrm{i}\sigma_{m-\nu} = 0$. The definition of t_0 therefore gives

$$(t_0\sigma)_0 = C\sum_{\nu=7}^{9}(2\sigma_{-\nu} + \sigma_\nu) = C(\sigma_7 + \sigma_8 + \sigma_9).$$

At most one of $\sigma_7, \sigma_8, \sigma_9$ is nonzero, so $\phi_0^{\pm}(t_0, \sigma) \le C$. Together with $(a_E\sigma)_0 = 0$ and $\phi_0^{+}(g, \sigma) \ge C$, linearity in the first argument of ϕ_0^{+} gives $\phi_0^{+}(v, \sigma) \ge 0$.

For $1 \le j < \ell$, let $a_j := H + w_{\kappa_j}|\delta_j|$ be the weight assigned to the position p_j. We have $\Re(\mathrm{i}\sigma_{p_j}) + \Im(\mathrm{i}\sigma_{p_j}) \le 1$, and the κ_j are distinct. Since $\sigma_0 = 1$, the definition of v gives

$$\phi_0^{+}(v, \sigma) = \sum_{j=1}^{\ell-1} a_j \left[\Re(\mathrm{i}\sigma_{p_j}) + \Im(\mathrm{i}\sigma_{p_j})\right] - sH - B \le (\ell - 1)H + W - sH - B.$$

If $\ell \le s$, the upper bound is at most $-H + W - B = -B - 1 < 0$, contradicting $\phi_0^{+}(v, \sigma) \ge 0$. Thus $\ell = s + 1$ and $\kappa_j = j$ for $1 \le j \le s$.

We next show that all nonzero complex coefficients of σ equal 1. By Lemma 4.4, $p_j - p_{j-1} \in \{7, 8, 9\}$ for $1 \le j \le s$, whereas $p_j - p_c \ge 15$ when $0 \le c < j \le s$ and $j - c \ge 2$. The definition of t_0 therefore gives

$$(t_0\sigma)_{p_j} = \begin{cases} C\sigma_{p_1}, & j = 0, \\ 2C\sigma_{p_{j-1}} + C\sigma_{p_{j+1}}, & 1 \le j < s, \\ 2C\sigma_{p_{s-1}}, & j = s. \end{cases}$$

Suppose $\sigma_{p_j} \ne \sigma_{p_{j-1}}$ for some $1 \le j \le s$, and let $\gamma := \sigma_{p_{j-1}}/\sigma_{p_j} = \overline{\sigma_{p_j}}\sigma_{p_{j-1}} \in \{-1, \mathrm{i}, -\mathrm{i}\}$ be the ratio of the preceding coefficient to the current one. One of $\Re\gamma \pm \Im\gamma$ equals -1. By (4.3), the preceding coefficient contributes $-2C$ to $\phi_{p_j}^{\varepsilon}(t_0, \sigma)$ for some $\varepsilon \in \{+, -\}$. The contribution from the following coefficient is at most C (and is 0 when $j = s$). Hence $\phi_{p_j}^{\varepsilon}(t_0, \sigma) \le -2C + C$. Lemma 4.1 bounds $|\phi_{p_j}^{\varepsilon}(v, \sigma)|$ by $\|v\|_1 = C - 1$. Since $(a_E\sigma)_{p_j} = 0$, we get

$$\phi_{p_j}^{\varepsilon}(g, \sigma) \le -2C + C + (C - 1) = -1 < C,$$

contradicting $\theta_g(\sigma) \ge C$. Thus consecutive coefficients agree. Since $\sigma_{p_0} = 1$, all σ_{p_j} equal 1, giving the stated form. □

In the form established in Lemma 4.5, the position of the coefficient 1 in each three-element set determines a Boolean choice. The next lemma shows that $\|f\sigma\|_\infty \le T$ forces these choices to solve the Subset Sum instance. Conversely, every solution yields a vector of ℓ_∞-norm exactly T.

Lemma 4.6. *For g constructed in Section 4.2, we have $\theta_g(\sigma) \le C$ for every $\sigma \in \mathcal{U}_m$. There exists $\sigma \in \mathcal{U}_m$ with $\theta_g(\sigma) = C$ if and only if the equation $\sum_{h=1}^{s} w_h\xi_h = B$ has a solution $\boldsymbol{\xi} \in \{0, 1\}^s$. Moreover, a solution to the* Subset Sum *instance can be recovered in deterministic polynomial time from any $\sigma \in \mathcal{U}_m$ with $\theta_g(\sigma) = C$.*

Proof. Suppose $\sigma \in \mathcal{U}_m$ satisfies $\theta_g(\sigma) \ge C$. By Lemma 4.5, $X^\nu\sigma = 1 + \sum_{h=1}^{s} X^{8h+\delta_h}$ for some $\nu \in \mathbb{Z}$. The proof of Lemma 4.5 gives $\theta_g(X^\nu\sigma) = \theta_g(\sigma)$, so we replace σ by $X^\nu\sigma$. Set $\xi_h := |\delta_h| \in \{0, 1\}$ for $1 \le h \le s$ and $Z := \sum_{h=1}^{s} w_h\xi_h - B$. At 0, we have $(a_E\sigma)_0 = 0$ by Lemma 4.3, and $(t_0\sigma)_0 = C$ by the definition of t_0. Moreover,

$$(v\sigma)_0 = \mathrm{i}\Big[\sum_{h=1}^{s}(H + w_h\xi_h) - (sH + B)\Big] = \mathrm{i}Z. \tag{4.10}$$

Since $\sigma_0 = 1$, we have $\phi_0^{\pm}(v, \sigma) = \pm Z$. Hence $\phi_0^{\pm}(g, \sigma) = C \pm Z$. By the definition of θ_g,

$$C \le \theta_g(\sigma) \le \min\{C + Z, C - Z\} = C - |Z|.$$

Hence $Z = 0$ and $\theta_g(\sigma) = C$, so $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_s)$ solves the Subset Sum instance. In particular, $\theta_g(\sigma) \le C$ for every $\sigma \in \mathcal{U}_m$.

Conversely, let $\boldsymbol{\xi} \in \{0,1\}^s$ satisfy $\sum_{h=1}^{s} w_h \xi_h = B$. Set $p_0 := 0$, $p_h := 8h + \xi_h$ for $1 \le h \le s$, and $\sigma := \sum_{h=0}^{s} X^{p_h} \in \mathcal{U}_m$. Every pairwise cyclic distance between its support indices belongs to E, so $(a_E \sigma)_{p_h} = 0$ for $0 \le h \le s$ by Lemma 4.3. The definition of t_0 gives $(t_0\sigma)_0 = C$ and real coefficients $(t_0\sigma)_{p_h} \ge 2C$ for $1 \le h \le s$, since the preceding coefficient $\sigma_{p_{h-1}} = 1$ contributes $2C$ and any contribution from the following coefficient is nonnegative. Equation (4.10) gives $(v\sigma)_0 = 0$, so $\phi_0^{\pm}(g, \sigma) = C$. At every other p_h, Lemma 4.1 gives $\phi_{p_h}^{\pm}(g, \sigma) \ge 2C - (C-1) = C + 1$. The minimum defining $\theta_g(\sigma)$ is therefore attained at index 0 and equals C. Lemma 4.2 with $M = T + C$ gives $\|f\sigma\|_\infty = T$.

Given any $\sigma \in \mathcal{U}_m$ with $\theta_g(\sigma) = C$, test $X^\nu \sigma$ for $0 \le \nu < 2n$ to find the form in Lemma 4.5. Replace σ by the polynomial found, which still satisfies $\theta_g(\sigma) = C$, and let $0 = p_0 < p_1 < \cdots < p_s$ be the indices of its nonzero complex coefficients. Set $\xi_h := |p_h - 8h|$ for $1 \le h \le s$. The inequalities $\phi_0^{\pm}(g, \sigma) \ge C$ and the coefficient calculation in (4.10) give $\sum_{h=1}^{s} w_h \xi_h = B$. The enumeration and recovery take deterministic polynomial time. □

We now verify the reduction and its running time.

Theorem 4.7. *There exists a deterministic polynomial-time reduction from* Subset Sum *to* $\mathsf{IdealSVP}_\infty$ *that maps each instance to an instance of the form* $(n, (f), T)$*, where* $0 \ne f \in R_n$*. The first minimum of* (f) *is* T *on YES instances and at least* $T + 1$ *on NO instances. Consequently,* $\mathsf{IdealSVP}_\infty$ *is* NP*-complete for principal ideals of* R_n*, where* n *ranges over powers of two.*

Proof. The definition of T gives $T + C > 3\|g\|_1$. The bounds in (4.2) with $M = T + C$ and Lemma 2.4 therefore imply that $f \ne 0$ and that every shortest nonzero vector of (f) has the form $f\sigma$ with $\sigma \in \mathcal{U}_m$. By Lemma 4.6, $\theta_g(\sigma) \le C$ for every $\sigma \in \mathcal{U}_m$. The first minimum of (f) is therefore at least T by Lemma 4.2. On a YES instance, some $\sigma \in \mathcal{U}_m$ satisfies $\theta_g(\sigma) = C$ and hence $\|f\sigma\|_\infty = T$, so the first minimum equals T. On a NO instance, $\theta_g(\sigma) \le C - 1$ for every $\sigma \in \mathcal{U}_m$ by integrality, so the first minimum is at least $T + 1$.

The choice of m gives $n = 2m \le 16(8s + 1)$. Since $C = O(sW + B)$ and $\|a_E\|_1 \le 5^{m/2}$, we have $\|g\|_1 = O(C5^{m/2})$. Thus $T = 3\|g\|_1 + 1 = O(C5^{m/2})$, and $\|f\|_\infty \le T + C + \|g\|_1 = O(C5^{m/2})$. Hence T and each entry of $\mathbf{M}_f$ have $O(s + \log(sW + B)) = O(s + \beta + \log s)$ bits. The output basis $\mathbf{M}_f$ has n^2 entries, so the output has $O(s^2(s + \beta + \log s))$ bits. The explicit formulas therefore give a deterministic polynomial-time construction. Membership in NP follows from Lemma 2.2. □

The proof of Theorem 4.7 also gives the following corollary. Comparing the norm of a shortest vector with T decides the source Subset Sum instance. On a YES instance, the linear algebra in Section 2.3 recovers σ from a shortest vector $y = f\sigma$, and Lemma 4.6 recovers a solution to the Subset Sum instance in polynomial time.

Corollary 4.8. *Search-*$\mathsf{IdealSVP}_\infty$ *is* NP*-hard for principal ideals of* R_n *under polynomial-time Turing reductions, where* n *ranges over powers of two.*

5 Transfer to cyclic rings

In this section, we transfer the reductions in Sections 3 and 4 from $R_n = \mathbb{Z}[X]/(X^n + 1)$ to the cyclic polynomial rings $S_{2n} := \mathbb{Z}[X]/(X^{2n} - 1)$. We extend the scalar construction used for Euclidean CVP by Liu, Feng, and Pan [LFP26a] to polynomial matrices. The construction preserves module rank while doubling the ring degree and the first minimum in the coefficient ℓ_∞-norm.

Each element of S_{2n} has a unique representative $f = \sum_{\ell=0}^{2n-1} [f]_\ell X^\ell$ of degree less than $2n$. We identify it with the coefficient vector $([f]_0, \ldots, [f]_{2n-1})^{\mathsf{T}} \in \mathbb{Z}^{2n}$. Since $X^{2n} = 1$, multiplication by X cyclically permutes these coefficients. An ideal of S_{2n} has *full rank* if its coefficient lattice has rank $2n$.

Let $n \ge 1$ be a power of two and $r \ge 1$. Let $\mathbf{G} = (g_{ab}) \in R_n^{r \times r}$ satisfy $\det \mathbf{G} \ne 0$, and represent its entries by polynomials of degree less than n. Set $F := \max_{1 \le a,b \le r} \|g_{ab}\|_\infty$ and $C := 2F + 1$. Define

$$\widehat{\mathbf{G}} := (1 - X^n)\mathbf{G} + C(1 + X^n)\mathbf{I}_r \in S_{2n}^{r \times r}. \tag{5.1}$$

Over $\mathbb{Q}$, the Chinese remainder theorem gives

$$\mathbb{Q} \otimes_{\mathbb{Z}} S_{2n} \cong \mathbb{Q}[X]/(X^n + 1) \times \mathbb{Q}[X]/(X^n - 1).$$

Reducing the matrix in (5.1) modulo X^n+1 gives $2\mathbf{G}$, while reducing it modulo X^n-1 gives $2C\mathbf{I}_r$.

Theorem 5.1. *The matrix $\widehat{\mathbf{G}}$ defined by (5.1) has the following properties.*

(i) The module $\widehat{\mathbf{G}}S_{2n}^r$ is free of rank r, and its coefficient lattice has rank $2rn$. For $r=1$, it is a principal ideal of S_{2n}.
(ii) The first minima satisfy

$$\lambda_{1,\infty}(\widehat{\mathbf{G}}S_{2n}^r) = 2\lambda_{1,\infty}(\mathbf{G}R_n^r). \tag{5.2}$$

(iii) Every entry of $\widehat{\mathbf{G}}$ has coefficients of absolute value at most $3F+1$.

Proof. For $\mathbf{u}\in S_{2n}^r$, write its canonical representative as $\mathbf{u}=\mathbf{a}+X^n\mathbf{b}$ with $\mathbf{a},\mathbf{b}\in\mathbb{Z}[X]^r$ of degree less than n. Its images modulo X^n+1 and X^n-1 are $\mathbf{a}-\mathbf{b}$ and $\mathbf{a}+\mathbf{b}$, respectively. Let $\mathbf{v}=(v_1,\dots,v_r)\in\mathbb{Z}[X]^r$ be the vector obtained by reducing each coordinate of $\mathbf{G}(\mathbf{a}-\mathbf{b})$ modulo X^n+1 to degree less than n. Expanding (5.1) yields

$$\begin{aligned}\widehat{\mathbf{G}}\mathbf{u} &= (1-X^n)\mathbf{G}(\mathbf{a}-\mathbf{b}) + C(1+X^n)(\mathbf{a}+\mathbf{b})\\ &= (1-X^n)\mathbf{v} + C(1+X^n)(\mathbf{a}+\mathbf{b})\\ &= \big(\mathbf{v}+C(\mathbf{a}+\mathbf{b})\big) + X^n\big(-\mathbf{v}+C(\mathbf{a}+\mathbf{b})\big).\end{aligned} \tag{5.3}$$

The first equality uses $X^{2n}=1$ in S_{2n}. The second uses the definition of $\mathbf{v}$ and $(1-X^n)(X^n+1)=0$.

Applying $\max\{|x+t|,|-x+t|\}=|x|+|t|$ to corresponding coefficients in the two blocks of (5.3) gives

$$\left\|\widehat{\mathbf{G}}\mathbf{u}\right\|_\infty = \max_{1\le j\le r,\ 0\le k<n}\big(|[v_j]_k| + C|[a_j+b_j]_k|\big). \tag{5.4}$$

For (i), suppose $\widehat{\mathbf{G}}\mathbf{u}=\mathbf{0}$. Equation (5.4) gives $\mathbf{a}+\mathbf{b}=\mathbf{0}$ and $\mathbf{v}=\mathbf{0}$. The definition of $\mathbf{v}$ and injectivity of $\mathbf{G}$ give $\mathbf{a}-\mathbf{b}=\mathbf{0}$, so $\mathbf{a}=\mathbf{b}=\mathbf{0}$. Thus $\mathbf{u}=\mathbf{0}$, so the expanded integer matrix of $\widehat{\mathbf{G}}$ is nonsingular, proving (i).

For (ii), set $\lambda := \lambda_{1,\infty}(\mathbf{G}R_n^r)\le F$ and consider any nonzero vector $\widehat{\mathbf{G}}\mathbf{u}$. If $\mathbf{a}+\mathbf{b}\neq\mathbf{0}$, equation (5.4) gives $\left\|\widehat{\mathbf{G}}\mathbf{u}\right\|_\infty \ge C > 2\lambda$. If $\mathbf{b}=-\mathbf{a}$, set $\mathbf{y}:=\mathbf{G}\mathbf{a}\in R_n^r\setminus\{\mathbf{0}\}$ and represent each coordinate of $\mathbf{y}$ by a polynomial of degree less than n. Equation (5.3) gives $\left\|\widehat{\mathbf{G}}\mathbf{u}\right\|_\infty = 2\left\|\mathbf{y}\right\|_\infty \ge 2\lambda$ and

$$\widehat{\mathbf{G}}\mathbf{u} = 2\mathbf{y} - X^n(2\mathbf{y}).$$

Choose $\mathbf{a}\in R_n^r$ with $\left\|\mathbf{G}\mathbf{a}\right\|_\infty=\lambda$ and set $\mathbf{u}:=\mathbf{a}-X^n\mathbf{a}\in S_{2n}^r$ using the canonical representative of $\mathbf{a}$. Equation (5.3) gives $\left\|\widehat{\mathbf{G}}\mathbf{u}\right\|_\infty = 2\lambda$, proving (5.2).

For (iii), expanding $\widehat{\mathbf{G}} = (\mathbf{G}+C\mathbf{I}_r)+X^n(-\mathbf{G}+C\mathbf{I}_r)$ shows that every coefficient has absolute value at most $F+C=3F+1$. □

Corollary 5.2. *For every fixed integer $r\ge 1$, decision-*SVP *in the coefficient ℓ_∞-norm is* NP*-complete for free modules of rank r over $S_{2n}=\mathbb{Z}[X]/(X^{2n}-1)$ with n a power of two. In particular, this holds for the following input classes.*

(i) principal ideals of S_{2n}.
(ii) free modules of rank two over S_{2n}.

Proof. Take the output $(n,(f),T)$ of Theorem 4.7. Set $\mathbf{G}_1:=(f)$ and, for $r\ge 2$, $\mathbf{G}_r:=\operatorname{diag}(f,(T+1)\mathbf{I}_{r-1})$. The added coordinates have norm at least $T+1$ when nonzero, so $\mathbf{G}_rR_n^r$ has first minimum T on YES instances and at least $T+1$ on NO instances. Theorem 5.1 transforms $\mathbf{G}_r$ into a generator matrix $\widehat{\mathbf{G}}_r$ over S_{2n}. Let $\mathcal{M}:=\widehat{\mathbf{G}}_rS_{2n}^r$. We output the instance $(2n,\mathcal{M},2T)$. For $r=1$, we provide an integer basis of the ideal by taking the coefficient vectors of the cyclic shifts of the entry of $\widehat{\mathbf{G}}_1$. By (5.2), the output has first minimum $2T$ on YES instances and at least $2T+2$ on NO instances.

For fixed r, the parameter bounds in Theorems 4.7 and 5.1(iii), together with the explicit formula (5.1), give a deterministic polynomial-time reduction. A nonzero coefficient vector of norm at most the input bound is a certificate of polynomial bit length. Integer linear algebra checks input validity, and Hermite normal form tests lattice membership in polynomial time [Coh93]. These decision problems therefore belong to NP. □

Every nonzero vector in $\widehat{\mathbf{G}} S_{2n}^r$ of norm less than C has the form $2\mathbf{y} - X^n(2\mathbf{y})$ with $\mathbf{0} \neq \mathbf{y} \in \mathbf{G}R_n^r$. Taking its coefficients of degrees $0, \ldots, n-1$ in each coordinate and dividing by 2 recovers $\mathbf{y}$ in polynomial time.

The proof of Corollary 5.2 also gives the following corollary. Comparing the norm of a shortest vector with $2T$ decides the source Subset Sum instance. On a YES instance, taking the first n coefficients of its first coordinate and dividing by 2 gives a shortest vector of (f), from which Section 4.3 recovers a solution in polynomial time.

Corollary 5.3. *Search-*SVP *in the coefficient ℓ_∞-norm is* NP*-hard for principal ideals and free modules of any fixed rank $r \geq 1$ over S_{2n} under polynomial-time Turing reductions, where n ranges over powers of two.*

6 Conclusion

We prove that decision-SVP in the coefficient ℓ_∞-norm is NP-complete for principal ideals and free modules of rank two over the power-of-two cyclotomic rings $R_n = \mathbb{Z}[X]/(X^n + 1)$. Both results hold under deterministic polynomial-time reductions from the Subset Sum problem, with lattice dimension linear in the number of input integers.

We also establish NP-completeness for principal ideals and free modules of every fixed positive rank over the power-of-two cyclic rings $S_{2n} = \mathbb{Z}[X]/(X^{2n} - 1)$ by transferring the reductions from R_n. Over both ring families, the corresponding search problems are NP-hard under polynomial-time Turing reductions.

Use of AI

The reductions and proofs in this paper were found using OpenAI's GPT-6.1 Sol (Ultra). The model initially produced a reduction from NAE-3SAT, which gave a more complicated construction with a larger lattice dimension and much larger constant factors. Working with the model, we switched to Subset Sum and simplified the constructions to obtain smaller constant factors and lattice dimensions linear in the number of input integers. We also used the model to generate the accompanying Lean formalization. We reorganized and polished the manuscript, verified all mathematical proofs and references ourselves, and take full responsibility for the final paper.

References

[Ajt98] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions (extended abstract). In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 10–19. Association for Computing Machinery, 1998.

[BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, pages 575–584. Association for Computing Machinery, 2013.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*, *Graduate Texts in Mathematics* 138. Springer, 1993.

[Din02] I. Dinur. Approximating SVP_∞ to within almost-polynomial factors is NP-hard. *Theoretical Computer Science*, 285(1):55–71, 2002.

[Kar72] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.

[Kho05] S. Khot. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52(5):789–808, 2005.

[LFP26a] J. Liu, Y. Feng, and Y. Pan. CVP is NP-complete for principal cyclotomic ideals. arXiv preprint arXiv:2608.23828v2, 2026.

[LFP26b] J. Liu, Y. Feng, and Y. Pan. SVP is NP-hard for some rank-2 cyclotomic modules. arXiv preprint arXiv:2609.01469v1, 2026.

[LM06] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, Languages and Programming—ICALP 2006, Part II*, *Lecture Notes in Computer Science* 4052, pages 144–155. Springer, 2006.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology—EUROCRYPT 2010*, *Lecture Notes in Computer Science* 6110, pages 1–23. Springer, 2010.

[LS15] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Designs, Codes and Cryptography*, 75(3):565–599, 2015.

[Mar26] D. E. Martin. NP-hardness of ideal lattice problems. arXiv preprint arXiv:2609.15813v1, 2026.

[Mic01] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM Journal on Computing*, 30(6):2008–2035, 2001.

[Nat24] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. Federal Information Processing Standards Publication 203, National Institute of Standards and Technology, 2024.

[Pei08] C. Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *Computational Complexity*, 17(2):300–351, 2008.

[Pei09] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, pages 333–342. Association for Computing Machinery, 2009.

[PR06] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography—TCC 2006*, *Lecture Notes in Computer Science* 3876, pages 145–166. Springer, 2006.

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6):34:1–34:40, 2009.

[vEB81] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical Report MI-UvA-81-04, Mathematisch Instituut, University of Amsterdam, 1981. `https://staff.fnwi.uva.nl/p.vanemdeboas/vectors/mi8104c.html`.

[Wan26a] D. Wan. Euclidean SVP is deterministically NP-hard to approximate within any constant factor. arXiv preprint arXiv:2608.12664v2, 2026.

[Wan26b] D. Wan. Euclidean SVP is NP-hard for cyclic lattices. arXiv preprint arXiv:2609.16711v1, 2026.

[Was97] L. C. Washington. *Introduction to Cyclotomic Fields*, *Graduate Texts in Mathematics* 83. Springer, second edition, 1997.