International Journal of Applied Mathematics

Volume 33 No. 4 2020, 663-672
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v33i4.10

WELL-ROUNDED LATTICES VIA POLYNOMIALS WITH REAL ROOTS

Carina Alves[1 §], William L.S. Pinto[2], Antonio A. Andrade[3]

[1,2] Department of Mathematics
São Paulo State University
Rio Claro - SP, 13506-900, BRAZIL

[3] Department of Mathematics
São Paulo State University
São Jos do Rio Preto-SP, 15054-000, BRAZIL

Abstract: Well-rounded lattices have been a topic of recent studies with applications in wiretap channels and in cryptography. A lattice of full rank in Euclidean space is called well-rounded if its set of minimal vectors spans the whole space. In this paper, we investigate the well-roundedness of lattices coming from polynomials with integer coefficients and real roots.

AMS Subject Classification: 11H31, 11H06, 11H71
Key Words: well-rounded lattice; minimum norm; polynomials; dense packing

1. Introduction

A large class of the problems in coding theory is related to the properties of lattices [1, 9]. A *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^n$. Equivalently, $\Lambda \subset \mathbb{R}^n$ is a lattice if there are linearly independent vectors $v_1, \ldots, v_m \in \mathbb{R}^n$, with $m \leq n$, such that any $v \in \Lambda$ can be written as $v = \sum_{i=1}^{m} x_i v_i$, where $x_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, m$. The set $\{v_1, \ldots, v_m\}$ is called a basis for Λ.A matrix

Received: April 19, 2020

§Correspondence author

M whose rows are these vectors is said to be a *generator matrix* for Λ and its *Gram matrix* is $G = MM^t$, where ^{t} stands for the transpose. If $m = n$, then Λ is a *full-ranked lattice*. The *determinant* of Λ is given by $det(\Lambda) = det(G)$ and it is an invariant under basis change, Conway and Sloane [2].

The *minimum* of a lattice Λ is defined by $|\Lambda| = \min\{\|v\|^2 : v \in \Lambda,\ v \neq 0\}$ and its *center density* is $\delta(\Lambda) = \frac{(\sqrt{|\Lambda|}/2)^n}{|det(M)|}$. The set of minimal vectors of Λ is defined by $S(\Lambda) = \{v \in \Lambda : \|v\|^2 = |\Lambda|\}$ and its elements are called *minimal vectors* of Λ. We denote the number of minimal vectors by $|S(\Lambda)|$ and we say a lattice Λ is well-rounded when $S(\Lambda)$ spans $\mathbb{R}^n$.

Fukshansky and Petersen [4] investigated the connection between well-rounded lattices and the well known class of ideal lattices, focusing especially on the case of lattices in $\mathbb{R}^2$. Polynomials with integer coefficients are used in [8] to construct cyclic lattices, i.e., sublattices in $\mathbb{Z}^n$, whereas Fukshansky and Sun [5] have investigated the well-roundedness property.

Polynomials can also be used to obtain lattices in $\mathbb{R}^2$ and $\mathbb{R}^3$ (see Flores et al. [3]). In this paper, we construct lattices that are generated by vectors that have as their entries the roots of a polynomial with integer coefficients and real roots. More precisely, if $\{\rho_1, \ldots, \rho_n\}$ is the set of roots of a polynomial, we perform $rot(\rho_1, \ldots, \rho_n)$, where rot is the rotational shift operator defined by $rot(\rho_1, \rho_2, \ldots, \rho_{n-1}, \rho_n) = (\rho_n, \rho_1, \rho_2, \ldots, \rho_{n-1})$.

We use the well known Vieta's formulas to prove the linear independence of the vectors considered and to obtain the Euclidean norm in terms of the polynomial coefficients. An advantage is that we can establish conditions involving such coefficients in order to increase the number of minimum vectors of the lattice, as will be shown in this paper. We also find conditions to obtain lattices with the highest packing densities in dimensions 2 and 3. For dimension 4, we obtain a lattice with center density approximately 0.083333, which is 0.041667 lower than the center density of the lattice with the highest packing density in $\mathbb{R}^4$.

Due to the importance of well-rounded lattices, in this paper, we also investigate in which conditions lattices obtained via polynomials up to dimension 4 are well-rounded.

This paper is organized as follows. In Section 2, we present conditions to obtain well-rounded lattices via quadratic polynomials. We also obtain lattices with the highest center density in dimension 2. In Section 3, we present conditions to obtain well-rounded lattices via cubic polynomials. In dimension 3, we obtain lattices with the highest center density. In Section 4, we present conditions to obtain well-rounded lattices via quartic polynomials. Finally, in

Section 5, we present our conclusions.

2. Well-rounded lattices via quadratic polynomials

In this section, we establish conditions to obtain well-rounded lattices via monic polynomials of degree 2 with real distinct roots.

Let $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$ be a polynomial with two real distinct roots denoted by α and β. In this case, the discriminant of $f(x)$ is greater than zero, i.e, $a^2 - 4b > 0$. Let us construct a lattice Λ_f by identifying a linearly independent set $\{v_1, v_2\}$ over $\mathbb{R}$, where the vectors v_1 and v_2 are permutations of the roots of the polynomial $f(x)$.

In order to choose linearly independent vectors v_1 and v_2 it is enough to ensure that the matrix M with these vectors as rows has a non-zero determinant. The matrix M will be then a generator matrix of Λ_f.

Consider $v_1 = (\alpha, \beta)$ and $v_2 = (\beta, \alpha)$. Thus,

$$det(M) = \begin{vmatrix} \alpha & \beta \\ \beta & \alpha \end{vmatrix} = -2a\sqrt{a^2 - 4b} \neq 0,$$

since $a \neq 0$. Therefore, if we consider $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, with $a \neq 0$, then we can define Λ_f as the lattice generated by the vectors $v_1 = (\alpha, \beta)$ and $v_2 = (\beta, \alpha)$.

The next result provides the minimum of Λ_f explicitly.

Lemma 1. *Let $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots α and β, and Λ_f be the lattice generated by $\{v_1, v_2\}$, where $v_1 = (\alpha, \beta)$ and $v_2 = (\beta, \alpha)$. If $v = x_1v_1 + x_2v_2$ is an element of Λ_f, where $x_1, x_2 \in \mathbb{Z}$, then $\|v\|^2 = a^2({x_1}^2 + {x_2}^2) - 2b(x_1 - x_2)^2$.*

Proof. Since $\|v\|^2 = v \cdot v = x_1^2\|v_1\|^2 + 2x_1x_2v_1 \cdot v_2 + x_2^2\|v_2\|^2$, $\|v_1\|^2 = \|v_2\|^2 = \alpha^2 + \beta^2 = a^2 - 2b$ and $v_1 \cdot v_2 = 2\alpha\beta = a^2 - 2b$, the result follows. □

We are interested in verifying in which conditions Λ_f is well-rounded. For notation purposes, define $g : \mathbb{Z}^2 \to \mathbb{R}_+$ by $g(v) = g(x_1, x_2) = a^2(x_1^2 + x_2^2) - 2b(x_1 - x_2)^2$, i.e., $\|v\|^2 = g(x_1, x_2)$. In order to identify when $g(x_1, x_2)$ takes minimum value, it is easy to see that it is enough to check its values when x_1 and x_2 vary between 0, 1 and -1. Note that

(i) $g(\pm 1, 0) = g(0, \pm 1) = a^2 - 2b$;

(ii) $g(1,1) = g(-1,-1) = 2a^2$;

(iii) $g(-1,1) = g(1,-1) = 2a^2 - 8b$.

We know from Fukshansky and Petersen [4] that $\Lambda_f \subset \mathbb{R}^2$ is well-rounded if and only if $|S(\Lambda)| = 4$ or $|S(\Lambda)| = 6$. In this latter case, Λ_f has the highest packing density in dimension 2. Note that $|S(\Lambda)| = 4$ if and only if $\min\{a^2 - 2b, 2a^2, 2a^2 - 8b\} = a^2 - 2b$, that is, $a^2 - 2b \leq 2a^2$ and $a^2 - 2b \leq 2a^2 - 8b$. Hence, $-2b \leq a^2$ and $6b \leq a^2$. When $b \geq 0$ (respectively, $b < 0$) the inequalities above are satisfied if and only if $a^2 \geq 6b$ (respectively, $a^2 \geq -2b$). It is easy to see that $|S(\Lambda)| = 6$ if and only if $a^2 - 2b = 2a^2$ or $a^2 - 2b = 2a^2 - 8b$ which is equivalent to $a^2 = -2b$ or $a^2 = 6b$. Consequently, we have proved the following theorem.

Theorem 2. *Let $f(x) = x^2 + ax + b \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots. If $\alpha, \beta \in \mathbb{R}$ are the distinct roots of $f(x)$, then the lattice Λ_f generated by the basis $\{(\alpha,\beta),(\beta,\alpha)\}$ is well-rounded if and only if $a^2 \geq -2b$ (with $b < 0$) or $a^2 \geq 6b$ (with $b \geq 0$). Moreover, Λ_f has the highest packing density in dimension 2 if and only if $a^2 = 6b$ or $a^2 = -2b$.*

3. Well-rounded lattices via cubic polynomials

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be a polynomial with three real distinct roots denoted by α, β and γ. Let us construct a lattice Λ_f by identifying a linearly independent set $\{v_1, v_2, v_3\}$ over $\mathbb{R}$.

Consider $v_1 = (\alpha, \beta, \gamma)$. The other vectors $v_2 = (\gamma, \alpha, \beta)$ and $v_3 = (\beta, \gamma, \alpha)$ are obtained from the rotational shift operator on $\mathbb{R}^3$. A simple calculation using Vieta's formulas shows that

$$det(M) = \begin{vmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{vmatrix} = -a(a^2 - 3b).$$

Since $f(x)$ has real distinct roots, so does its derivative $f'(x)$. This implies that the discriminant of $f'(x)$ is greater than zero, that is, $a^2 - 3b > 0$. Therefore, if $a \neq 0$, then $det(M) \neq 0$.

The next result provides the minimum of Λ_f, explicitly.

Lemma 3. *Let $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots α, β and γ. Let Λ_f be a lattice in $\mathbb{R}^3$ generated by the basis $\{v_1, v_2, v_3\}$, where $v_1 = (\alpha, \beta, \gamma)$, $v_2 = (\gamma, \alpha, \beta)$ and $v_3 = (\beta, \gamma, \alpha)$. If $v \in \Lambda_f$, where $v = x_1v_1 + x_2v_2 + x_3v_3$, with $x_1, x_2, x_3 \in \mathbb{Z}$, then*

$$\|v\|^2 = (a^2 - 2b)(x_1^2 + x_2^2 + x_3^2) + 2b(x_1x_2 + x_1x_3 + x_2x_3).$$

Proof. Since $\|v\|^2 = v \cdot v = x_1^2\|v_1\|^2 + x_2^2\|v_2\|^2 + x_3^2\|v_3\|^2 + 2(x_1x_2v_1 \cdot v_2 + x_1x_3v_1 \cdot v_3 + x_2x_3v_2 \cdot v_3)$, by Vieta's formulas, it follows that $|v_i\|^2 = \alpha^2+\beta^2+\gamma^2 = a^2 - 2b$, for $i = 1, 2, 3$, $v_i \cdot v_j = \alpha\beta + \beta\gamma + \gamma\alpha = b$ for $i, j = 1, 2, 3$, with $i \neq j$, and therefore, the result follows. □

Now, from Lemma 3, we are able to formulate statements about the well-roundedness of Λ_f.

Theorem 4. *Let $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, with $a \neq 0$. If $\alpha, \beta, \gamma \in \mathbb{R}$ are the real distinct roots of $f(x)$, then the lattice Λ_f generated by the basis $\{(\alpha, \beta, \gamma), (\gamma, \alpha, \beta), (\beta, \gamma, \alpha)\}$ is well-rounded if and only if $a^2 \geq 4b$ (with $b \geq 0$) or $a^2 \geq -b$ (with $b < 0$). Moreover, Λ_f has the highest packing density for dimension 3 if and only if $a^2 = 4b$.*

Proof. Define $g : \mathbb{Z}^3 \to \mathbb{R}_+$ by $g(v) = g(x_1, x_2, x_3) = (a^2 - 2b)(x_1^2 + x_2^2 + x_3^2) + 2b(x_1x_2 + x_1x_3 + x_2x_3)$, i.e., $\|v\|^2 = g(x_1, x_2, x_3)$. In order to identify when $g(x_1, x_2, x_3)$ assumes minimum value, it is enough to check its value when x_1, x_2 and x_3 vary between 0, 1 and -1. Thus,

(i) $g(\pm1, 0, 0) = g(0, \pm1, 0) = g(0, 0, \pm1) = a^2 - 2b$;

(ii) $g(1, 1, 0) = g(-1, -1, 0) = g(1, 0, 1) = g(-1, 0, -1) = g(0, 1, 1) = g(0, -1, -1) = 2a^2 - 2b$;

(iii) $g(1, -1, 0) = g(-1, 1, 0) = g(1, 0, -1) = g(-1, 0, 1) = g(0, 1, -1) = g(0, -1, 1) = 2a^2 - 6b$;

(iv) $g(1, 1, 1) = g(-1, -1, -1) = 3a^2$;

(v) $g(1, \pm1, -1) = g(1, -1, 1) = g(-1, \pm1, 1) = g(-1, 1, -1) = 3a^2 - 8b$.

Let us denote $m = \min\{a^2 - 2b, 2a^2 - 2b, 2a^2 - 6b, 3a^2, 3a^2 - 8b\}$. Note that if

$$a^2 - 2b = m, \tag{1}$$

then Λ_f is well-rounded, since the vectors $v \in \Lambda_f$ such that $\|v\|^2 = a^2 - 2b$ are linearly independent. Conversely, let us show that (1) is also a necessary condition for Λ_f to be well-rounded. First, note that $3a^2 - 8b = (a^2 - 2b) + (2a^2 - 6b) > m$ and $2a^2 - 2b = a^2 + (a^2 - 2b) > m$. Thus,

$$3a^2 - 8b,\ 2a^2 - 2b \neq m. \tag{2}$$

Suppose that Λ_f is well-rounded and (1) does not hold true, that is,

$$a^2 - 2b \neq m. \tag{3}$$

Clearly, $b \neq 0$ since $a^2 - 2b = m$ otherwise. If $b > 0$, then $2a^2 - 6b < 3a^2$. From (2) and (3), it follows that $2a^2 - 6b = m$. Since the vectors $v \in \Lambda_f$ such that $\|v\|^2 = 2a^2 - 6b$ are linearly dependent, it follows that the set $S(\Lambda_f)$ does not span $\mathbb{R}^3$, which is a contradiction. If $b < 0$, then $m < 2a^2 - 2b < 2a^2 - 6b$. Again, from (2) and (3), it follows that $m = 3a^2$ and thus the set $S(\Lambda_f)$ does not span $\mathbb{R}^3$, which is a contradiction. Therefore, Λ_f is well-rounded if and only if $a^2 - 2b = m$. When $b \geq 0$ (respectively, $b < 0$) the last equality is satisfied if and only if $a^2 - 2b \leq 2a^2 - 6b$ (respectively, $a^2 - 2b \leq 3a^2$), that is, if and only if $a^2 \geq 4b$ ($a^2 \geq -b$). When $a^2 = -b$ or $a^2 = 4b$, it follows that $|S(\Lambda_f)|$ increases. This means that Λ_f has higher center density when these equalities are satisfied. Note that if $a^2 = -b$, where $b < 0$, then $\delta(\Lambda_f) = \frac{(\sqrt{3(-b)}/2)^3}{a(4b)} = \frac{3\sqrt{3}}{32} \approx 0.16238$. On the other hand, if $a^2 = 4b$, then $\delta(\Lambda_f) = \frac{(\sqrt{4b}/2)^3}{|ab|} = \frac{1}{4\sqrt{2}} \approx 0.17679$ corresponding to the highest center density in dimension 3. □

4. Well-rounded lattices via quartic polynomials

We consider here a monic polynomial of degree 4 with integer coefficients and real roots. The vectors are obtained from the rotational shift operator on $\mathbb{R}^4$. We will restrict our investigation to polynomials with two roots being opposite to each other. The reason behind this particular restriction will be detailed in the proposition that comes next.

Proposition 5. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots $\alpha, \beta, \gamma, \psi$ such that $\alpha = -\gamma$. Under these conditions, the vectors $(\alpha, \beta, \gamma, \psi)$, $(\psi, \alpha, \beta, \gamma)$, $(\gamma, \psi, \alpha, \beta)$ and $(\beta, \gamma, \psi, \alpha)$ are linearly independent.*

Proof. Since $\alpha = -\gamma$, it follows that $2\gamma = \gamma - \alpha$. Moreover, by Vieta's formulas, it follows that $\beta + \psi = -a$, $-\gamma^2 + \beta\psi = b$, $-\beta\gamma^2 - \gamma^2\psi = -c$ and $-\beta\gamma^2\psi = d$. Consider the matrix M whose rows are the vectors above, that is,

$$M = \begin{pmatrix} -\gamma & \beta & \gamma & \psi \\ \psi & -\gamma & \beta & \gamma \\ \gamma & \psi & -\gamma & \beta \\ \beta & \gamma & \psi & -\gamma \end{pmatrix}.$$

Note that

$$\begin{aligned} det(M) &= (-\beta^4 - \psi^4) + 2\beta^2\psi^2 - 4\beta^2\gamma^2 - 4\gamma^2\psi^2 - 8\beta\gamma^2\psi \\ &= -(\beta + \psi)^2(4\gamma^2 + (\beta - \psi)^2) \\ &= -a^2(4\gamma^2 + (\beta - \psi)^2) \\ &= -a^2((\gamma - \alpha)^2 + (\beta - \psi)^2) \\ &= -a^2(4\gamma^2 + a^2 - 4\beta\psi) \\ &= -a^2(-4b + a^2). \end{aligned}$$

Suppose that $det(M)$=0. Since $a \neq 0$, it follows that $-4b + a^2 = 0$. By Vieta's formulas, the last equality implies that $4(\gamma^2 - \beta\psi) + (\beta + \psi)^2 = 0$, i.e., $(\beta - \psi)^2 = -4\gamma^2$, which is a contradiction. Thus, $det(M) = -a^2(-4b + a^2) \neq 0$, and therefore, the result follows. □

According to Proposition 5, we can consider a lattice in $\mathbb{R}^4$ generated by the linearly independent vectors $v_1 = (\alpha, \beta, \gamma, \psi)$, $v_2 = (\beta, \gamma, \psi, \alpha)$, $v_3 = (\gamma, \psi, \alpha, \beta)$ and $v_4 = (\psi, \alpha, \beta, \gamma)$ over $\mathbb{R}$, where $\alpha, \beta, \gamma, \psi$ are the roots of $x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$, with $a \neq 0$, such that $\alpha = -\gamma$. We will denote such lattice by Λ_f, as usual.

Remark 6. Note that the hypothesis $\alpha = -\gamma$ is essential to determining $det(M)$ in terms of the coefficients of $f(x)$. The same remark can be done about the calculation of norm of a vector in Λ_f, as we see next.

Lemma 7. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots $\alpha, \beta, \gamma, \psi$ such that $\alpha = -\gamma$ and Λ_f be a lattice generated by $\{v_1, v_2, v_3, v_4\}$, where $v_1 = (\alpha, \beta, \gamma, \psi)$, $v_2 = (\beta, \gamma, \psi, \alpha)$, $v_3 = (\gamma, \psi, \alpha, \beta)$ and $v_4 = (\psi, \alpha, \beta, \gamma)$. If $v = x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4$ is a point of Λ_f, where $x_1, x_2, x_3, x_4 \in \mathbb{Z}$, then $\|v\|^2 = (a^2 - 2b)(x_1^2 + x_2^2 + x_3^2 + x_4^2) + 4b(x_1x_3 + x_2x_4)$.*

Proof. It is easy to see that $\|v\|^2 = (x_1\alpha + x_2\beta + z_3\gamma + z_4\psi)^2 + (x_1\beta + x_2\gamma + z_3\psi + z_4\alpha)^2 + (x_1\gamma + x_2\psi + z_3\alpha + z_4\beta)^2 + (x_1\psi + x_2\alpha + z_3\beta + z_4\gamma)^2$. Rearranging, it follows that

$$\begin{aligned}\|v\|^2 &= (\alpha^2+\beta^2+\gamma^2+\psi^2)(x_1^2+x_2^2+x_3^2+x_4^2) + 2(\alpha\beta+\alpha\psi+\\ &\quad \beta\gamma+\gamma\psi)(x_1x_2+x_1x_4+x_3x_4+x_2x_3) + 4(\alpha\gamma+\beta\psi)(x_1\\ &\quad x_3+x_2x_4). \end{aligned} \tag{4}$$

Since $\alpha = -\gamma$, by Vieta's formulas, it follows that $\alpha\beta + \alpha\psi + \beta\gamma + \gamma\psi = 0$ and $\alpha\gamma + \beta\psi = b$. Moreover, $\alpha^2 + \beta^2 + \gamma^2 + \psi^2 = 2\gamma^2 + \beta^2 + \psi^2 = 2\gamma^2 - 2\beta\psi + (\beta+\psi)^2 = -2b + a^2$. Consequently, the Equation (4) implies $\|v\|^2 = (a^2-2b)(x_1^2+x_2^2+x_3^2+x_4^2) + 4b(x_1x_3+x_2x_4)$. □

We are interested in verifying in which conditions Λ_f is well-rounded. To do this, define $g : \mathbb{Z}^4 \to \mathbb{R}_+$ by $g(x_1,x_2,x_3,x_4) = (a^2-2b)(x_1^2+x_2^2+x_3^2+x_4^2) + 4b(x_1x_3+x_2x_4)$, i.e., $g(x_1,x_2,x_3,x_4) = \|v\|^2$. In order to identify when $g(x_1,x_2,x_3,x_4)$ assumes minimum value, it is enough to check its values when x_i varies between 0, 1 and -1, for $i \in \{1,2,3,4\}$. In particular,

(i) $g(\pm1,0,0,0) = g(0,\pm1,0,0) = g(0,0,\pm1,0) = g(0,0,0,\pm1) = a^2-2b$;

(ii) $g(1,0,1,0) = g(-1,0,-1,0) = g(0,1,0,1) = g(0,-1,0,-1) = 2a^2$;

(iii) $g(1,0,-1,0) = g(-1,0,1,0) = g(0,1,0,-1) = g(0,-1,0,1) = 2a^2-8b$.

Set $A = a^2-2b$, $B = 2a^2$ and $C = 2a^2-8b$. The remaining possibilities for $g(x_1,x_2,x_3,x_4)$, with x_i varying between 0,1 and -1 for all $i \in \{1,2,3,4\}$, are all greater than A, B or C, as we can see:

(iv) $g(1,\pm1,-1,0) = g(1,0,-1,\pm1) = g(0,1,\pm1,-1) = g(0,-1,\pm1,1) = g(\pm1,1,0,-1) = g(\pm1,-1,0,1) = g(-1,\pm1,1,0) = g(-1,0,1,\pm1) = 3a^2-10b = A+C > A$;

(v) $g(\pm1,1,0,0) = g(\pm1,-1,0,0) = g(0,0,1,\pm1) = g(0,0,-1,\pm1) = g(1,0,0,\pm1) = g(-1,0,0,\pm1) = g(0,1,\pm1,0) = g(0,\pm1,-,1,0) = 2(a^2-2b) = 2A > A$;

(vi) $g(1,\pm1,1,0) = g(-1,\pm1,-1,0) = g(\pm1,1,0,1) = g(\pm1,-1,0,-1) = g(1,0,1,\pm1) = g(0,1,\pm1,1) = g(0,-1,\pm1,-1) = g(-1,0,-1,\pm1) = 3a^2-2b = A+B > A$;

(vii) $g(1,1,1,1) = g(-1,-1,-1,-1) = g(1,-1,1,-1) = g(-1,1,-1,1) = 4a^2 = 2B > B$;

(viii) $g(1,1,-1,-1) = g(1,-1,-1,1) = g(-1,1,1,-1) = g(-1,-1,1,1) = 2C > C$;

(ix) $g(1,1,1,-1) = g(-1,1,-1,-1) = g(1,-1,1,1) = g(-1,-1,-1,1) = g(1,1,-1,1) = g(1,-1,-1,-1) = g(-1,1,1,1) = g(-1,-1,1,-1) = 4A > A$.

According to the analysis done above, $|\Lambda_f| = A, B$ or C, i.e., $|\Lambda_f| = a^2 - 2b, 2a^2$ or $2a^2 - 8b$. Let $m = \min\{a^2-2b, 2a^2, 2a^2-8b\}$. Note that if $a^2-2b = m$, then Λ_f is well-rounded, since the vectors $v \in \Lambda_f$ such that $\|v\|^2 = a^2 - 2b$ are linearly independent. Let us show that $a^2-2b = m$ is also a necessary condition for Λ_f to be well-rounded. The proof is similar to that of the Theorem 4. Suppose that Λ_f is well-rounded and $a^2 - 2b \neq m$. Clearly $b \neq 0$. When $b > 0$, it follows that $2a^2 - 8b < 2a^2$. By our assumption, $2a^2 - 8b < a^2 - 2b$ and then we conclude that $2a^2 - 8b = m$. Since the vectors $v \in \Lambda_f$ such that $\|v\|^2 = 2a^2 - 8b$ are linearly dependent, it follows that $S(\Lambda_f)$ does not span $\mathbb{R}^4$. On the other hand, when $b < 0$, it follows that $2a^2 < 2a^2 - 8b$. By our assumption, $2a^2 < a^2 - 2b$ and then we conclude that $m = 2a^2$. Again, it is easy to see that in this case $S(\Lambda_f)$ does not span $\mathbb{R}^4$. Thus, Λ_f is well-rounded if and only if $a^2 - 2b = m$. This means that $a^2 - 2b \leq 2a^2 - 8b$ and $a^2 - 2b \leq 2a^2$. When $b \geq 0$ (respectively, $b < 0$) the last two inequalities are satisfied if and only if $a^2 \geq 6b$ (respectively, $a^2 \geq -2b$). Consequently, we have proved that the following theorem holds true.

Theorem 8. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$, with $a \neq 0$, be a polynomial with real distinct roots $\alpha, \beta, \gamma, \psi$, where $\alpha = -\gamma$. Under these conditions,*

(i) if $b < 0$, then Λ_f is well-rounded if and only if $a^2 \geq -2b$;

(ii) if $b \geq 0$, then Λ_f is well-rounded if and only if $a^2 \geq 6b$.

Remark 9. Although $|S(\Lambda_f)|$ increases when $a^2 = -2b$ or $a^2 = 6b$, these situations do not give us the scenario where Λ_f has the highest packing density in dimension 4, since in both cases Λ_f has 12 minimal vectors, while the ideal situation happens when the number of minimum vectors is 24. This can also be verified by calculating the center density in these cases: if $a^2 = -2b$, then $\delta(\Lambda_f) = \frac{(\sqrt{2a^2})^2}{2^4 3a^4} = \frac{1}{12} \approx 0.083333$. Also, if $a^2 = 6b$, then $\delta(\Lambda_f) = \frac{1}{12}$, while the center density of D_4 is 0.125.

5. Conclusion

In this paper, we have investigated the construction and the well-roundedness of lattices in $\mathbb{R}^n$, $n \leq 4$ via polynomials up to degree 4 with integers coefficients and real roots. The lattices constructed in this work can be useful for applications in coding theory. The difficulty of this type of construction lies in finding linearly independent vectors and to identify the determinant of the generator matrix and the norm of a point in the lattice in terms of the coefficients of the polynomial considered. In dimension 4, the hypothesis $\alpha = -\gamma$ was essential to deal with these issues in our approach. Well-rounded lattices have been recently studied in several scenarios [7, 6], which makes this subject attractive and current.

Acknowledgments

This work has been supported by FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) under Grants 2013/25977-7 and 2018/12702-3.

References

[1] A.A. Andrade and J.C. Interlando, Construction of even-dimensional lattices of full diversity, *International Journal of Applied Mathematics*, **32**, No 2 (2019), 325-332; doi: 10.12732/ijam.v32i2.12.

[2] J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag (1999).

[3] A.L. Flores, J.C. Interlando and T.P. Nóbrega Neto, Optimal families of two and three-dimensional lattice packings from polynomials with integer coefficients, *JP J. of Algebra, Number Theory and Applications*, **15**, No 1 (2009), 45-51.

[4] L. Fukshansky and K. Petersen, On well-rounded ideal lattices, *J. of Number Theory*, **8**, No 1 (2012), 189-206.

[5] L. Fukshansky and X. Sun, On the geometry of cyclic lattices, *Discrete & Computational Geometry*, **52** (2014), 240-259.

[6] O.W. Gnilke, A. Barreal, A. Karrila, H.T.N. Tran, D.A. Karpuk and C. Hollanti, Well-rounded lattices for coset coding in MIMO wiretap channels, In: *Intern. Telecommunication Networks and Applications Conference* (2016), 289-294.

[7] O.W. Gnilke, H.T.N. Tran, A. Karrila and C. Hollanti, Well-rounded lattices for reliability and security in Rayleigh fading SISO channels, In: *IEEE Information Theory Workshop* (2016), 359-363.

[8] D. Micciancio, Generalized compact knapsacks, cyclic lattices and efficient one-way functions from worst-case complexity assumptions, In: *FOCS, IEEE Computer Society* (2002), 356-365.

[9] C.C. Trinca Watanabe, J.-C. Belfiore, E.D. De Carvalho, J. Vieira Filho and R.A. Watanabe, Construction of nested real ideal lattices for interference channel coding, *International Journal of Applied Mathematics*, **32**, No 2 (2019), 295-323; doi: 10.12732/ijam.v32i2.11.