Quantum Information Processing (2020) 19:34
https://doi.org/10.1007/s11128-019-2528-7

Discrete quantum computation and Lagrange's four-square theorem

J. Lacalle[1] · **L. N. Gatti**[1]

Received: 14 February 2019 / Accepted: 26 November 2019

Abstract
We study a problem that arises naturally in the discrete quantum computation model introduced in Gatti and Lacalle (Quantum Inf Process 17:192, 2018). Given an orthonormal system of discrete quantum states of level k ($k \in \mathbb{N}$), can this system be extended to an orthonormal basis of discrete quantum states of the same level? This question turns out to be a difficult problem in number theory with very deep implications. In this article, we focus on the simplest version of the problem, 2-qubit systems with integers (instead of Gaussian integers) as coordinates, but with normalization factor $\sqrt{p}$ ($p \in \mathbb{N}^*$), instead of $\sqrt{2^k}$, being p a prime number. With these simplifications, we prove the following orthogonal version of Lagrange's four-square theorem: Given a prime number p and $v_1, \ldots, v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, then there exists a vector $v = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and

$$\|v\|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = p.$$

This means that, in $\mathbb{Z}^4$, any system of orthogonal vectors of norm p can be completed to a basis. Besides, we conjecture that the result holds for every integer norm $p \geq 1$ and for every space $\mathbb{Z}^n$ where $n \equiv 0 \bmod 4$, and that the initial question has a positive answer.

Keywords Discrete quantum states · p-orthonormal basis extension theorem · Systems of p-orthonormal vectors · Orthogonal lattices

✉ J. Lacalle
jlacalle@etsisi.upm.es

L. N. Gatti
ln.gatti@alumnos.upm.es

[1] Dep. de Matemática Aplicada a las Tecnologías de la Información y las Comunicaciones, ETSI de Sistemas Informáticos, Universidad Politécnica de Madrid, C/ Alan Turing s/n, 28031 Madrid, Spain

Published online: 05 December 2019

1 Introduction

The model of discrete quantum computation introduced in [5] is focused on the discrete quantum states (from now on discrete states). Its objective is to define a set of discrete states that verify the following properties: It describes real states in quantum physics, preserves the main characteristics of quantum states (superposition and entanglement), allows to approximate general quantum states and, above all, contains simple quantum states. Of all the possible sets of discrete states, there is one that, fulfilling the first three properties, is the most outstanding in terms of simplicity of the states. It is the set of Gaussian coordinate states, which includes all the quantum states whose coordinates in the computational basis, except for a normalization factor $\sqrt{2^{-k}}$, belong to the ring of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

For this, the authors introduce a set of quantum gates that verify the following properties: It contains quantum gates that transform discrete states into discrete states and it generates all discrete states. The model includes two elementary quantum gates that verify the above properties: H and G. The Hadamard gate H allows superposition, while the other one, G, is a 3-qubit gate. Two of them are control qubits, while the third is the target. If the control qubits are in state $|1\rangle$, then the gate V is applied to the third qubit

$$V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

These quantum gates allow the construction of all Gaussian coordinate states ([5], Theorem 3.8) and allow to identify these states with the discrete states on which the model of discrete quantum computation is based.

Then an n-qubit Ψ is a discrete state if and only if there is a natural number k such that

$$\Psi = \frac{1}{\sqrt{2^k}} \sum_{j=0}^{2^n-1} (a_j + b_j i)|j\rangle \qquad \text{with } a_j, b_j \in \mathbb{Z} \text{ for all } 0 \leq j < 2^n. \tag{1}$$

Therefore, the discrete state Ψ is associated with the Diophantine equation

$$a_0^2 + b_0^2 + \cdots + a_{2^n-1}^2 + b_{2^n-1}^2 = 2^k \quad \text{with } a_j, b_j \in \mathbb{Z} \text{ for all } 0 \leq j < 2^n. \tag{2}$$

The index k in the normalization factor provides an interesting point of view about the discrete states [5]. Namely, the states can be classified in different levels of discretization, depending on k. Given a discrete state, the authors say that it belongs to the level k if k is in smaller natural number for which Eq. (2) is fulfilled. These levels depict the degree of precision or approximation of discrete states in relation to continuous states.

The results that we present in this article are closely linked to the properties and to the conjecture about the generation of discrete quantum gates (from now on discrete

gates) exposed in [5]. The authors define the discrete gates as those quantum gates that leave the set of discrete states invariant. They prove that a quantum gate is a discrete gate if and only if in its matrix representation, with respect to the computational basis, its columns are discrete states of levels of the same parity ([5], Theorem 4.2). Obviously the rows of the discrete gates verify the same property. They also prove a surprising property that initially was not part of the objectives of the discrete quantum computing model: Every 2-qubit discrete gate can be decomposed into a product of H and G gates ([5], Theorem 4.16). They also conjecture that every n-qubit discrete gate, with $n \geq 3$, can also be generated within the model ([5], Abstract and Introduction). In our work, we reformulate (expand) this conjecture in the following way.

Conjecture 1 *Given a set of n-qubit discrete states of levels of the same parity and orthogonal two to two, it is possible to build all of them simultaneously (applying a given circuit to different states of the computational basis), using the conforming gates H and G.*

Observe that the conjecture also makes sense for 2-qubits, since in [5] it has only been proved for sets of 4 discrete states. And note that the conjecture is also interesting in the non-discrete case, since it asks about the possibility of simultaneously constructing up to 2^n quantum states simultaneously. In this case, the conjecture is obviously true. Simply complete the orthonormal basis, for example using the Gram–Schmidt method, and decompose the resulting unitary matrix into product of basic quantum gates. Therefore, it makes sense to ask whether it is in the case of discrete quantum computation.

Before continuing, let us relax the discrete state level definition given in [5] to any value of k for which the discrete state verifies Eq. (2). We will call these values *widespread levels*. Note that if k is a widespread level of a discrete state then $k+2$ is also. To prove this, it is enough to divide the normalization factor by 2 and multiply by 2 the Gaussian coordinates of the representation of the discrete state with widespread level k [in Eq. (1)]. Then, a discrete state has widespread level k if and only if it is of the form $k_0 + 2j$, where k_0 is the level of the discrete state and j a natural number. This property allows to write all discrete states (with levels of the same parity) at the same widespread level.

Let us see that, somehow, building a set of orthogonal discrete states is equivalent to completing the set to an orthonormal basis. For this reason, we will focus on this article in the following problem.

Problem 1 *Given a natural number k and $\Psi_1, \ldots, \Psi_j$ n-qubit discrete states with widespread level k, $1 \leq j < 2^n$, such that $\langle \Psi_i | \Psi_m \rangle = 0$ for all $1 \leq i < m \leq j$, then is there an n-qubit discrete state with widespread level k, Ψ, such that $\langle \Psi_i | \Psi \rangle = 0$ for all $1 \leq i \leq j$?*

Based on the following result, every 2-qubit discrete gate can be decomposed into a product of H and G gates ([5], Theorem 4.16); it is easy to establish the following equivalence: For 2-qubits, Conjecture 1 is true if and only if Problem 1 has an affirmative answer.

We have established the relationship between Problem 1, whose study is the objective of this article, and the simultaneous construction of discrete states of levels of the

same parity and orthogonal two to two (Conjecture 1). The resolution of this problem would allow us to build bases with special characteristics, and it would help us to demonstrate the conjecture that any n-qubit discrete gate, with $n \geq 3$, can be generated with the elementary quantum gates of the discrete quantum computation model [5].

Undoubtedly the problem that is studied in this article has important connections with the model of discrete quantum computing and, consequently, with quantum computing. As we are going to see, it also has implications for scientific fields such as number theory, geometry of numbers and theory of lattices. In addition, we believe that discrete models will have a great influence on quantum information theory and, indirectly, on quantum physics itself. Quantum computing, to be viable, needs some kind of discretization and that quantum physics, somehow, allows some self-correcting system beyond the quantum error-correcting codes. We will analyze these considerations in the conclusions.

Now, let us analyze the connection between discrete quantum computing and Lagrange's four-square theorem. The fact that establishes this connection is that the discrete states have to satisfy Eq. (2). Lagrange's four-square theorem [8] says that every natural number is a sum of four squared integer numbers and, consequently, guarantees that there exist discrete states for any level $k \geq 0$ and for any number of qubits $n \geq 1$.

As we have already commented, the discrete quantum computation model would have better properties if all orthonormal systems of discrete states could always be extended to an orthonormal basis, i.e., if Problem 1 has an affirmative answer.

Problem 1 is an orthogonal version of Lagrange's four-square theorem, i.e., the discrete state Ψ must verify the Diophantine equation (2) and the following orthogonality conditions:

$$\langle \Psi_i | \Psi \rangle = 0 \quad \text{for all} \quad 1 \leq i \leq j.$$

Note that given a value of k, if Eq. 2 has a solution for a 1-qubit, then it has a solution for every number of qubits $n \geq 2$. Nevertheless, this generalization is not necessarily true for Problem 1, because of orthogonality conditions. Therefore, the problem has its own entity for any number of qubits n.

Problem 1 turns out to be a difficult question in number theory and has deep implications. For this reason, we begin with the following simplification that most resembles Lagrange's four-square problem: $n = 2$, integers as coordinates instead of Gaussian integers and normalization factor $\sqrt{p}$, being p a prime number, instead of $\sqrt{2^k}$.

Problem 2 *Given a prime number p and $v_1, \ldots, v_k \in \mathbb{Z}^4$, $1 \leq k \leq 3$, such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, then is there a vector $v = (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and $\|v\|^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 = p$?*

The outline of the article is as follows: In Sect. 2, we prove the main result. In Sect. 3, we expose several generalizations and conjectures related to the proposed problems. In Sect. 4, we include some conclusions. Finally we include references and "Appendices A and B," respectively. In "Appendix A," we put Problem 2 in context, discussing the main results related to Lagrange's four-square problem. And in "Appendix B," we

include the demonstration of the most complicated case of the main result given in Sect. 2.

2 Orthogonal version of Lagrange's four-square theorem

First of all, let us introduce some basic concepts. Given a natural number $1 \leq k \leq 4$ and a set of vectors $v_1, \ldots, v_k \in \mathbb{Z}^4$ such that $\|v_i\|^2 = p$ for all $1 \leq i \leq k$ and $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, we will say that $S = \{ v_1, \ldots, v_k \}$ is a *p-orthonormal system* and, if $k = 4$, that S is a *p-orthonormal basis*.

Given a *p-orthonormal system* S, we will call *support of* S, $\mathrm{supp}(S)$, to $\{ i \mid \exists j$ such that the i-coordinate of $v_j \neq 0 \}$ and we will say that $|\mathrm{supp}(S)|$ is the *support size of* S.

In this context, the problem we are dealing with (Problem 2) is stated as follows: Given a prime number p and a p-orthonormal system $S = \{ v_1, \ldots, v_k \}$, $1 \leq k \leq 3$, prove that there exists $v \in \mathbb{Z}^4$ such that $\langle v_i | v \rangle = 0$ for all $1 \leq i \leq k$ and $\|v\|^2 = p$.

To prove the result, we consider four cases. Three of them are solved with basic linear algebra techniques. However, the fourth case is much more difficult and requires the use of lattices and some number theory results. The details of this case are included in "Appendix B."

Case 1: one-vector p-orthonormal systems.

If the p-orthonormal system S has a single vector $v_1 = (x_1, x_2, x_3, x_4)$, the solution (valid for all $p \geq 1$) is trivial: The required vector is, for example, $v = (x_2, -x_1, x_4, -x_3)$.

Case 2: two-vector p-orthonormal systems with support size 2.

If the p-orthonormal system S has two vectors with $|\mathrm{supp}(S)| = 2$, the solution (valid for all $p \geq 1$) is as well trivial. Suppose, without loss of generality, that $\mathrm{supp}(S) = \{1, 2\}$, $v_1 = (x_1, x_2, 0, 0)$ and $v_2 = (y_1, y_2, 0, 0)$. Then, the required vector is, for example, $v = (0, 0, x_1, x_2)$.

Case 3: three-vector p-orthonormal systems.

If the p-orthonormal system S has three vectors, their exterior product allows us to obtain the required vector (valid for all $p \geq 1$).

We will use identities among polynomials in many variables whose demonstration only requires proving that the polynomial expansion of the difference of both members of the equalities equals 0. We will call this type of proof *polynomial checking*.

Given the coordinates of the three vectors of S, $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ and $v_3 = (z_1, z_2, z_3, z_4)$, we consider the exterior product $t = (t_1, t_2, t_3, t_4)$ where

$$t_1 = -\begin{vmatrix} x_2 & x_3 & x_4 \\ y_2 & y_3 & y_4 \\ z_2 & z_3 & z_4 \end{vmatrix}, \quad t_2 = \begin{vmatrix} x_1 & x_3 & x_4 \\ y_1 & y_3 & y_4 \\ z_1 & z_3 & z_4 \end{vmatrix},$$

$$t_3 = -\begin{vmatrix} x_1 & x_2 & x_4 \\ y_1 & y_2 & y_4 \\ z_1 & z_2 & z_4 \end{vmatrix} \text{ and } t_4 = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}.$$

It can be proved, by polynomial checking, that $\langle v_i | t \rangle = 0$ for all $1 \leq i \leq 3$.

In order to calculate $\|t\|^2$, let us prove that $t_i^2 = p^2(p - x_i^2 - y_i^2 - z_i^2)$ for all $1 \leq i \leq 4$. We do it for t_4 since, by symmetry, the demonstration for the rest of coordinates of t is analogous.

Considering the vectors $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ and $z = (z_1, z_2, z_3)$, we can prove, again by polynomial checking, that

$$\begin{aligned} t_4^2 = \|x\|^2 \|y\|^2 \|z\|^2 + 2\langle x|y\rangle\langle x|z\rangle\langle y|z\rangle \\ -\|x\|^2\langle y|z\rangle^2 - \|y\|^2\langle x|z\rangle^2 - \|z\|^2\langle x|y\rangle^2. \end{aligned} \tag{3}$$

Now we can prove that

$$\begin{aligned} p^2\left(p - x_4^2 - y_4^2 - z_4^2\right) = \|x\|^2 \|y\|^2 \|z\|^2 + 2\langle x|y\rangle\langle x|z\rangle\langle y|z\rangle \\ -\|x\|^2\langle y|z\rangle^2 - \|y\|^2\langle x|z\rangle^2 - \|z\|^2\langle x|y\rangle^2, \end{aligned} \tag{4}$$

entering on the right side of the previous equality the values

$$\begin{aligned} \|x\|^2 &= p - x_4^2, & \langle x|y\rangle &= -x_4 y_4, \\ \|y\|^2 &= p - y_4^2, & \langle x|z\rangle &= -x_4 z_4, \\ \|z\|^2 &= p - z_4^2, & \langle y|z\rangle &= -y_4 z_4 \end{aligned}$$

and applying, once again, polynomial checking.

Joining Eqs. 3 and 4, it is concluded that $t_4^2 = p^2(p - x_4^2 - y_4^2 - z_4^2)$.

Finally, the vector $v = t/p$ has the required properties: $\langle v_i|v\rangle = 0$ for all $1 \leq i \leq 3$ and $\|v\|^2 = p$.

Case 4: two-vector p-orthonormal system with support size > 2.

Given a prime number p and a p-orthonormal system $S = \{ v_1, v_2 \}$ with $|\mathrm{supp}(S)| > 2$, there exists $v \in \mathbb{Z}^4$ such that it verifies $\langle v_1|v\rangle = \langle v_2|v\rangle = 0$ and $\|v\|^2 = p$ (see Theorem 3).

Details of the demonstration are included in "Appendix B."

The following theorem is a consequence of the four cases considered previously.

Theorem 1 *Given a prime number p and a p-orthonormal system in $\mathbb{Z}^4$, S, then S can be extended to a p-orthonormal basis.*

3 Generalizations

We have proved that every p-orthonormal system of vectors in $\mathbb{Z}^4$ can be extended to a p-orthonormal basis if p is a prime number. Besides, we have verified the result for every $1 \leq p \leq 10{,}000$. In this section, all verifications for given values of p and n have been made by exhaustive checking of all p-orthonormal systems in $\mathbb{Z}^n$, using a specific C program on a personal computer. From the previous results, we conjecture that the following result holds.

Conjecture 2 *Given an integer number $p \geq 1$ and a p-orthonormal system in $\mathbb{Z}^4$, S, then S can be extended to a p-orthonormal basis.*

The most natural generalization of the problem is to consider it in any dimension $n \geq 1$, i.e., to study the problem in $\mathbb{Z}^n$.

Problem 3 *Given an integer number $p \geq 1$ and a p-orthonormal system in $\mathbb{Z}^n$, S, can S be extended to a p-orthonormal basis?*

An analogous construction to that given in Sect. 2, Case 1 shows the result for $n = 2$. Note that if p cannot be written as a sum of two squares [6] (the prime decomposition of p contains a prime congruent to $3 \bmod 4$ raised to an odd power), there are no p-orthonormal systems in $\mathbb{Z}^2$. The case of dimension 4 has already been studied, and in the case $n = 8$, we have checked the result for $1 \leq p \leq 36$.

To analyze the problem in other dimensions, we try to find counterexamples that help us to understand in which cases the problem has a positive answer. If p is not a square and there exists a p-orthonormal basis in $\mathbb{Z}^n$, then there are counterexamples for p in dimension $n + 1$. Indeed, let $\{v_1 \ldots, v_n\}$ be a p-orthonormal basis in dimension n. Then $\{w_1 \ldots, w_n\}$ is a p-orthonormal system in dimension $n + 1$ that cannot be extended to a p-orthonormal basis, being:

$$w_j = (v_{j,1}, \ldots, v_{j,n}, 0) \quad \text{where} \quad v_j = (v_{j,1}, \ldots, v_{j,n}) \qquad 1 \leq j \leq n.$$

This construction allows us to find counterexamples for any dimension $n \not\equiv 0 \bmod 4$, $n \neq 1$ and $n \neq 2$. Given an integer $p \geq 1$, we consider the p-orthonormal basis $S_1 = \{v_1, v_2, v_3, v_4\}$ in $\mathbb{Z}^4$ and the matrix A,

$$\begin{array}{l} v_1 = (x_1, x_2, x_3, x_4) \\ v_2 = (-x_2, x_1, -x_4, x_3) \\ v_3 = (-x_3, x_4, x_1, -x_2) \\ v_4 = (x_4, x_3, -x_2, -x_1) \end{array} \quad \text{and} \quad A = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ -x_2 & x_1 & -x_4 & x_3 \\ -x_3 & x_4 & x_1 & -x_2 \\ x_4 & x_3 & -x_2 & -x_1 \end{pmatrix},$$

where $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. If p can be written as a sum of two squares, $p = y_1^2 + y_2^2$, we define the p-orthonormal basis $S_2 = \{u_1, u_2\}$ in $\mathbb{Z}^2$ and the matrix B,

$$\begin{array}{l} u_1 = (y_1, y_2) \\ v_2 = (-y_2, y_1) \end{array} \qquad \text{and} \qquad B = \begin{pmatrix} y_1 & y_2 \\ -y_2 & y_1 \end{pmatrix}.$$

Then, the rows of the following matrices C_1, C_2 and C_3 define non-extensible p-orthonormal systems, for dimensions n such that $n \bmod 4$ is 1, 2 or 3, respectively:

(i) C_1 if p is not a square, $n \equiv 1 \bmod 4$ and $n \neq 1$.
(ii) C_2 if p cannot be written as a sum of two squares, $n \equiv 2 \bmod 4$ and $n \neq 2$.
(iii) C_3 if p is not a square and can be written as a sum of two squares and $n \equiv 3 \bmod 4$.

$$C_1 = \begin{pmatrix} A & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & A & 0 \end{pmatrix} \quad C_2 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \end{pmatrix} \quad C_3 = \begin{pmatrix} A & \cdots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & A & 0 & 0 \\ 0 & \cdots & 0 & B & 0 \end{pmatrix}.$$

The experimental verifications and the previous counterexamples make us think that the generalization of Conjecture 2 should be the following.

Conjecture 3 *Given $n \equiv 0 \, mod \, 4$ ($n \geq 1$) and $p \geq 1$ and a p-orthonormal system in $\mathbb{Z}^n$, S, then S can be extended to a p-orthonormal basis.*

But, what happens if p is a square? We have verified the result for $n = 3, 5$ and $1^2 \leq p \leq 100^2$, $n = 6$ and $1^2 \leq p \leq 33^2$, $n = 7$ and $1^2 \leq p \leq 13^2$ and $n = 9$ and $1^2 \leq p \leq 2^2$. Nevertheless, we have found that Problem 3 has a negative answer if $n = 9$, $p = 9$ and $S = \{(1, \ldots, 1)\}$. This counterexample can be generalized as follows: If $n = \bar{n}^2$ and $p = n\bar{p}^2$ are odd integers, then the set $S = \{v_1 = (\bar{p}, \ldots, \bar{p})\}$ cannot be extended to a p-orthonormal basis in $\mathbb{Z}^n$. Indeed, S cannot be extended with a vector v because, on the one hand, the number of odd components of v must be odd because $\|v\|^2 = p$ is odd and, on the other hand, the number of odd components of v must be even because $\langle v_1 | v \rangle = 0$ is even. Hence, if p is a square, our conjecture is as follows.

Conjecture 4 *Given numbers $n \geq 1$ and $p \geq 1$, so that either n is even or p is even or $n \nmid p$, and a p^2-orthonormal system in $\mathbb{Z}^n$, S, then S can be extended to a p^2-orthonormal basis.*

3.1 Structural properties of the problem

Given the integer number k and the vectors $u = (x_1, \ldots, x_n)$ and $v = (y_1, \ldots, y_n)$ belonging to $\mathbb{Z}^n$, we denote the *parity of* k by $P(k) \equiv k \bmod 2$, the *parity of* u by $P(u) \equiv (x_1 + \cdots + x_n) \bmod 2$ and the *parity of* u *and* v by $P(u, v) \equiv \langle u | v \rangle \bmod 2$. Note that $P(u) = P(\|u\|^2)$.

These definitions allow us to consider the conditions of p-orthonormality in terms of parities (module 2), proving the following result.

Proposition 1 *Given a p-orthonormal system in $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$, then it holds that $P(p) = P(v_i)$, $1 \leq i \leq k$, and $P(v_i, v_j) = 0$, $1 \leq i < j \leq k$.*

3.2 Orthogonal extensions

Given a set of vectors belonging to $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$, such that $\langle v_i | v_j \rangle = 0$ for all $1 \leq i < j \leq k$, we will say that S is an *orthogonal system* and, if $k = n$, that S is an *orthogonal basis*.

The relaxation of the condition from p-orthonormality to orthogonality allows to extend any orthogonal system. Indeed, Lemma 1 ("Appendix B") does not depend on the normalization of the vectors and can be applied in $\mathbb{Z}^n$, proving the following proposition.

Proposition 2 *Given an orthogonal system in $\mathbb{Z}^n$, S, then S can be extended to an orthogonal basis.*

Given an orthogonal set in $\mathbb{Z}^n$, $S = \{v_1, \ldots, v_k\}$ ($1 \leq k \leq n$), we denote the *norm of* S by $N(S) = \max\{\|v_i\|^2 \mid 1 \leq i \leq k\}$. So, an interesting problem, in view of Proposition 2, is the following:

Problem 4 *Given an orthogonal system in $\mathbb{Z}^n$, S, determine the orthogonal basis with the smallest norm that extends S.*

3.3 Conjecture about discrete states

Finally, we also believe that the answer to Problem 1 is positive. This fact is gathered in the following conjecture.

Conjecture 5 *Given a natural number k and $\Psi_1, \ldots, \Psi_j$ n-qubit discrete states of with widespread level k, $1 \leq j < 2^n$, such that $\langle \Psi_i | \Psi_m \rangle = 0$ for all $1 \leq i < m \leq j$, then there exists an n-qubit discrete state with widespread level k, Ψ, such that $\langle \Psi_i | \Psi \rangle = 0$ for all $1 \leq i \leq j$.*

4 Conclusions

As we have established in "Introduction," the orthogonal version of Lagrange's four-square theorem presented in this article is closely related to the discrete quantum computation model. The results obtained in the analysis of the proposed problem as well as in the generalizations included in Sect. 3 establish key properties of this model. The complexity of the proof presented in "Appendix B" clearly shows the difficulty of the studied problem and its connection to number theory, geometry of numbers and theory of lattices.

In "Introduction," we also comment that, in our opinion, the discrete quantum computation model, and indirectly the results of the present article, will have great influence on quantum information theory and on quantum physics. Researchers in quantum computing have learned that error control is a hugely complex problem, have mostly abandoned the project of building a quantum computer and have gone to work in quantum simulation.

We believe that with the current quantum physics, quantum computing is not scalable without technological cost overruns. The unitary evolution of quantum systems prevents the design of self-correcting systems based on attraction basins. These systems, which include digital electronics, automatically transform any state of the basin of attraction into the state without error that this represents. Obviously the current quantum physics does not allow to do this. And quantum error-correcting codes do not verify any of the two key hypotheses with which classic error-correcting codes work: All small errors are corrected and correction circuits do not introduce new errors. Decoherence introduces non-local errors that, although they are small if we consider them in short time intervals, the quantum error-correcting codes are not able to correct.

From the point of view of physics, a universal quantum computer is a system that can evolve from the $|0 \ldots 0\rangle$ state of zero entropy to any state (final n-qubit) following any path (algorithm) and keeping the entropy (error) close to zero. Raised like this, the second principle of thermodynamics puts serious doubts about the viability of the construction of such a system, more if we also take into account the impossibility of implementing an effective self-correcting structure.

All these difficulties could be overcome if quantum physics, in some way, could be discretized. We believe that current quantum physics predicts an unlimited capacity of superposition and, consequently, of entanglement and parallelism and that this fact is unrealistic. A second quantization, presumably of quantum states, would allow a physics with less capacity of superposition, entanglement and parallelism, but easier to control. We believe that in this context models of discrete quantum computing will be important.

Appendix A: Main results related to Lagrange's four-square problem

Long before Lagrange proved his theorem, Diophantus had asked whether every positive integer could be represented as the sum of four perfect squares greater than or equal to zero. This question later became known as Bachet's conjecture, after the 1621 translation of Diophantus by Bachet. In parallel, Fermat proposed the problem of representing every positive integer as a sum of at most n n-gonal numbers. Lagrange [8] proved the square case of the Fermat polygonal number theorem in 1770, also solving Bachet's conjecture. Gauss [4] proved the triangular case in 1796 and the full polygonal number theorem was not solved until it was finally proved by Cauchy in 1813. Later, in 1834, Jacobi discovered a simple formula for the number of representations of an integer as the sum of four integer squares.

The same year in which Lagrange proved his theorem, Waring asked whether each natural number k has an associated positive integer s such that every natural number is the sum of at most s natural numbers to the power of k. For example, every natural number is the sum of at most 4 squares, 9 cubes or 19 fourth powers. The affirmative answer to the Waring's problem, known as the Hilbert–Waring theorem, was provided by Hilbert in 1909.

A natural generalization of Lagrange's problem is the following: Given natural numbers a, b, c and d, can we solve $n = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ for all positive integers n in integers x_1, x_2, x_3 and x_4? Lagrange's four-square theorem answered in the positive the case $a = b = c = d = 1$ and the general solution was given by Ramanujan [10]. He proved that if we assume that $a \leq b \leq c \leq d$ then there are exactly 54 possible choices for a, b, c and d such that the problem is solvable in integers x_1, x_2, x_3 and x_4 for all $n \in \mathbb{N}$. Ye [15] establishes formulas for the number of representations of integers by the quadratic forms $x_1^2 + \cdots + x_k^2 + m(x_{k+1}^2 + \cdots + x_{2k}^2)$ for $m = 2, 4$, and Eum et al. [3] study the representation number of a nonnegative integer by the quaternary quadratic form $x_1^2 + 2x_2^2 + x_3^2 + x_4^2 + x_1x_3 + x_1x_4 + x_2x_4$. Sun [13] and Ju et al. [7] have studied a generalization of the problems of Lagrange and Remanujan, in which x_1, x_2, x_3 and x_4 are replaced by generalized octagonal numbers.

Another generalization, due to Mordel [9], tries to represent positive definite integral binary quadratic forms instead of positive integers. He proved that the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ represents all positive definite integral binary quadratic forms.

Sun et al. [12,14] has proposed some refinements of Lagrange's theorem such as, for example, the following: $n \in \mathbb{N}$ can be written as $x_1^2 + x_2^2 + x_3^2 + x_4^2$ with

$x_1, x_2, x_3, x_4 \in \mathbb{Z}$ such that $x_1 + x_2 + x_3$ (or $x_1 + 2x_2$, or $x_1 + x_2 + 2x_2$) is a square (or a cube).

Appendix B: Case 4—two-vector *p*-orthonormal system with support size > 2

Notations and basic properties

We consider $\mathbb{Z}^4$ as a part of the vector space $\mathbb{R}^4$ provided with the inner product $\langle v|w\rangle = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$, where $v = (x_1, x_2, x_3, x_4)$ and $w = (y_1, y_2, y_3, y_4)$ are vectors of $\mathbb{R}^4$, and with the canonical basis $\{e_1, \ldots, e_4\}$.

Given a set of linearly independent vectors $v_1, \ldots, v_k \in \mathbb{R}^4$, they generate the *lattice* $\Lambda = \{ b_1v_1 + \cdots + b_kv_k \mid b_1, \ldots, b_k \in \mathbb{Z} \}$ [1] and constitute a *basis of* Λ, B. So the *dimension of* Λ will be k. From now on, we will only consider bases whose vectors belong to $\mathbb{Z}^4$, i.e., Λ will always be an *integral lattice*.

Given a point $v \in \Lambda$, described by its coordinates in B, $v = (b_i)_B$, the number $N(v) = \|v\|^2 = \langle v|v\rangle$ is called the *norm of* v and can be calculated by the expression $N(v) = b^t Gb$, where G is the *Gram matrix* of the vectors of B. The determinant of G, $\det(G)$, is an invariant of Λ whose square root is denoted by $\det(\Lambda)$. So $\det(\Lambda) = \sqrt{\det(G)}$, and geometrically, it is interpreted as the volume of the fundamental parallelepiped of Λ. The matrix G is symmetric and positive definite and is associated with a quadratic form that collects the main properties of Λ.

Let us consider the *coordinate matrix* V, formed by the vectors of the basis B of Λ placed by rows. If V is a square matrix, we can compute the determinant of Λ from V, $\det(\Lambda) = |\det(V)|$, and it holds that $\det^2(V) = \det(G)$.

However, we are not interested in Λ, but rather in its *orthogonal lattice*

$$\Lambda^\perp = \{ v \in \mathbb{Z}^4 \mid \langle v_i|v\rangle = 0 \text{ for all } 1 \le i \le k \}.$$

The resolution method of systems of linear Diophantine equations [2] computes a basis of $\Lambda^\perp$ with $4 - k$ vectors. Then the dimension of $\Lambda^\perp$ will be $k^\perp = 4 - k$. In order to do this we have to solve the linear system $VX = 0$, computing the *Smith normal form* [11] of V and its *invariant factors* $\alpha_1, \ldots, \alpha_k$:

$$LVR = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_k \end{pmatrix} = N \quad \text{such that} \quad \begin{array}{l} L \in GL_k(\mathbb{Z}) \\ R \in GL_4(\mathbb{Z}) \\ 0 < \alpha_1, \ldots, \alpha_k \\ \alpha_1|\alpha_2, \ \ldots \ \alpha_{k-1}|\alpha_k. \end{array}$$

Lemma 1 *Given a number $p \ge 1$ and a p-orthonormal system $S = \{ v_1, \ldots, v_k \}$, $1 \le k \le 3$, with associated lattice Λ, then the last $4 - k$ columns of the matrix R, in the Smith normal form of V, constitute a basis of $\Lambda^\perp$.*

Proof It holds that $VX = 0 \Leftrightarrow LVRR^{-1}X = L0 = 0$, and considering $Y = R^{-1}X$, we have that $VX = 0 \Leftrightarrow NY = 0 \Leftrightarrow y_1 = \cdots = y_k = 0$. So, the basis

that generates the solutions of $VX = 0$ is $B^{\perp} = \{ R\, e_{k+1}, \ldots, R\, e_4 \}$, i.e., the set with the last $4 - k$ columns of R. □

We will use again the polynomial checking introduced in Sect. 2 Case 3, specifically in Propositions 3 and 4 and in Lemma 3.

Proposition 3 *Given a prime number p and a p-orthonormal system $S = \{ v_1, v_2 \}$, $v_1 = (x_1, \ldots, x_4)$ and $v_2 = (y_1, \ldots, y_4)$, with $|supp(S)| > 2$, then $gcd(x_1, \ldots, x_4) = gcd(y_1, \ldots, y_4) = 1$ and the invariant factors of V also verify $\alpha_1 = \alpha_2 = 1$.*

Proof Suppose, by contradiction, that $\gcd(x_1, \ldots, x_4) = g > 1$. Then $N(v_1) = g^2(x_1'^2 + \cdots + x_4'^2) = p$, where $x_i' = \dfrac{x_i}{g}$ for all $1 \leq i \leq 4$, and this fact contradicts the primality of p. So, we have that $\gcd(x_1, \ldots, x_4) = 1$, and in the same way, we conclude that $\gcd(y_1, \ldots, y_4) = 1$. Applying these results, together with the property of the first invariant factor, we get $\alpha_1 = 1$.

In order to obtain the value of α_2, we will use the following identity, that can be proved by polynomial checking:

$$N(v_1)N(v_2) - \langle v_1 | v_2 \rangle^2 = \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}^2 + \begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}^2 + \cdots + \begin{vmatrix} x_3 & x_4 \\ y_3 & y_4 \end{vmatrix}^2.$$

By hypothesis, $N(v_1)N(v_2) - \langle v_1 | v_2 \rangle^2 = p^2$. Suppose, again by contradiction, that $g = \gcd(m_{12}, \ldots, m_{34}) > 1$, where

$$m_{ij} = \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} \qquad \text{and} \qquad m_{ij}' = \frac{m_{ij}}{g}.$$

Then $p^2 = g^2(m_{12}'^2 + \cdots + m_{34}'^2)$ and there are, at least, two minors different from 0 because $|\text{supp}(S)| > 2$. These facts contradict the primality of p. So, we have that $\gcd(m_{12}, \ldots, m_{34}) = 1$, and since this value matches the second invariant factor, we get $\alpha_2 = 1$. □

Finally, we introduce the fundamental result of the branch of number theory called the geometry of numbers, proved by Minkowski in 1889.

Theorem 2 ([1]) *Let K be a convex set in $\mathbb{R}^n$ which is symmetric with respect to the origin. If the volume of K is greater than 2^n times the volume of the fundamental domain (parallelepiped) of a lattice Λ, then K contains a nonzero lattice point.*

Two-vector *p*-orthonormal system with support size > 2

First of all, let us get a basis of $\Lambda^{\perp}$, $B^{\perp}$, by computing a Smith quasi-normal form in which $L \in GL_k(\mathbb{Q})$. Note that in this case Lemma 1 also holds. Let V be the coordinate matrix of the p-orthonormal system $S = \{ v_1, v_2 \}$ with $|\text{supp}(S)| > 2$, $v_1 = (x_1, x_2, x_3, x_4)$, $v_2 = (y_1, y_2, y_3, y_4)$ and $p \geq 1$. Suppose, rearranging the coordinates of v_1 and v_2 if necessary, that

$$x_1 \neq 0, \quad \begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix} \neq 0 \quad \text{and} \quad 4 \in \text{supp}(S), \text{ i.e., } x_4 \neq 0 \text{ or } y_4 \neq 0.$$

The Smith quasi-normal form of S is:

$$L\,V\,R = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & cd & 0 & 0 \end{pmatrix} \quad \text{such that} \quad \begin{array}{l} L \in GL_k(\mathbb{Q}) \\ R \in GL_4(\mathbb{Z}) \\ 0 < c, d \\ R = R_1\,R_2\,R_3\,R_4\,R_5, \end{array}$$

where the matrices L and R_i, $1 \leq i \leq 5$, and the parameters c and d are those that appear in Table 1.

Lemma 2 *Given a number $p \geq 1$ and a p-orthonormal system $S = \{v_1, v_2\}$ with associated lattice Λ, then $B^{\perp} = \{w_1, w_2\}$ is a basis of $\Lambda^{\perp}$, where*

$$w_1 = \left(\frac{x_2\,y_3'}{c_1\,d_1} - \frac{x_3\,y_2'\,\sigma_1}{c_2\,d_1}, -\frac{x_1\,y_3'}{c_1\,d_1} - \frac{x_3\,y_2'\,\tau_1}{c_2\,d_1}, \frac{c_1\,y_2'}{c_2\,d_1}, 0 \right)$$

$$w_2 = \left(\frac{y_4'(c_1\,x_3\,\sigma_1\,\tau_4 + c_2\,x_2\,\sigma_4)}{c_1\,c_2\,d} - \frac{d_1\,x_4\,\sigma_1\,\sigma_2}{c\,d}, \right.$$
$$\left. \frac{y_4'(c_1\,x_3\,\tau_1\,\tau_4 - c_2\,x_1\,\sigma_4)}{c_1\,c_2\,d} - \frac{d_1\,x_4\,\sigma_2\,\tau_1}{c\,d}, -\frac{d_1\,x_4\,\tau_2}{c\,d} - \frac{c_1\,y_4'\,\tau_4}{c_2\,d}, \frac{c_2\,d_1}{c\,d} \right).$$

Proof We obtain the result just by multiplying the matrices R_1, R_2, R_3, R_4 and R_5 and applying Lemma 1 to the Smith quasi-normal form of S. □

Remark 1 Let V and G_V be the coordinate matrix and the Gram matrix, respectively, of the set of vectors $B \cup B^{\perp}$, and let G be the Gram matrix of the set of vectors $B^{\perp}$. Then, $\det^2(V) = \det(G_V) = p^2\det(G)$, and since $\det^2(\Lambda^{\perp}) = \det(G)$, we concluded that $\det(\Lambda^{\perp}) = \dfrac{|\det(V)|}{p}$.

We can use Remark 1 to compute $\det(\Lambda^{\perp})$ and, indirectly, to study the matrix G, considered as a symmetric positive definite quadratic form.

Proposition 4 *Given a number $p \geq 1$ and a p-orthonormal system $S = \{v_1, v_2\}$, with associated lattice Λ, then $det(\Lambda^{\perp}) = \dfrac{p}{c\,d}$, where c and d are the parameters that appear in* Table 1.

Proof To obtain the result we only have to compute det(V), by Remark 1. Developing the expression of the determinant of V, where w_1 and w_2 are the vectors obtained in Lemma 2, we obtain:

Table 1 Smith quasi-normal form data

$$R_1 = \begin{pmatrix} \sigma_1 & \frac{-x_2}{c_1} & 0 & 0 \\ \tau_1 & \frac{x_1}{c_1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} x_1\sigma_1 + x_2\tau_1 = c_1 = \gcd(x_1, x_2) \\ y_1' = \sigma_1 y_1 + \tau_1 y_2 \\ y_2' = \dfrac{-x_2}{c_1} y_1 + \dfrac{x_1}{c_1} y_2 \end{array}$$

$$R_2 = \begin{pmatrix} \sigma_2 & 0 & \frac{-x_3}{c_2} & 0 \\ 0 & 1 & 0 & 0 \\ \tau_2 & 0 & \frac{c_1}{c_2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{array}{l} c_1\sigma_2 + x_3\tau_2 = c_2 = \gcd(c_1, x_3) \\ y_1'' = \sigma_2 y_1' + \tau_2 y_3 = \sigma_2\sigma_1 y_1 + \sigma_2\tau_1 y_2 + \tau_2 y_3 \\ y_3' = \dfrac{-x_3}{c_2} y_1' + \dfrac{c_1}{c_2} y_3 = \dfrac{-x_3}{c_2}\sigma_1 y_1 + \dfrac{-x_3}{c_2}\tau_1 y_2 + \dfrac{c_1}{c_2} y_3 \end{array}$$

$$R_3 = \begin{pmatrix} \sigma_3 & 0 & 0 & \frac{-x_4}{c} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \tau_3 & 0 & 0 & \frac{c_2}{c} \end{pmatrix} \quad c_2\sigma_3 + x_4\tau_3 = c = \gcd(c_2, x_4)$$

$$y_1''' = \sigma_3 y_1'' + \tau_3 y_4 = \sigma_3\sigma_2\sigma_1 y_1 + \sigma_3\sigma_2\tau_1 y_2 + \sigma_3\tau_2 y_3 + \tau_3 y_4$$
$$y_4' = \frac{-x_4}{c} y_1'' + \frac{c_2}{c} y_4 = \frac{-x_4}{c}\sigma_2\sigma_1 y_1 + \frac{-x_4}{c}\sigma_2\tau_1 y_2 + \frac{-x_4}{c}\tau_2 y_3 + \frac{c_2}{c} y_4$$

$$L = \begin{pmatrix} 1 & 0 \\ -y_1''' & c \end{pmatrix}$$

$$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_4 & \frac{-y_3'}{d_1} & 0 \\ 0 & \tau_4 & \frac{y_2}{d_1} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad y_2'\sigma_4 + y_3'\tau_4 = d_1 = \gcd(y_2', y_3')$$

$$R_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sigma_5 & 0 & \frac{-y_4'}{d} \\ 0 & 0 & 1 & 0 \\ 0 & \tau_5 & 0 & \frac{d_1}{d} \end{pmatrix} \quad d_1\sigma_5 + y_4'\tau_5 = d = \gcd(d_1, y_4')$$

$$\begin{aligned} \det(V)c_1c_2d_1cd = {} & cy_4'\Big(c_1\Big(x_1^2y_4 - x_1x_4y_1 + x_2\left(x_2y_4 - x_4y_2\right)\Big) \\ & + x_3\Big(\underline{x_1\sigma_1 + x_2\tau_1}\Big)\left(x_3y_4 - x_4y_3\right)\Big)\Big(\underline{y_2'\sigma_4 + y_3'\tau_4}\Big) \\ & + d_1\Big(c_1^2y_2'\Big(c_2\left(x_1y_2 - x_2y_1\right) + x_1x_4y_4\sigma_2\tau_1 \\ & - x_4\sigma_2\Big(x_2y_4\sigma_1 + x_4\left(y_1\tau_1 - y_2\sigma_1\right)\Big)\Big) \\ & + c_1x_3y_2'\Big(c_2\Big(x_1y_3\tau_1 - x_2y_3\sigma_1 + x_3\left(y_2\sigma_1 - y_1\tau_1\right)\Big) \\ & + x_4\tau_2\Big(x_1y_4\tau_1 - x_2y_4\sigma_1 + x_4\left(y_2\sigma_1 - y_1\tau_1\right)\Big)\Big) \\ & + c_2y_3'\Big(c_2\Big(x_1^2y_3 - x_1x_3y_1 + x_2\left(x_2y_3 - x_3y_2\right)\Big) \\ & + x_4\Big(x_1^2y_4\tau_2 - x_1\Big(x_3y_4\sigma_1\sigma_2 + x_4\left(y_1\tau_2 - y_3\sigma_1\sigma_2\right)\Big) \\ & + x_2\Big(x_2y_4\tau_2 - x_3y_4\sigma_2\tau_1 + x_4\left(y_3\sigma_2\tau_1 - y_2\tau_2\right)\Big)\Big)\Big)\Big)\Big), \end{aligned}$$

Table 2 Monomials of $\det(V)c_1c_2cd$

1		$c_1c_2x_1^2y_2^2$	2		$c_1c_2x_1^2y_3^2$
3		$c_1c_2x_1^2y_4^2$	4		$-2c_1c_2x_1x_2y_1y_2$
5	×	$-c_1c_2x_1x_3y_1y_3$	6	×	$-c_1c_2x_1x_4y_1y_4$
7		$c_1c_2x_2^2y_1^2$	8		$c_1c_2x_2^2y_3^2$
9		$c_1c_2x_2^2y_4^2$	10	×	$-c_1c_2x_2x_3y_2y_3$
11	×	$-c_1c_2x_2x_4y_2y_4$	12		$c_1c_2x_3^2y_4^2$
13	×	$-c_1c_2x_3x_4y_3y_4$	14	×	$-c_1x_1^2x_4y_1y_4\sigma_1\sigma_2$
15	×	$-c_1x_1x_2x_4y_1y_4\sigma_2\tau_1$	16	×	$-c_1x_1x_2x_4y_2y_4\sigma_1\sigma_2$
17	×	$-c_1x_1x_3x_4y_3y_4\sigma_1\sigma_2$	18	×	$c_1x_1x_4^2y_1^2\sigma_1\sigma_2$
19	×	$c_1x_1x_4^2y_2^2\sigma_1\sigma_2$	20	×	$c_1x_1x_4^2y_3^2\sigma_1\sigma_2$
21	×	$-c_1x_2^2x_4y_2y_4\sigma_2\tau_1$	22	×	$-c_1x_2x_3x_4y_3y_4\sigma_2\tau_1$
23	×	$c_1x_2x_4^2y_1^2\sigma_2\tau_1$	24	×	$c_1x_2x_4^2y_2^2\sigma_2\tau_1$
25	×	$c_1x_2x_4^2y_3^2\sigma_2\tau_1$	26	×	$-c_1x_3^2x_4y_1y_4\sigma_1\sigma_2$
27	×	$-c_1x_3^2x_4y_2y_4\sigma_2\tau_1$	28	×	$-c_1x_3^2x_4y_3y_4\tau_2$
29	×	$c_1x_3x_4^2y_1y_3\sigma_1\sigma_2$	30	×	$c_1x_3x_4^2y_2y_3\sigma_2\tau_1$
31	×	$c_1x_3x_4^2y_3^2\tau_2$	32	×	$-c_2x_1^2x_3y_1y_3\sigma_1$
33	×	$-c_2x_1x_2x_3y_1y_3\tau_1$	34	×	$-c_2x_1x_2x_3y_2y_3\sigma_1$
35	×	$c_2x_1x_3^2y_1^2\sigma_1$	36	×	$c_2x_1x_3^2y_2^2\sigma_1$
37	×	$-c_2x_2^2x_3y_2y_3\tau_1$	38	×	$c_2x_2x_3^2y_1^2\tau_1$
39	×	$c_2x_2x_3^2y_2^2\tau_1$	40	×	$-x_1^2x_3x_4y_1y_4\sigma_1\tau_2$
41	×	$-x_1x_2x_3x_4y_1y_4\tau_1\tau_2$	42	×	$-x_1x_2x_3x_4y_2y_4\sigma_1\tau_2$
43	×	$x_1x_3^2x_4y_1y_4\sigma_1^2\sigma_2$	44	×	$x_1x_3^2x_4y_2y_4\sigma_1\sigma_2\tau_1$
45	×	$x_1x_3x_4^2y_1^2\sigma_1\tau_2$	46	×	$-x_1x_3x_4^2y_1y_3\sigma_1^2\sigma_2$
47	×	$x_1x_3x_4^2y_2^2\sigma_1\tau_2$	48	×	$-x_1x_3x_4^2y_2y_3\sigma_1\sigma_2\tau_1$
49	×	$-x_2^2x_3x_4y_2y_4\tau_1\tau_2$	50	×	$x_2x_3^2x_4y_1y_4\sigma_1\sigma_2\tau_1$
51	×	$x_2x_3^2x_4y_2y_4\sigma_2\tau_1^2$	52	×	$x_2x_3x_4^2y_1^2\tau_1\tau_2$
53	×	$-x_2x_3x_4^2y_1y_3\sigma_1\sigma_2\tau_1$	54	×	$x_2x_3x_4^2y_2^2\tau_1\tau_2$
55	×	$-x_2x_3x_4^2y_2y_3\sigma_2\tau_1^2$			

where all the parameters appear in Table 1.

Throughout the proof, we will replace expressions by applying equalities from Table 1.

Substituting the underlined expressions by c_1 and d_1, respectively, all occurrences of d_1 are canceled. Similarly, substituting c_1y_2', c_2y_3' and cy_4' for the expressions

$$\begin{aligned}&x_1y_2 - x_2y_1,\\ &c_1y_3 - x_3(\sigma_1y_1 + \tau_1y_2) \text{ and}\\ &c_2y_4 - x_4(\sigma_2\sigma_1y_1 + \sigma_2\tau_1y_2 + \tau_2y_3),\end{aligned}$$

respectively, the parameter c disappears from the second equality member.

Table 3 Monomials resulting from operations

14	×	15	$-c_1^2x_1x_4y_1y_4\sigma_2$	16	×	21	$-c_1^2x_2x_4y_2y_4\sigma_2$
17	×	22	$-c_1^2x_3x_4y_3y_4\sigma_2$	18	×	23	$c_1^2x_4^2y_1^2\sigma_2$
19	×	24	$c_1^2x_4^2y_2^2\sigma_2$	20	×	25	$c_1^2x_4^2y_3^2\sigma_2$
32	×	33	$-c_1c_2x_1x_3y_1y_3$	34	×	37	$-c_1c_2x_2x_3y_2y_3$
35		38	$c_1c_2x_3^2y_1^2$	36		39	$c_1c_2x_3^2y_2^2$
40	×	41	$-c_1x_1x_3x_4y_1y_4\tau_2$	42	×	49	$-c_1x_2x_3x_4y_2y_4\tau_2$
43	×	50	$c_1x_3^2x_4y_1y_4\sigma_1\sigma_2$	44	×	51	$c_1x_3^2x_4y_2y_4\sigma_2\tau_1$
45	×	52	$c_1x_3x_4^2y_1^2\tau_2$	46	×	53	$-c_1x_3x_4^2y_1y_3\sigma_1\sigma_2$
47	×	54	$c_1x_3x_4^2y_2^2\tau_2$	48	×	55	$-c_1x_3x_4^2y_2y_3\sigma_2\tau_1$
14	×	40	$-c_1c_2x_1x_4y_1y_4$	16	×	42	$-c_1c_2x_2x_4y_2y_4$
17	×	28	$-c_1c_2x_3x_4y_3y_4$	18		45	$c_1c_2x_4^2y_1^2$
19		47	$c_1c_2x_4^2y_2^2$	20		31	$c_1c_2x_4^2y_3^2$
26	×	43	0	27	×	44	0
29	×	46	0	30	×	48	0
5		32	$-2c_1c_2x_1x_3y_1y_3$	6		14	$-2c_1c_2x_1x_4y_1y_4$
10		34	$-2c_1c_2x_2x_3y_2y_3$	11		16	$-2c_1c_2x_2x_4y_2y_4$
13		17	$-2c_1c_2x_3x_4y_3y_4$				

The expression $\det(V)c_1c_2cd$ is a homogeneous polynomial of total degree 6 in the variables c_1, c_2, x_1, x_2, x_3, x_4, y_1, y_2, y_3 and y_4, in which only the parameters σ_1, τ_1, σ_2 and τ_2 appear. The monomials of the aforementioned polynomial are included in Table 2 and are identified by indexes placed in the first cells of the corresponding rows.

In order to eliminate the parameters σ_1, τ_1, σ_2 and τ_2, we group the monomials of Table 2 in pairs to apply the following operations:

(1) Substitute $x_1\sigma_1 + x_2\tau_1$ by c_1.
(2) Substitute $c_1\sigma_2 + x_3\tau_2$ by c_2.
(3) Cancel opposite monomials.
(4) Add equal monomials.

Applied operations are detailed in Table 3, where the resulting monomials are identified by the indexes of the first monomials that are operated on. Each time an operation is applied, the monomials involved are marked with a × to the right of the index that identifies the monomial, so as not to use them again. The operations are done iteratively on monomials of Tables 2 and 3 that are not marked, until no operation can be further applied.

All the resulting monomials have the factor c_1c_2. Therefore, by simplifying this factor the next equality is obtained:

Table 4 Monomials of $N(w_1)c_1^2c_2^2d_1^2$ and resulting from operations

1	$c_1^2x_1^2y_2^2$		6	$-2c_1x_1^2x_3y_1y_3\sigma_1$	
2	$c_1^2x_1^2y_3^2$		7	$-2c_1x_1x_2x_3y_1y_3\tau_1$	$-2c_1^2x_1x_3y_1y_3$
3	$-2c_1^2x_1x_2y_1y_2$		8	$-2c_1x_1x_2x_3y_2y_3\sigma_1$	
4	$c_1^2x_2^2y_1^2$		9	$-2c_1x_2^2x_3y_2y_3\tau_1$	$-2c_1^2x_2x_3y_2y_3$
5	$c_1^2x_2^2y_3^2$				
10	$x_1^2x_3^2y_1^2\sigma_1^2$	$c_1^2x_3^2y_1^2$	11	$x_1^2x_3^2y_2^2\sigma_1^2$	$c_1^2x_3^2y_2^2$
12	$2x_1x_2x_3^2y_1^2\sigma_1\tau_1$		13	$2x_1x_2x_3^2y_2^2\sigma_1\tau_1$	
14	$x_2^2x_3^2y_1^2\tau_1^2$		15	$x_2^2x_3^2y_2^2\tau_1^2$	

$$\begin{aligned}\det(V)cd = {} & x_1^2y_2^2 + x_1^2y_3^2 + x_1^2y_4^2 - 2x_1x_2y_1y_2 - 2x_1x_3y_1y_3 - 2x_1x_4y_1y_4\\ & x_2^2y_1^2 + x_2^2y_3^2 + x_2^2y_4^2 - 2x_2x_3y_2y_3 - 2x_2x_4y_2y_4 + x_3^2y_4^2\\ & -2x_3x_4y_3y_4 + x_4^2y_1^2 + x_4^2y_2^2 + x_4^2y_3^2 + x_3^2y_1^2 + x_3^2y_2^2.\end{aligned}$$

By polynomial checking, it is easy to verify the next equality:

$$\det(V)cd = \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) - (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2.$$

By hypothesis, the second member of the previous equality is equal to p^2. Therefore, by applying Remark 1, we conclude that:

$$\det(\Lambda^{\perp}) = \frac{p}{cd}.$$

□

Lemma 3 *Given a number $p \geq 1$, a p-orthonormal system $S = \{v_1, v_2\}$ and w_1 the first vector of the basis $B^{\perp}$ of the orthogonal lattice $\Lambda^{\perp}$, then $N(w_1) = \dfrac{p(p - x_4^2 - y_4^2)}{c_2^2d_1^2}$, where c_2 and d_1 are the parameters in* Table 1.

Proof The proof is similar to that of Proposition 4. Considering the vector w_1 obtained in Lemma 2 and calculating $N(w_1)$, the following equality is obtained:

$$N(w_1)c_1^2c_2^2d_1^2 = c_1^4y_2'^2 + c_1^2x_3^2y_2'^2\left(\sigma_1^2 + \tau_1^2\right) + 2c_1c_2x_3y_2'y_3'(x_1\tau_1 - x_2\sigma_1) + c_2^2y_3'^2\left(x_1^2 + x_2^2\right).$$

Substituting in the second member of equality c_1y_2' by $-x_2y_1 + x_1y_2$ and c_2y_3' by $-x_3\sigma_1y_1 - x_3\tau_1y_2 + c_1y_3$, a homogeneous polynomial of total grade 6 in the variables $c_1, x_1, x_2, x_3, y_1, y_2$ and y_3 is obtained, in which only the parameters σ_1 and τ_1 appear.

The monomials of the aforementioned polynomial are listed in Table 4. The results of the following substitution are also included in the table: Replace $x_1\sigma_1 + x_2\tau_1$ by c_1.

All the remaining monomials are multiplied by the factor c_1^2. Therefore, simplifying this factor, we obtain:

$$\begin{aligned} N(w_1)c_2^2d_1^2 = {} & x_1^2y_2^2 + x_1^2y_3^2 - 2x_1x_2y_1y_2 + x_2^2y_1^2 + x_2^2y_3^2 \\ & -2x_1x_3y_1y_3 - 2x_2x_3y_2y_3 + x_3^2y_1^2 + x_3^2y_2^2. \end{aligned}$$

By polynomial checking, it is easy to verify the next equality:

$$\begin{aligned} N(w_1)c_2^2d_1^2 = {} & \left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) \\ & -(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 - x_4^2\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) \\ & -y_4^2\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right) + 2x_4y_4(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4). \end{aligned}$$

By hypothesis, the second member of the previous equality is equal to $p^2 - px_4^2 - py_4^2$. Therefore, we conclude that:

$$N(w_1) = \frac{p\left(p - x_4^2 - y_4^2\right)}{c_2^2d_1^2}.$$

□

Lemma 4 *Given a prime number p and a p-orthonormal system $S = \{v_1, v_2\}$ with $|supp(S)| > 2$, associated with the lattice Λ, then $c = d = 1$, where c and d are the parameters that appear in* Table 1.

Proof According to Table 1, it holds that $c = \gcd(x_1, x_2, x_3, x_4)$, and by Proposition 3, we conclude that $c = 1$. This result implies that the Smith quasi-normal form described in Table 1 is actually a normal form, because in this case $L \in GL_k(\mathbb{Z})$, and consequently, d is the second invariant factor of V. Considering once more Proposition 3, we conclude that $d = 1$. □

Proposition 5 *Given a prime number p, a p-orthonormal system $S = \{v_1, v_2\}$ with $|supp(S)| > 2$ and the Gram matrix G of the basis $B^\perp = \{w_1, w_2\}$ of the orthogonal lattice $\Lambda^\perp$, then it holds that $p \mid G$.*

Proof Suppose that the Gram matrix $G = \begin{pmatrix} \mu & \lambda \\ \lambda & \nu \end{pmatrix}$.

Let us consider the value of $\mu = N(w_1)$ obtained in Lemma 3. The prime factorization of $p(p - x_4^2 - y_4^2)$ contains only one factor p, because p is prime and $-p < p - x_4^2 - y_4^2 < p$. (Remember that we are assuming that $x_4 \neq 0$ or $y_4 \neq 0$.) Then, the prime factorization of $c_2^2\, d_1^2$ does not contain p, because the number of times it contains each prime factor is even. Consequently, $c_2^2\, d_1^2 \mid (p - x_4^2 - y_4^2)$ and this implies that $p \mid \mu$, i.e., $\mu = p\,\mu'$. Moreover, $|\mu'| < p$.

Applying Proposition 4, Lemma 4 and the property $\det^2(\Lambda^\perp) = \det(G)$, we get $p^2 = p\,\mu'\,\nu - \lambda^2$. This implies $p \mid \lambda^2$, and keeping in mind that p is a prime, we have that $p \mid \lambda$, i.e., $\lambda = p\,\lambda'$.

Reconsidering the previous equality, and canceling a factor p, we obtain $p = \mu'\,\nu - p\,\lambda'^2$. This implies again that $p \mid \mu'\,\nu$, and considering that p is prime and $|\mu'| < p$, we get $p \mid \nu$, i.e., $\nu = p\,\nu'$.

We arrive to the final conclusion that $G = p \begin{pmatrix} \mu' & \lambda' \\ \lambda' & \nu' \end{pmatrix}$, i.e., $p \mid G$. □

Theorem 3 *Given a prime number p, a p-orthonormal system $S = \{ v_1, v_2 \}$ with $|supp(S)| > 2$ and associated lattices Λ and $\Lambda^\perp$, there exists $v \in \Lambda^\perp$ such that it verifies $N(v) = p$.*

Proof Let G be the Gram matrix of the basis $B^\perp$ of the associated lattice $\Lambda^\perp$.

Proposition 4, Lemma 4 and property $\det^2(\Lambda^\perp) = \det(G)$ allow us to conclude that $\det(G) = p^2$. Applying now Proposition 5, we obtain that $G' = \dfrac{G}{p}$ is an unimodular matrix, i.e., $G' \in GL_2(\mathbb{Z})$, and that, given a vector $v \in \Lambda^\perp$, $N(v) = b^t\, G\, b = p$ if and only if $b^t\, G'\, b = 1$, b being the coordinate vector of v in the basis $B^\perp$.

Let $K = \{ x \in \mathbb{R}^2 \mid x^t\, G'\, x \leq 1 \}$ and $\{u_1, u_2\}$ be an orthonormal basis of eigenvectors of G' with eigenvalues λ_1 and λ_1, respectively. Note that λ_1 and λ_2 are real, since G' is symmetric, positive, because G' is definite positive, and verify $\lambda_1\, \lambda_2 = \det(G') = 1$. Then K is the ellipse $\lambda_1 x^2 + \lambda_2 y^2 \leq 1$, with respect to the reference system determined by u_1 and u_2, and has volume $\pi \frac{1}{\sqrt{\lambda_1}} \frac{1}{\sqrt{\lambda_2}} = \pi$.

Given a $0 < \epsilon < 1$, let be E_ϵ the ellipse K scaled by a factor $f_\epsilon = \frac{2}{\sqrt{\pi}} + \epsilon$. The ellipse E_ϵ has volume $\pi\, f_\epsilon^2 > \pi \frac{2^2}{\pi} = 2^2$. Then, for Theorem 2, there exists a point b in the lattice $\mathbb{Z}^2$ (with volume of the fundamental domain 1) such that $b \neq 0$ and $b \in E_\epsilon$. Since the set of points of $\mathbb{Z}^2$ that belong to any of the ellipses E_ϵ is finite, it is shown that there is a point b in the lattice $\mathbb{Z}^2$ such that $b \neq 0$ and $b \in K$.

The point b defines a vector $v \in \Lambda^\perp$ that verifies $0 < b^t\, G'\, b \leq 1$. Then, it holds $b^t\, G'\, b = 1$, since $b^t\, G'\, b$ is integer, and, at last, is the wanted vector of $\Lambda^\perp$, because $N(v) = b^t\, G\, b = p$. □

References

1. Cassels, J.W.S.: An Introduction to the Geometry of Numbers. Springer, Berlin (1997)
2. Chou, T.-W.J., Collins, G.E.: Algorithms for the solution of systems of linear Diophantine equations. SIAM J. Comput. **11**, 687–708 (1982)
3. Eum, I.S., Shin, D.H., Yoon, D.S.: Representations by $x_1^2 + 2x_2^2 + x_3^2 + x_4^2 + x_1x_3 + x_1x_4 + x_2x_4$. J. Number Theory **131**, 2376–2386 (2011)
4. Gauss, C.F.: Disquisitiones Arithmeticae. Yale University Press, New Haven (1966)
5. Gatti, L.N., Lacalle, J.: A model of discrete quantum computation. Quantum Inf. Process. **17**, 192 (2018)
6. Jones, G.A., Jones, J.M.: Elementary Number Theory. Springer, Berlin (1998)
7. Ju, J., Oh, B.-K.: Universal sums of generalized octagonal numbers. J. Number Theory **190**, 292–302 (2018)
8. Lagrange, J.L.: Demonstration d'un theoreme d'arithmétique. Oeuvres Complètes **3**, 189–201 (1869)
9. Mordell, L.J.: A new Waring's problem with squares of linear forms. Q. J. Math. Oxf. **1**, 276–288 (1930)
10. Ramanujan, S.: On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$. Proc. Camb. Philos. Soc. **19**, 11–21 (1917)
11. Smith, H.J.S.: On systems of linear indeterminate equations and congruences. Philos. Trans. Lond. **151**, 293–326 (1861)
12. Sun, Y.-C., Sun, Z.-W.: Some variants of Lagrange's four squares theorem. arXiv:1605.03074v7 [math.NT] 14 Mar (2018)

13. Sun, Z.-W.: A result similar to Lagrange's theorem. J. Number Theory **162**, 190–211 (2016)
14. Sun, Z.-W.: Refining Lagrange's four-square theorem. J. Number Theory **175**, 167–190 (2017)
15. Ye, D.: Representations of integers by certain 2k-ary quadratic forms. J. Number Theory **179**, 50–64 (2017)