Quantum Information Processing (2026) 25:113
https://doi.org/10.1007/s11128-026-05143-y

On finding PUBO problems on Diophantine equations

J. M. Hernández Cáceres[1] · I. F. Rúa[1]

Received: 19 September 2025 / Accepted: 12 March 2026
© The Author(s) 2026

Abstract
We apply a standard encoding technique to reformulate Diophantine equations as polynomial unconstrained binary optimization (PUBO) problems and study their solvability using the quantum approximate optimization algorithm (QAOA).

Keywords HOBO (PUBO) problems · Diophantine equations · QAOA

1 Introduction

Diophantine equations are polynomial equations with integer coefficients, involving one or more integer variables. Linear Diophantine equations admit complete solutions via the extended Euclidean algorithm and its generalizations. Additionally, certain quadratic and cubic forms such as Pell's equations or equations defining elliptic curves can be solved algorithmically using continued fractions, descent methods, or the theory of heights.

However, there exists no algorithm that can determine, for every Diophantine equation, whether a solution exists. In fact, it is known as Hilbert's tenth problem:

Given any polynomial equation with any number of unknowns and with integer coefficients: To devise a universal process according to which it can be determined by a finite number of operations whether the equation has integer solutions.

The resolution of Hilbert's Tenth Problem was given by Matiyasevich in January 1970, building on prior work by Davis, Putnam, and Robinson. Together, their results established the undecidability of the general Diophantine problem, now known as the DPRM (Davis–Putnam–Robinson–Matiyasevich) theorem, or Matiyasevich's theorem [1, 2].

This motivates the present research: to study the solvability of a Diophantine equation in a finite domain using quantum approximate optimization algorithm (QAOA). For that, we study a standard encoding technique to reformulate it as a polynomial

✉ J. M. Hernández Cáceres
jmhernandez@uniovi.es

I. F. Rúa
rua@uniovi.es

[1] Department of Mathematics, University of Oviedo, C/ Leopoldo Calvo Sotelo 18, Oviedo, Spain

Published online: 26 March 2026

unconstrained binary optimization (PUBO) problem and then apply QAOA to it. As a proof of concept, we demonstrate this procedure on some Diophantine equations, including both solvable and unsolvable cases. Furthermore, we explore the scalability and complexity of this procedure when applied to a specially chosen system of Diophantine equations whose unsolvability is known to be equivalent to the Riemann hypothesis.

The remainder of the paper is organized as follows. In Sect. 2, we review PUBO problems and discuss how they can be approached using quantum techniques. In Sect. 3, we present a methodology for determining whether a given Diophantine equation is unsolvable over a defined domain using QAOA. In Subsection 3.2, we provide simulation results that illustrate the application of this methodology. Finally, we present our conclusions in Sect. 4.

2 PUBO problems

Optimization problems in which we are asked to minimize a binary polynomial (binary variables) of any degree, with no additional restrictions, are called higher-order binary optimization problems, HOBO for short, or polynomial unconstrained binary optimization problems, PUBO for short. More explicitly, they are problems of the form

$$\begin{aligned} \min \quad & q\left(x_0, \ldots, x_m\right) \\ \text{subject to} \quad & x_j \in \{0, 1\}, \quad j = 0, \ldots, m, \end{aligned}$$

where $q\left(x_0, \ldots, x_m\right)$ is a polynomial on the x_j binary variables of any degree. One approach to solving HOBO problems is through hybrid quantum–classical methods, such as the quantum approximate optimization algorithm (QAOA), which is among the most widely studied quantum algorithms for combinatorial optimization on gate-based quantum computers. It was introduced by Farhi et al. [3] as a discretized version of adiabatic quantum computing (introduced by Farhi, Goldstone, Gutmann, and Sipser in a widely influential paper [4]).

Unlike quantum annealing, QAOA operates in the gate-based circuit model and allows for binary polynomials of arbitrary degree. Such polynomials can be directly transformed into a Hamiltonian by substituting each binary variable x_i with $\frac{1-Z_i}{2}$, where Z_i is the Pauli Z operator acting on qubit i. The resulting Hamiltonian is then expressed as a sum of tensor products of Z matrices. For further details on this transformation, see [5, Section 5.1.5].

3 Standard method

In this section, we present a methodology, structured through three algorithms, for determining whether a given Diophantine equation is solvable over a finite domain by using quantum approximate optimization algorithm (QAOA). This approach involves encoding the Diophantine equation as a polynomial unconstrained binary optimization (PUBO) problem and analyzing the minimum value of the resulting cost function. If

Table 1 Computational cost of Algorithm 1

Step	Description	Cost
1	Expand P	$O(n^d)$
2	Compute P^2	$O(k^2)$
3	Substitute integer variables of P^2	$O(k^2 M^d)$
4	Expand and simplify binary powers	$O(k^2 M^d)$

the minimum value is zero, a solution exists within the given domain; otherwise, the equation is unsolvable over that domain.

Algorithm 1 (Construction of the PUBO problem)
Input: *A Diophantine equation $P(x_1, \ldots, x_n) = 0$, with n unknowns $x's$, of degree d, with k number of terms, with no exponential variables, and a positive integer M.*
Construction of the corresponding PUBO problem:

1. *If P is not expanded then expand it. Otherwise move to step 2.*
2. *Square the polynomial P (P^2).*
3. *Substitute each integer variable by a binary representation of length M. Using for instance, two's complement encoding (see below).*
4. *Expand the polynomial and reduce powers of each binary variables, i.e., $b_i^j = b_i$ for all $j \in \mathbb{N}$ and $j \geq 2$.*

Output:

$$\begin{aligned} &min \quad q\,(b_1, \ldots, b_m) \\ &subject\ to \quad b_j \in \{0, 1\}, \quad j = 0, \ldots, m \quad with\ m = M \cdot n. \end{aligned}$$

In cases where the Diophantine equation P contains exponential variables, these expressions are evaluated directly by substituting with integer values, and Algorithm 1 is then applied to the resulting polynomial. In Step 2 of Algorithm 1, we use the two's complement representation to encode integer variables. This encoding allows all integers in the range from -2^{M-1} to $2^{M-1} - 1$ to be represented using M-bit binary strings. Positive integers are encoded in standard binary form, whereas a negative integer x is represented by $2^M - x$. This binary representation maintains a finite and symmetric search space, which is essential for formulating the problem as a bounded binary optimization task.

The finiteness of the domain also permits the application of Algorithm 2, which leverages quantum optimization techniques such as QAOA to explore the binary search space efficiently.

Table 1 outlines the computational cost associated with executing Algorithm 1.

Algorithm 2 (In search of the solution)
Input: *A PUBO problem, and two positive integers* p, l.
Procedure: Step 1: Hamiltonian Construction
Substitute each binary variable b_i *in the PUBO by* $(1 - Z_i)/2$ *where* Z_i *is the Pauli Z operator acting on qubit* i*, to construct the cost Hamiltonian* H.
Step 2: QAOA Execution *Apply the QAOA algorithm with depth* $p = 1$ *(or greater), using Hamiltonian* H *and the initial state* $|+\rangle^{\otimes n}$. *Optimize over variational parameters* $(\boldsymbol{\gamma}, \boldsymbol{\beta})$ *to minimize the expectation value* $\langle H \rangle$.
Step 3: Bitstring Evaluation *Measure the QAOA circuit* s *times. For each resulting bitstring* $x \in \{0, 1\}^n$*, compute its energy using the Hamiltonian* H *and select the* l *bitstrings with the lowest cost.*
Output: *If the cost among top-*l *bitstrings is* 0 *then Output: Yes, Otherwise Output No.*

Algorithm 3 (Decision)
Input: *A Diophantine equation* $P(x_1, \ldots, x_n) = 0$*, with* n *unknowns* $x's$*, of degree* d*, with* k *number of terms, two positive integers* M, N.
Output: *Yes, Not found for integers less or equal than* $M + N$.
Procedure:

```
found ← false
for i ≤ N do
    Apply Algorithm 1 with parameter M + i
    Apply Algorithm 2
    if Output of Algorithm 2 is Yes then
        found ← true
        break
    else
        continue                    ▷ go to next iteration of the for loop
    end if
end for
if found then
    return Yes
else
    return Not found for integers on [−2^{M−1}, 2^{M−1} − 1]^n.
end if
```

It is worth mentioning that the output of Algorithm 2, in which Step 2 is QAOA, provides only an approximation to the solutions of the optimization problem. This approximation is given by the approximation ratio, which theoretically improves as the depth parameter p increases [6].

Consequently, the proposed hybrid methodology, consisting of Algorithm 1 through Algorithm 3, yields an approximate solvability test for a Diophantine equation within a bounded domain, with performance directly to the quality of that ratio.

Proposition 1 *Let $P(x_1, \ldots, x_n) = 0$ be a Diophantine equation with n unknowns, total degree d, and k terms. Let $M \in \mathbb{Z}^+$. Let $Q(b_1, \ldots, b_m)$ be the PUBO (polynomial unconstrained binary optimization) function obtained by applying Algorithm 1 to P, where $m = M \cdot n$. Then:*

1. *If P has a solution, then* $\min Q = 0$.
2. *If* $\min Q > 0$, *then P has no solution in* $[-2^{M-1}, 2^{M-1} - 1]^n$.

Furthermore, the computational cost of constructing the corresponding PUBO problem is

$$O\left(n^d + k^2 + k^2\, M^d\right).$$

And the number of qubits required to implement Algorithm 2 is at least $O(M \cdot n)$.

Proof If P has a solution, then by construction, $\min Q = 0$. Now, let us suppose that $Q(\vec{b}) > 0$ for all $\vec{b} \in \{0, 1\}^m$. Since,

$$Q(\vec{b}) = \left(P(x_1(\vec{b}), \ldots, x_n(\vec{b}))\right) \cdot \left(P(x_1(\vec{b}), \ldots, x_n(\vec{b}))\right) > 0$$

It implies that $\left(P(x_1(\vec{b}), \ldots, x_n(\vec{b}))\right) \neq 0$, where $x_i(\vec{b})$ represent the binary expression of the integer x_i. Therefore, there exists no $\vec{x} \in [-2^{M-1}, 2^{M-1} - 1]^n$ such that $P(\vec{x}) = 0$. Hence, P has no solution in the given domain. □

Remark 1 This result holds over the finite domain 2^{M-1} to $2^{M-1} - 1$. If P has a solution outside this range, then Q may not detect it unless M is sufficiently large. To make a claim about all integer solutions, i.e, $M \to \infty$, is computationally infeasible since proving unsolvability in general requires infinitely many operations.

Remark 2 When dealing with Diophantine equations whose solutions are constrained to the positive integers, we enforce this constraint within the QAOA framework by adding a penalization term to the cost Hamiltonian. Specifically, to constrain a variable x to take only positive values, we introduce the term $\lambda \frac{1 - Z_{\mathrm{MSB}_x}}{2}$, where Z_{MSB_x} is the Pauli Z operator acting on the most significant bit (MSB) in the binary encoding of x. The penalty strength λ should be chosen sufficiently large relative to the typical energy scale of the original cost Hamiltonian to effectively suppress negative solutions while preserving the true minima.

3.1 Examples

As a proof of concept, we apply the proposed hybrid methodology, namely Algorithm 1 followed by Algorithm 2 and Algorithm 3, to some well-known Diophantine equations, such as Catalan's equation, Hardy–Ramanujan number, Erdös–Strauss, Pells, and two more in which one has not solution and the other is yet to be proved if its solvable or not. We provide a table (see Table 2) in which give the number of qubits requried, the depth of QAOA apply, and the minimum cost. In all cases, without loss of generality, we choose $l = 5$, which specifies the number of bitstrings in the output of Algorithm 2.

Table 2 Simulation results for selected diophantine equations using QAOA

Equation	M	# Qubits	QAOA Depth (p)	Minimum cost
Catalan's Equation: $x^2 - y^3 = 1$	4	8	1	0
Hardy–Ramanujan Number: $w^3 + x^3 = y^3 + z^3$	4	16	1	0
Pells: $x^2 - 7y^2 = 1$	8	4	1	0
Erdös–Strauss ($n = 4$): $4xyz = 4(yz + xz + xy)$	4	12	1	0 with $\lambda = 10$
Erdös–Strauss ($n = 10^{18}$): $4xyz = 10^{18}(yz + xz + xy)$	4	12	1	> 0 with $\lambda = 10^{21}$
$x^2 + y^2 = 3$	4	8	1	> 0
	7	14	4	> 0
	8	16	6	> 0
$x^4 + y^4 = z^2 - 1$	4	12	1	> 0
	5	15	1	> 0
	6	18	1	> 0
	8	24	1	> 0

As desired, the minimum cost for the **Catalan's equation** is found to be **0** when using $M = 4$, indicating the existence of a solution. This aligns with the known solution: $x = 3,\ a = 2,\ y = 2,\ b = 3$. Similarly, for the **Hardy–Ramanujan number equation**, it is well known that the smallest non-trivial solution in positive integers is given by $12^3 + 1^3 = 9^3 + 10^3 = 1729$. Algorithm 3 correctly identifies this solution by also yielding a minimum cost of **0** for $M = 4$.

For the **Erdös–Strauss equation** with $n = 4$, using $M = 4$ and $\lambda = 100$, the algorithm indicates the existence of a solution. This is consistent with extensive computational results verifying the existence of solutions for all $n \leq 10^{17}$. However, for $n = 10^{18}$ with $M = 4$ and $\lambda = 10^{21}$, the minimum cost is found to be greater than **0**, suggesting that no solution is found within this bounded domain.

In contrast, the Diophantine equation $x^2 + y^2 = 3$ has no integer solutions, since the square of any integer modulo 4 is either 0 or 1, and thus, the sum of two such squares cannot be congruent to 3 modulo 4. Accordingly, in all tested configurations $M = 4,\ 7,\ 8$ with QAOA depths $p = 1,\ 4,\ 6$, respectively, the minimum cost remained strictly **greater than 0**, as expected. Finally, we consider the equation $x^4 + y^4 = z^2 - 1$, for which it is known that no integer solutions exist with $0 < y < 7.9 \cdot 10^7$. We tested this equation for $M = 4,\ 5,\ 6,\ 8$ and QAOA depth $p = 1$; in all cases, the minimum cost remained strictly **greater than 0**, confirming unsolvability within the explored domain. All simulation results referenced here can be found in Table 2 and in. [1]

To illustrate the scalability and complexity of the methodology, we further consider a specially chosen system of Diophantine equations whose unsolvability is known to be equivalent to the Riemann hypothesis.

[1] https://github.com/JMiguel01/On-finding-a-HOBO-problem-on-a-Diophantine-Equation.

For that, let us recall that for $s \in \mathbb{C}_1 = \{z \in \mathbb{C} \mid \mathrm{Re} z > 1\}$ the Riemann zeta function $\zeta(s)$ is defined by the absolutely convergent Dirichlet series $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. It can be analytically continued to the whole complex plane $\mathbb{C}$ as a meromophic function with the only simple pole at $s = 1$, and the residue at this pole is equal to 1. The non-real zeros of the Riemann zeta function are known to lie in the critical strip $\mathcal{L} = \{s \in \mathbb{C} \mid 0 < \mathrm{Re} s < 1\}$ and the set of its real zeros is known to coincide with the set of the negative even integers, i.e., $\zeta(-2n) = 0$ for $n \in \mathbb{N}$; those are the so-called trivial zeros of the Riemann zeta function. Those definitions and assertions can be found, for instance, in Davenport's book [7], or [8, Section 12.8].

The (unproved) Riemann hypothesis asserts that all the non-real zeros of the Riemann zeta function lie on the line $\mathrm{Re} s = 1/2$. And it has many equivalent formulations [9, 10]. In particular, in the context of the present research, Matiyasevich's theorem states that every recursively enumerable set is Diophantine. Namely, given a recursively enumerable subset S of $\mathbb{N}$, one can actually construct a polynomial $P_S(t; x)$ in $\mathbb{Z}[t; x]; x = (x_1, \ldots, x_n)$ for some $n \in \mathbb{N}$, such that

$$S = \left\{a \in \mathbb{N} \mid \exists b \in \mathbb{Z}^n \, P_S(a; b) = 0\right\}.$$

Hence, one can construct a system of Diophantine equations whose unsolvability is equivalent to the Riemann hypothesis. In fact, following [11, Section 6.4] together with procedures described in [12], and by the well-known Schoenfeld's theorem [13], Hernández Cáceres [14] gave such an equation on several pages, which requires around 2286 integer variables; certain inaccuracies contained in it [14] were corrected in [15]. However, using a restatement of a system of conditions equivalent to the Riemann hypothesis given by Matiyasevich in [16], Moroz and Norkin in [17] gave a system of Diophantine equations whose unsolvability is equivalent to the Riemann hypothesis, in which the number of variables were significantly reduced (around 166). Here, we use that system to explicitly construct a Diophantine equation equivalent to it, and then apply Algorithm 1.

3.2 Construction of the system of diophantine equations

Let us first consider the system of conditions in which [16] shows an equivalence with the Riemann hypothesis. Following their notation, the system is:

$$\begin{aligned}
&2^l \le n < 2^{l+1}, \quad 2^m \le 2^q < 2^{m+1}, \quad s = \frac{B^{n+1}\left(B^{(n+1)n} - n - 1\right) + n}{(B^{n+1} - 1)^2}, \\
&t = \frac{(2^m - 1)(B^{n^2} - 1)}{B^n - 1}, \quad \binom{t}{r} \equiv 1 \pmod 2, u = \mathrm{rem}(rs, B^{n^2 - n}), \\
&rs - u \equiv \frac{B^{n^2-n}(B^n - 1)}{B - 1} q \pmod{B^{n^2}}, \quad p = \mathrm{rem}(r, B^n + 1), \\
&mp < nq - 15l^2 q\sqrt{n}
\end{aligned} \tag{1}$$

where $B = 2^{l+m+1}$, and $\mathrm{rem}(a, b)$ stands for the remainder of dividing a by b. So, if the Riemann hypothesis is true, then the system (1) has no solution in positive integers $l, m, n, p, q, r, s, t, u$. An if the Riemann hypothesis is false, then the system (1) has infinitely many such solutions. With that, [17] construct the following system of Diophantine equations

$$\begin{aligned}
n &= w_1 + z_1 - 1 = 2w_1 - z_2, \quad 2q = w_2 + z_3 - 1 = 2w_2 - z_4\\
s(2w_1w_2w_3 - 1)^2 &= \left(2w_1w_2w_3(w_4w_3^2 - n - 1) + n\right),\\
t(w_3 - 1) &= (w_2 - 1)(w_4w_3 - 1), \quad t = r + z_5 - 1, \quad w_6 = 2w_7(h_1 - 1) + u,\\
w_6 &= w_7 + z_6 = 2w_7 - z_7, \quad rs = (h_2 - 1)w_4 + h_3 - 1\\
w_4 &= h_3 + z_8 - 1, \quad r = (h_4 - 1)(w_3 + 1) + p, \quad w_3 = p + z_9 - 1\\
w_3z_{10} &= q + (h_2 - 1)(2w_1w_2 - 1), \quad nq = mp + z_{11},\\
(nq - mp)^2 &= (225l^4q^2n + z_{12}), \quad 0 = E(w_1, 2, l; \mathbf{z^{(2)}}), \quad 0 = E(w_2, 2, m; \mathbf{z^{(3)}})\\
0 &= E(w_3, 2, n(l + m + 1); \mathbf{z^{(4)}}),\\
0 &= E(w_4, 2, (n^2 - n)(l + m + 1); \mathbf{z^{(4)}}), \quad 0 = E(w_5, 2, t; \mathbf{z^{(6)}})\\
0 &= E(w_6, w_5 + 1, t; \mathbf{z^{(7)}}), \quad 0 = E(w_7, 2, rt; \mathbf{z^{(8)}}),
\end{aligned} \tag{2}$$

where $w_1 = 2^l$, $w_2 = 2^m$, $w_3 = B^n$, $w_4 = B^{n^2-n}$, $w_5 = 2^t$, $w_6 = (2^t + 1)^t$, $w_7 = 2^{rt}$, $\mathbf{z} = (z_1, \ldots, z_{12}) \in \mathbb{N}^{12}$, $\mathbf{z^{(i)}} = (z_{13+20(i-1)}, \ldots, z_{32+20(i-1)}) \in \mathbb{N}^{12}$ for $1 \leq i \leq 8$, and

$$\begin{aligned}
E(\alpha, \beta, \gamma; x) &= \left(x_1^2 - (x_2^2 - 1)x_3^2 - 1\right)^2 + \left(x_4^2 - (x_2^2 - 1)x_5^2 - 1\right)^2\\
&+ \left(x_6^2 - (x_7^2 - 1)x_8^2 - 1)\right)^2 + \left(x_5 - x_9x_3^2\right)^2 + (x_7 - (1 + 4x_{10}x_3))^2\\
&+ (x_1 + x_{12}x_4 - x_6)^2 + (\gamma + 4(x_{13} - 1)x_3 - x_8)^2 + (\gamma + x_{14} - 1 - x_3)^2\\
&+ \left(x_1 - x_3(x_2 - \beta) - \alpha)^2 - (x_{15} - 1)^2(2x_2\beta - \beta^2 - 1)^2\right)^2\\
&+ \left(\alpha + x_{16} - \left(2x_2\beta - \beta^2 - 1\right)\right)^2 + (\gamma + x_{19} - x_{17})^2\\
&+ \left(x_2^2 - (x_{17}^2 - 1)(x_{17} - 1)^2x_{20}^2 - 1\right)^2.
\end{aligned}$$

The unsolvability of that system of Eq. (2) in positive integers is equivalent to the Riemann hypothesis; moreover, if the Riemann hypothesis does not hold, then this system of equations has infinitely many solutions in $\mathbb{N}$.

Now, note that the unsolvability of the system of equations of (2) is equivalent to the unsolvability of the Diophantine equation

$$P(w, X, h, Z) = P_1(w, X, h, z) + P_2(w, l, m, n, r, t, Z), \tag{3}$$

where

$$
\begin{aligned}
P_1(w, X, h, z) &= (w_1 + z_1 - n - 1)^2 + (2w_1 - z_2 - n)^2 + (w_2 + z_3 - 1 - 2q)^2 \\
&+ (2w_2 - z_4 - 2q)^2 + \left(s(2w_1w_2w_3 - 1)^2 - \Big(2w_1w_2w_3(w_4w_3^2 - n - 1) + n\Big)\right)^2 \\
&+ (t(w_3 - 1) - (w_2 - 1)(w_4w_3 - 1))^2 + (r + z_5 - 1 - t)^2 \\
&+ (2w_7(h_1 - 1) + u - w_6)^2 + (w_7 + z_6 - w_6)^2 + (2w_7 - z_7 - w_6)^2 \\
&+ ((h_2 - 1)w_4 + h_3 - 1 - rs)^2 + (h_3 + z_8 - 1 - w_4)^2 \\
&+ ((h_4 - 1)(w_3 + 1) + p - r)^2 + (p + z_9 - 1 - w_3)^2 \\
&+ (q + (h_2 - 1)(2w_1w_2 - 1) - w_3z_{10})^2 + (mp + z_{11} - nq)^2 \\
&+ (225l^4q^2n + z_{12} - (nq - mp)^2)^2,
\end{aligned}
$$

$$
\begin{aligned}
P_2(w, l, m, n, r, t, Z) &= (E(w_1, 2, l; \mathbf{z^{(2)}}))^2 + (E(w_2, 2, m; \mathbf{z^{(3)}}))^2 \\
&+ (E(w_3, 2, n(l + m + 1); \mathbf{z^{(4)}}))^2 + (E(w_4, 2, (n^2 - n)(l + m + 1); \mathbf{z^{(4)}}))^2 \\
&+ (E(w_5, 2, t; \mathbf{z^{(6)}}))^2 + (E(w_6, w_5 + 1, t; \mathbf{z^{(7)}}))^2 + (E(w_7, 2, rt; \mathbf{z^{(8)}}))^2,
\end{aligned}
$$

with $w = (w_1 \ldots, w_7)$, $\mathbf{X} = (l, m, n, p, q, r, s, t, u)$, $\mathbf{h} = (h_1, h_2, h_3, h_4)$, and $Z = \left(\mathbf{z^{(2)}}, \ldots, \mathbf{z^{(8)}}\right)$.

3.3 On finding a HOBO problem

Having established the Diophantine equation, we now proceed to apply Algorithm 1.

1. Now, let us expand P to see its degree and the number of monomials. To do so, we implemented a code in Python[2] which finds that P has 21 monomials of degree 24 and 134,629 additional monomials of lower degree (see Table 3). The fully expanded expression for P is also available in the repository.
2. Since $\left(\sum_{i=1}^{n} x_i\right)^2 = \sum_{i=1}^{n} x_i^2 + 2\left(\sum_{1 \le i, j \le n} x_i x_j\right)$ for $n \ge 2, n \in \mathbb{Z}$ and x_i variables, the maximum number of terms of $\left(\sum_{i=1}^{n} a_i\right)^2$, is at most $n + \binom{n}{2} = \frac{n(n+1)}{2}$. Based on this, we estimate the number of terms in the expansion of P^2. In fact, P^2 is of degree 48 and contains at most $\sum_{i=1}^{36} U_i = 695951380661052222$ terms,where U_i is given in Table 4.
3. Now, for each integer variable, consider the binary representation of length M, with $M \in \mathbb{Z}^+$. Thus, to express P^2 in terms of binary variables, we would require less than $\sum_{i=1}^{36} U_i M$ binary variables, where M_i is given in Table 4.

Now, let us construct our HOBO problem.

[2] https://github.com/JMiguel01/On-finding-a-HOBO-problem-on-a-Diophantine-Equation.

Table 3 Degree and number of terms in the expansion of P

Polynomial	Highest degree	No of terms
$P_1(w, X, h, \mathbf{z})$	$M_1 = 50625l^8n^2q^4$	164
$(E(w_1, 2, l; \mathbf{z^{(2)}}))^2$	$M_2 = z_{49}^{16}z_{52}^{8}$	12,020
$(E(w_2, 2, m; \mathbf{z^{(3)}}))^2$	$M_3 = z_{69}^{16}z_{72}^{8}$	12,020
$(E(w_3, 2, n(l+m+1); \mathbf{z^{(4)}}))^2$	$M_4 = z_{89}^{16}z_{92}^{8}$	15,682
$(E(w_4, 2, (n^2-n)(l+m+1); \mathbf{z^{(4)}}))^2$	$M_5 = z_{109}^{16}z_{112}^{8}$	21,527
$(E(w_5, 2, t; \mathbf{z^{(6)}}))^2$	$M_6 = z_{129}^{16}z_{132}^{8}$	12,020
$(E(w_6, w_5+1, t; \mathbf{z^{(7)}}))^2$	$M_7 = 256w_6^8z_{134}^{8}z_{147}^{8}$	49,205
$(E(w_7, 2, rt; \mathbf{z^{(8)}}))^2$	$M_8 = z_{169}^{16}z_{172}^{8}$	12,020

Proposition 2 *Consider the following PUBO problem:*

$$\begin{aligned} &min \left(P\left(\sum_{j=0}^{M} w_{1_j} 2^j, \ldots, \sum_{j=0}^{M} z_{172_j} 2^j \right) \right)^2 \\ &subject\ to \quad w_{1_i}, \ldots, z_{172_i} \in \{0, 1\}\ for\ all\ i\,. \end{aligned}$$

So, if the Eq. (3) *has infinitely many solutions in* $\mathbb{N}$*, then the minimum value would be zero; moreover, if the minimum value is not zero, then the Eq.* (3) *has no solution in the positive integers.*

Proof If the system of Eq. (2) has infinitely many solutions in $\mathbb{N}$, let (w, X, h, Z) be a solution, then $P_1(w, X, h, z) = (0)^2+(0)^2+(0)^2+\cdots+(0)^2$ and $E(w_1, 2, l; \mathbf{z^{(2)}}) = 0$, $E(w_2, 2, m; \mathbf{z^{(3)}}) = 0, \ldots, E(w_6, w_5{+}1, t; \mathbf{z^{(7)}}) = 0$, so $P_2(w, l, m, r, t, Z) = 0$; hence, $P(w, X, h, Z) = 0$ and $P(w, X, h, Z)^2 = 0$. Now, note that

$$\left(P\left(\sum_{j=0}^{M} w_{1_j} 2^j, \ldots, \sum_{j=0}^{M} z_{172_j} 2^j \right) \right)^2 \geq 0$$

for all $w_{1_i}, \ldots, z_{172_i} \in \{0, 1\}$ and for all i, so this makes the problem a minimization of a nonnegative function; hence, the minimum value over all assignments is at most 0.

Now, if the minimum value is not zero, this means that for all $w_{1_i}, \ldots, z_{172_i} \in \{0, 1\}$ and for all i, $0 \neq P(w, X, h, Z)^2 = P(w, X, h, Z) \cdot P(w, X, h, Z)$ so, $P(w, X, h, Z) \neq 0$ meaning that (w, X, h, Z) is not a solution to the system. □

4 Conclusions

In this work, we presented a methodology for determining whether a given Diophantine equation is unsolvable over a defined domain using the quantum approximate

Table 4 Degree and upper bound on the number of terms in the expansion of P.

Polynomial	Highest degree	Upper Bound of terms
$P_1(w, X, h, \mathbf{z})^2$	$M_1 = 2562890625l^{16}n^4q^8$	$U_1 = 12432$
$E_2 = (E(w_1, 2, l; \mathbf{z^{(2)}}))^4$	$M_2 = z_{49}^{32}z_{52}^{16}$	$U_2 = 72252621$
$E_3 = (E(w_2, 2, m; \mathbf{z^{(3)}}))^4$	$M_3 = z_{69}^{32}z_{72}^{16}$	$U_3 = 72252621$
$E_4 = (E(w_3, 2, n(l+m+1); \mathbf{z^{(4)}}))^4$	$M_4 = z_{89}^{32}z_{92}^{16}$	$U_4 = 122995523$
$E_5 = (E(w_4, 2, (n^2-n)(l+m+1); \mathbf{z^{(4)}}))^4$	$M_5 = z_{109}^{32}z_{112}^{16}$	$U_5 = 231684378$
$E_6 = (E(w_5, 2, t; \mathbf{z^{(6)}}))^4$	$M_6 = z_{129}^{32}z_{132}^{16}$	$U_6 = 72252621$
$E_7 = (E(w_6, w_5+1, t; \mathbf{z^{(7)}}))^4$	$M_7 = 65536w_6^{16}z_{134}^{16}z_{147}^{16}$	$U_7 = 1212906543$
$E_8 = (E(w_7, 2, rt; \mathbf{z^{(8)}}))^4$	$M_8 = z_{169}^{32}z_{172}^{16}$	$U_8 = 72252621$
$P_1 \cdot E_2$	$M_1 \cdot M_2$	$U_9 = 8979611592$
$P_1 \cdot E_3$	$M_1 \cdot M_3$	$U_{10} = 8979611592$
$P_1 \cdot E_4$	$M_1 \cdot M_4$	$U_{11} = 15276482808$
$P_1 \cdot E_5$	$M_1 \cdot M_5$	$U_{12} = 28773611784$
$P_1 \cdot E_6$	$M_1 \cdot M_6$	$U_{13} = 8979611592$
$P_1 \cdot E_7$	$M_1 \cdot M_7$	$U_{14} = 75486502176$
$P_1 \cdot E_8$	$M_1 \cdot M_8$	$U_{15} = 8979611592$
$E_2 \cdot E_3$	$M_2 \cdot M_3$	$U_{16} = 5220463841765641$
$E_2 \cdot E_4$	$M_2 \cdot M_4$	$U_{17} = 8896453217612983$
$E_2 \cdot E_5$	$M_2 \cdot M_5$	$U_{18} = 16742252188280188$
$E_2 \cdot E_6$	$M_2 \cdot M_6$	$U_{19} = 5220463841765641$
$E_2 \cdot E_7$	$M_2 \cdot M_7$	$U_{20} = 87578738444099930$
$E_2 \cdot E_8$	$M_2 \cdot M_8$	$U_{21} = 5220463841765641$
$E_3 \cdot E_4$	$M_3 \cdot M_4$	$U_{22} = 8896453217612983$
$E_3 \cdot E_5$	$M_3 \cdot M_5$	$U_{23} = 16742252188280188$
$E_3 \cdot E_6$	$M_3 \cdot M_6$	$U_{24} = 5220463841765641$
$E_3 \cdot E_7$	$M_3 \cdot M_7$	$U_{25} = 87578738444099930$
$E_3 \cdot E_8$	$M_3 \cdot M_8$	$U_{26} = 5220463841765641$
$E_4 \cdot E_5$	$M_4 \cdot M_5$	$U_{27} = 22566580109465492$
$E_4 \cdot E_6$	$M_4 \cdot M_6$	$U_{28} = 4439679646347561$
$E_4 \cdot E_7$	$M_4 \cdot M_7$	$U_{29} = 74287913699071644$
$E_4 \cdot E_8$	$M_4 \cdot M_8$	$U_{30} = 4439679646347561$
$E_5 \cdot E_6$	$M_5 \cdot M_6$	$U_{31} = 8355194190499280$
$E_5 \cdot E_7$	$M_5 \cdot M_7$	$U_{32} = 140826147302939360$
$E_5 \cdot E_8$	$M_5 \cdot M_8$	$U_{33} = 8355194190499280$
$E_6 \cdot E_7$	$M_6 \cdot M_7$	$U_{34} = 87460583795319150$
$E_6 \cdot E_8$	$M_6 \cdot M_8$	$U_{35} = 5222460064776841$
$E_7 \cdot E_8$	$M_7 \cdot M_8$	$U_{36} = 87460583795319150$

optimization algorithm (QAOA). We provided simulation results to demonstrate the practical applicability of the method, showing that the proposed approach can be employed as a research tool for studying the solvability of Diophantine equations whose status remains unknown.

Furthermore, we explored a connection between a PUBO problem and the Riemann hypothesis through a specially chosen system of equations. To that end, we estimated the cost in terms of the number of binary variables required to construct this combinatorial problem. We then analyzed the degree and number of monomials in the resulting polynomial, as these characteristics directly influence the complexity of the PUBO instance.

It is important to note that any attempt to solve the associated PUBO problem of its corresponding Diophantine equation inherently encounters the fundamental limits of computability. In future work, our aim is to explore alternative quantum techniques, such as Grover adaptive search (GAS) [18], which has been proposed as a way to improve quantum oracles for PUBO problems. Additionally, we plan to investigate whether the exponential growth in the number of integer variables in Diophantine encoding can be mitigated through more efficient representations or problem transformations.

Acknowledgements This work was partially supported by Grant PID 2021-123461 NB-C22 from the Spanish Ministry of Economic Affairs and Digital Transformation; and by Grant MRR-MAETD-24-INCIBE-01 from the Spanish National Cybersecurity Institute (INCIBE). Finally, the authors, members of the Universidad de Oviedo research team GACYC, also acknowledge support from the Spanish Network of Mathematics in the Information Society (MatSI).

Author Contributions J.M Hernández Cáceres and I.F. Rúa wrote the main manuscript text. All authors reviewed the manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data Availability No datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Matiyasevich, Y.V.: Enumerable sets are Diophantine, Doklady AN SSSR, 191:2 (1970), 279–282 translated in: Soviet Math. Doklady, 11 (1970), 354-358

2. Matiyasevich, Y.V.: Diophantine representation of enumerable predicates, Izvestiya AN SSSR. Seriya Matematicheskaya, 35:1 (1971), 3-30. Translated in: Mathematics of the USSR. Izvestiya, 15(1) (1971), 1-28. Adiabatic quantum computation is equivalent to standard quantum computation, Proceedings of the 45th Annual ACM Symposium on Theory of Computing, 2004, pp. 42–51
3. Farhi, E., Goldstone, J., Gutmann, S.: A quantum approximate optimization algorithm (2014)
4. Farhi, E., Goldstone, J., Gutmann, S., Sipser, M.: Quantum computation by adiabatic evolution. Chem. Phys. Lett. **219**(5–6), 343–348 (1994)
5. Combarro, E. F., González-Castillo, S.: A Practical Guide to Quantum Machine Learning and Quantum Optimization: Hands-on Approach to Modern Quantum Algorithms, Packt Publishing (2023)
6. Blekos, K., Brand, D., Ceschini, A., Chou, C.-H., Li, R.-H., Pandya, K., Summer, A.: A review on quantum approximate optimization algorithm and its variants. Phys. Rep. **1068**, 1–66 (2024). https://doi.org/10.1016/j.physrep.2024.03.002
7. Davenport, H.: Multiplicative Number Theory, Springer, Berlin (2000)
8. Apostol, T.M.: Introduction to Analytic Number Theory, Springer, Berlin
9. Broughan, K.: Equivalents of the Riemann Hypothesis. Arithmetic Equivalents, vol. 1. Cambridge University Press, Cambridge (2017)
10. Broughan, K.: Equivalents of the Riemann Hypothesis. Analytic Equivalents, vol. 2. Cambridge University Press, Cambridge (2017). https://doi.org/10.1017/9781108178266
11. Davis, M., Matiyasevich, Y.V., Robinson, J.: Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution. In: Proceedings of Symposia in Pure Maths, vol. 28, pp. 323–378 (1976)
12. Davis, M.: *Hilbert's Tenth Problem is Unsolvable*, The American Mathematical Monthly, Vol 80, No 3, pp. 233–269 (1973). Available at http://www.jstor.org/stable/2318447
13. Schoenfield, L.: Sharper bounds for the Chebyshev function $\psi(x)$ and $\vartheta(x)$. Math. Comput. **30**, 337–360 (1976)
14. Hernández Cáceres, J.M.: The Riemann Hypothesis and Diophantine Equations, Master's Thesis Mathematics, Mathematical Institute, University of Bonn (2018)
15. Moroz, B. Z.: The Riemann hypothesis and the Diophantine equations, Preprint no. 2018-03 (St. Petersburg Math. Soc., St. Petersburg, 2018) [in Russian]
16. Matiyasevich, Y.V.: The Riemann hypothesis as the parity of special binomial coefficients. Dokl. Math. **106**(Suppl 2), S256–S261 (2022). https://doi.org/10.1134/S1064562422700247
17. Moroz, B.Z., Norkin, A.A.: On a theorem of Matiyasevich. Math. Notes **108**(3), 344–355 (2020)
18. Gilliam, A., Woerner, S., Gonciulea, C.: Grover adaptive search for constrained polynomial binary optimization. Quantum **5**, 428 (2021)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.