

On the lattice of polynomials with integer coefficients: successive minima in $L_2(0, 1)$

WOJCIECH BANASZCZYK (Łódź)

Abstract. Let $\mathbf{P}_n^{\mathbb{Z}}$ be the additive subgroup of the real Hilbert space $L_2(0, 1)$ consisting of polynomials of order $\leq n$ with integer coefficients. We may treat $\mathbf{P}_n^{\mathbb{Z}}$ as a lattice in $(n + 1)$ -dimensional Euclidean space; let $\lambda_i(\mathbf{P}_n^{\mathbb{Z}})$ ($1 \leq i \leq n + 1$) be the corresponding successive minima. We give rather precise estimates of $\lambda_i(\mathbf{P}_n^{\mathbb{Z}})$ for $i \gtrsim \frac{2}{3}n$.

1. Introduction. Notation and results. Let \mathbf{P}_n be the space of polynomials of degree $\leq n$, with real coefficients, and let $\mathbf{P}_{n,r}$, where $0 \leq r \leq \lfloor n/2 \rfloor$, be the subspace consisting of polynomials divisible by the polynomial $x^r(1 - x)^r$. Let then $\mathbf{P}_n^{\mathbb{Z}}$ (resp. $\mathbf{P}_{n,r}^{\mathbb{Z}}$) be the lattice in \mathbf{P}_n (resp. in $\mathbf{P}_{n,r}$) consisting of polynomials with integer coefficients. In the previous paper [BL] we considered the following question: how well can polynomials in $\mathbf{P}_{n,r}$ be approximated in $L_p(0, 1)$ by elements of $\mathbf{P}_{n,r}^{\mathbb{Z}}$? In other words, what is the covering radius of the lattice $\mathbf{P}_{n,r}^{\mathbb{Z}}$ in the space $L_p(0, 1)$? In [BL] we gave some estimates of the covering radius for $r \lesssim n/6$; especially precise estimates were obtained for $p = 2$.

The present paper is devoted to a deeper analysis of the geometry of the lattice $\mathbf{P}_n^{\mathbb{Z}}$ in the space $L_2(0, 1)$. The main result is Theorem 1.1, which gives fairly precise estimates of the successive minima $\lambda_i(\mathbf{P}_n^{\mathbb{Z}})$ for $i \gtrsim \frac{2}{3}n$. In Section 5 we give some estimates of the successive minima of the dual lattice $(\mathbf{P}_{n,r}^{\mathbb{Z}})^*$ and derive some transference theorems.

Notation. We use the notation introduced in [BL]. For the reader's convenience we recall it below.

Let X be a real normed space. By a *lattice* in X we mean a non-zero finite-dimensional discrete additive subgroup of X . Every lattice L in X can

2020 *Mathematics Subject Classification*: Primary 41A10; Secondary 52C07.

Key words and phrases: polynomials with integer coefficients, lattice, covering radius, successive minima.

Received 13 April 2019.

Published online *.

be represented in the form

$$L = \{k_1x_1 + \cdots + k_nx_n : k_1, \dots, k_n \in \mathbb{Z}\},$$

where $n = \dim \text{span } L$ and x_1, \dots, x_n is a system of linearly independent vectors; any such system is called a *basis* of L .

Let L be a lattice in X . We denote by $\mu(L)$ the *covering radius* of L :

$$\mu(L) := \max\{d(x, L) : x \in \text{span } L\},$$

where $d(x, L)$ is the distance from x to L .

Let $n = \dim \text{span } L$. We denote by $\lambda_i(L)$ the *successive minima* of L :

$$\lambda_i(L) := \min\{t > 0 : \dim \text{span}(L \cap t\overline{B}) \geq i\}, \quad i = 1, \dots, n.$$

Here \overline{B} is the closed unit ball in X . By definition, $\lambda_1(L)$ is the length of the shortest non-zero vector in L .

In the present paper X will be the real Hilbert space $L_2(0, 1)$ or one of its subspaces.

We denote by \mathbf{P} the space of polynomials with real coefficients. We treat \mathbf{P} as a subspace of $L_2(0, 1)$, i.e. as an inner-product space with the usual norm

$$\|P\| = \left(\int_0^1 P(x)^2 dx \right)^{1/2}$$

and the usual inner product

$$(P | Q) = \int_0^1 P(x)Q(x) dx.$$

Let $P \in \mathbf{P}$ and let M be a finite-dimensional subspace of \mathbf{P} . The distance from P to M is denoted by $d(P, M)$. The orthogonal projection of P onto M will be denoted by $\pi(P; M)$.

Let $\Phi: \mathbf{P} \rightarrow \mathbf{P}$ be the operator given by

$$\Phi(P)(x) = P(1 - x), \quad P \in \mathbf{P}, x \in [0, 1].$$

Obviously, Φ is a linear isometry and $\Phi^{-1} = \Phi$. We denote

$$\mathbf{E} := \{P \in \mathbf{P} : \Phi(P) = P\}, \quad \mathbf{F} := \{P \in \mathbf{P} : \Phi(P) = -P\}.$$

It is clear that \mathbf{P} is the orthogonal direct sum $\mathbf{E} \oplus \mathbf{F}$.

Throughout the paper, m, n, r are non-negative integers.

Let $r \geq 0$. We denote by U_r, V_r, S_r and T_r the polynomials given by

$$\begin{aligned} U_r(x) &= x^r(1-x)^r, & V_r(x) &= (2x-1)x^r(1-x)^r, \\ S_r(x) &= x^{r+1}(1-x)^r, & T_r(x) &= x^r(1-x)^{r+1}. \end{aligned}$$

Note that $U_r \in \mathbf{E}$ and $V_r \in \mathbf{F}$. By definition we have

$$(1.1) \quad S_r = \frac{U_r + V_r}{2}, \quad T_r = \frac{U_r - V_r}{2}.$$

Observe that $\Phi(S_r) = T_r$.

We denote by \mathbf{P}_n ($n \geq 0$) the subspace of \mathbf{P} consisting of polynomials of degree $\leq n$.

Let $m \geq 0$. We denote $\mathbf{E}_m := \mathbf{P}_{2m} \cap \mathbf{E}$ and $\mathbf{F}_m := \mathbf{P}_{2m+1} \cap \mathbf{F}$. It is clear that $\mathbf{E}_m = \text{span}\{U_0, U_1, \dots, U_m\}$ and $\mathbf{F}_m = \text{span}\{V_0, V_1, \dots, V_m\}$. Observe that $\mathbf{P}_{2m+1} = \mathbf{E}_m \oplus \mathbf{F}_m$ and $\mathbf{P}_{2m} = \mathbf{E}_m \oplus \mathbf{F}_{m-1}$ (orthogonal direct sums). Here $\mathbf{F}_{-1} := \{0\}$.

Let $r \geq 0$. We denote by \mathbf{M}_r the subspace of \mathbf{P} consisting of polynomials divisible by the polynomial $U_r(x) = x^r(1-x)^r$. Thus $\mathbf{M}_0 := \mathbf{P}$,

$$\mathbf{M}_1 := \{P \in \mathbf{P} : P(0) = P(1) = 0\}$$

and, for $r \geq 2$,

$$\mathbf{M}_r := \{P \in \mathbf{P} : P^{(k)}(0) = P^{(k)}(1) = 0 \text{ for } k = 0, 1, \dots, r-1\}.$$

It is clear that $\Phi(\mathbf{M}_r) = \mathbf{M}_r$.

Let $m, r \geq 0$. We denote $\mathbf{E}_{m,r} := \mathbf{E}_m \cap \mathbf{M}_r$ and $\mathbf{F}_{m,r} := \mathbf{F}_m \cap \mathbf{M}_r$. Observe that

$$(1.2) \quad \mathbf{E}_{m,r} = \text{span}\{U_r, \dots, U_m\}, \quad \mathbf{F}_{m,r} = \text{span}\{V_r, \dots, V_m\}$$

if $0 \leq r \leq m$, and $\mathbf{E}_{m,r} = \mathbf{F}_{m,r} = \{0\}$ if $m < r$.

Let $n, r \geq 0$. We denote $\mathbf{P}_{n,r} := \mathbf{P}_n \cap \mathbf{M}_r$. Thus

$$\begin{aligned} \mathbf{P}_{2m+1,r} &= \text{span}\{U_r, V_r, \dots, U_m, V_m\}, & 0 \leq r \leq m, \\ \mathbf{P}_{2m,r} &= \text{span}\{U_r, V_r, \dots, U_{m-1}, V_{m-1}, U_m\}, & 0 \leq r \leq m-1, \end{aligned}$$

$\mathbf{P}_{2m,m} = \text{span}\{U_m\}$ for $m \geq 0$ and $\mathbf{P}_{n,r} = \{0\}$ if $n < 2r$.

If \mathbf{N} is a linear subspace of \mathbf{P} , then we denote by $\mathbf{N}^{\mathbb{Z}}$ the additive subgroup of \mathbf{N} consisting of polynomials with integer coefficients. Clearly, $\Phi(\mathbf{P}^{\mathbb{Z}}) = \mathbf{P}^{\mathbb{Z}}$.

Let $0 \leq r \leq m$. It is not hard to see that U_r, \dots, U_m is a basis of the lattice $\mathbf{E}_{m,r}^{\mathbb{Z}}$. Similarly, V_r, \dots, V_m is a basis of $\mathbf{F}_{m,r}^{\mathbb{Z}}$. Next, $S_r, T_r, \dots, S_m, T_m$ is a basis of $\mathbf{P}_{2m+1,r}^{\mathbb{Z}}$, and $S_r, T_r, \dots, S_{m-1}, T_{m-1}, U_m$ is a basis of $\mathbf{P}_{2m,r}^{\mathbb{Z}}$ (the 1-dimensional lattice $\mathbf{P}_{2m,m}^{\mathbb{Z}} = \mathbf{E}_{m,m}^{\mathbb{Z}}$ is generated by U_m). Observe that

$$\begin{aligned} \mathbf{E}_{m,r}^{\mathbb{Z}} + \mathbf{F}_{m,r}^{\mathbb{Z}} &\subsetneq \mathbf{P}_{2m+1,r}^{\mathbb{Z}} \subsetneq \frac{1}{2}(\mathbf{E}_{m,r}^{\mathbb{Z}} + \mathbf{F}_{m,r}^{\mathbb{Z}}), & 0 \leq r \leq m, \\ \mathbf{E}_{m,r}^{\mathbb{Z}} + \mathbf{F}_{m-1,r}^{\mathbb{Z}} &\subsetneq \mathbf{P}_{2m,r}^{\mathbb{Z}} \subsetneq \frac{1}{2}(\mathbf{E}_{m,r}^{\mathbb{Z}} + \mathbf{F}_{m-1,r}^{\mathbb{Z}}), & 0 \leq r \leq m-1. \end{aligned}$$

The above bases are not especially useful because the norms of the corresponding coordinate projections can be large (the elements of these bases are far from being orthogonal). To obtain bases with better properties we apply a procedure which might be called *lattice orthogonalization*.

Let $0 \leq r \leq m$. We denote

$$(1.3) \quad U_{m,r} := U_r - \pi(U_r; \mathbf{E}_{m,r+1}), \quad V_{m,r} := V_r - \pi(V_r; \mathbf{F}_{m,r+1}).$$

We have $\mathbf{E}_{m,m+1} = \mathbf{F}_{m,m+1} = \{0\}$, so that $U_{m,m} = U_m$ and $V_{m,m} = V_m$. By definition, $U_{m,r}$ (resp. $V_{m,r}$) is the shortest vector in the hyperplane

$\mathbf{E}_{m,r+1} + U_r$ (resp. in $\mathbf{F}_{m,r+1} + V_r$), so that

$$(1.4) \quad d(U_r, \mathbf{E}_{m,r+1}) = \|U_{m,r}\|, \quad d(V_r, \mathbf{F}_{m,r+1}) = \|V_{m,r}\|.$$

The sequence $U_{m,m}, U_{m,m-1}, \dots, U_{m,r}$ is just the orthogonalization of the sequence U_m, U_{m-1}, \dots, U_r . Similarly, $V_{m,m}, V_{m,m-1}, \dots, V_r$ is the orthogonalization of V_m, V_{m-1}, \dots, V_r .

Let $r \geq 0$ and $n \geq 2r + 1$. We denote

$$(1.5) \quad S_{n,r} := S_r - \pi(S_r; \mathbf{P}_{n,r+1}), \quad T_{n,r} := T_r - \pi(T_r; \mathbf{P}_{n,r+1}).$$

Then $S_{n,r}$ (resp. $T_{n,r}$) is the shortest vector in the hyperplane $\mathbf{P}_{n,r+1} + S_r$ (resp. $\mathbf{P}_{n,r+1} + T_r$). Naturally, $S_{n,r}$ and $T_{n,r}$ are both orthogonal to $\mathbf{P}_{n,r+1}$. Since $\Phi(S_r) = T_r$ and $\Phi(\mathbf{P}_{n,r+1}) = \mathbf{P}_{n,r+1}$, it follows that $\Phi(S_{n,r}) = T_{n,r}$ and

$$(1.6) \quad d(S_r, \mathbf{P}_{n,r+1}) = d(T_r, \mathbf{P}_{n,r+1}) = \|S_{n,r}\| = \|T_{n,r}\|.$$

The polynomials $S_{n,r}$ and $T_{n,r}$ are not orthogonal (see Lemma 2.4). The angle between them will be denoted by $\varphi_{n,r}$.

Let $\tilde{S}_{n,r}$ (resp. $\tilde{T}_{n,r}$) denote the shortest vector in the set $\mathbf{P}_{n,r+1}^{\mathbb{Z}} + S_r$ (resp. $\mathbf{P}_{n,r+1}^{\mathbb{Z}} + T_r$). If there are two or more such vectors, we fix any of them. Since $\Phi(\mathbf{P}_{n,r+1}^{\mathbb{Z}}) = \mathbf{P}_{n,r+1}^{\mathbb{Z}}$ and $\Phi(S_r) = T_r$, we may assume that $\Phi(\tilde{S}_{n,r}) = \tilde{T}_{n,r}$. It is clear that $\tilde{S}_{2m+1,r}, \tilde{T}_{2m+1,r}, \dots, \tilde{S}_{2m+1,m}, \tilde{S}_{2m+1,m}$ is a basis of the lattice $\mathbf{P}_{2m+1,r}^{\mathbb{Z}}$. Similarly, $\tilde{S}_{2m,r}, \tilde{T}_{2m,r}, \dots, \tilde{S}_{2m,m-1}, \tilde{T}_{2m,m-1}, U_m$ is a basis of $\mathbf{P}_{2m,r}^{\mathbb{Z}}$.

Finally, we denote

$$(1.7) \quad C_r := \sqrt{2(2r)!(2r+1)!}, \quad r \geq 0,$$

$$(1.8) \quad a_{m,r} := C_r^2 \frac{(2m-2r)!}{(2m+2r+2)!}, \quad 0 \leq r \leq m,$$

$$(1.9) \quad b_{m,r} := C_r^2 \frac{(2m-2r+1)!}{(2m+2r+3)!}, \quad 0 \leq r \leq m,$$

$$(1.10) \quad c_{n,r} := C_r^2 \frac{(n-2r-1)!}{(n+2r+2)!} \cdot \frac{n+1}{2}, \quad r \geq 0, n \geq 2r+1.$$

Thus

$$(1.11) \quad c_{n,r} = \frac{a_{m,r} + b_{m-1,r}}{4}, \quad n = 2m, 0 \leq r \leq m-1,$$

$$(1.12) \quad c_{n,r} = \frac{a_{m,r} + b_{m,r}}{4}, \quad n = 2m+1, 0 \leq r \leq m.$$

The results. To simplify the formulas we denote

$$\chi_{n,k} := \left[\frac{(2k/n)^2}{1 - (2k/n)^2} \right]^2, \quad 2k < n.$$

THEOREM 1.1. Let $0 \leq r \leq n/6 - 2$ and $0 \leq s \leq r$. Then

$$c_{n,r}^{1/2} \leq \lambda_{n-2r}(\mathbf{P}_{n,s}^{\mathbb{Z}}) = \lambda_{n-2r+1}(\mathbf{P}_{n,s}^{\mathbb{Z}}) < [1 + 0.26\chi_{n,r+1}]c_{n,r}^{1/2} < 1.0041c_{n,r}^{1/2}.$$

As a by-product we obtain the following estimate of $\mu(\mathbf{P}_{n,r}^{\mathbb{Z}})$:

THEOREM 1.2. Let $0 \leq r \leq n/6 - 2$. Then

$$\frac{c_{n,r}^{1/2}}{\kappa_{n,r}} \leq \mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) < [1 + 1.026\chi_{n,r+1}] \frac{c_{n,r}^{1/2}}{\kappa_{n,r}} < 1.0161 \frac{c_{n,r}^{1/2}}{\kappa_{n,r}},$$

where

$$\kappa_{n,r} := 2^{1/2} \left(1 + \frac{2r+1}{n+1} \right)^{1/2}.$$

Theorem 1.2 is a slight improvement of [BL, Theorem 1.1].

It follows directly from Theorem 1.2 and (1.10) that, for a fixed $r \geq 0$,

$$\mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) = \frac{C_r}{2n^{2r+1}}(1 + O(n^{-1})) \quad \text{as } n \rightarrow \infty.$$

This, in turn, is a slight improvement of [BL, Theorem 1.2].

2. Minimal polynomials

LEMMA 2.1.

(a) Let $n = 2m$ and $0 \leq r \leq m - 1$. Then

$$S_{n,r} = \frac{U_{m,r} + V_{m-1,r}}{2}, \quad T_{n,r} = \frac{U_{m,r} - V_{m-1,r}}{2}.$$

(b) Let $n = 2m + 1$ and $0 \leq r \leq m$. Then

$$S_{n,r} = \frac{U_{m,r} + V_{m,r}}{2}, \quad T_{n,r} = \frac{U_{m,r} - V_{m,r}}{2}.$$

Proof. (a) We have $\mathbf{P}_{n,r+1} = \mathbf{E}_{m,r+1} \oplus \mathbf{F}_{m-1,r+1}$ (the orthogonal direct sum), $U_r \perp \mathbf{F}$ and $V_r \perp \mathbf{E}$. So, $\pi(U_r; \mathbf{P}_{n,r+1}) = \pi(U_r; \mathbf{E}_{m,r+1})$ and $\pi(V_r; \mathbf{P}_{n,r+1}) = \pi(V_r; \mathbf{F}_{m-1,r+1})$. Hence

$$\begin{aligned} S_{n,r} &\stackrel{(1.5)}{=} S_r - \pi(S_r; \mathbf{P}_{n,r+1}) \stackrel{(1.1)}{=} \frac{U_r + V_r}{2} - \pi\left(\frac{U_r + V_r}{2}; \mathbf{P}_{n,r+1}\right) \\ &= \frac{U_r - \pi(U_r; \mathbf{P}_{n,r+1})}{2} + \frac{V_r - \pi(V_r; \mathbf{P}_{n,r+1})}{2} \\ &= \frac{U_r - \pi(U_r; \mathbf{E}_{m,r+1})}{2} + \frac{V_r - \pi(V_r; \mathbf{F}_{m-1,r+1})}{2} \stackrel{(1.3)}{=} \frac{U_{m,r} + V_{m-1,r}}{2} \end{aligned}$$

(to get $V_r - \pi(V_r; \mathbf{F}_{m-1,r+1}) = V_{m-1,r}$ we replace m by $m - 1$ in (1.3)). The proof of the second equality in (a) is analogous.

The proof of (b) is similar; in this case $\mathbf{P}_{n,r+1} = \mathbf{E}_{m,r+1} \oplus \mathbf{F}_{m,r+1}$. ■

LEMMA 2.2. Let $m \geq 0$. Then $\|U_m\| = a_{m,m}^{1/2}$, $\|V_m\| = b_{m,m}^{1/2}$ and

$$d(U_r, \mathbf{E}_{m,r+1}) = a_{m,r}^{1/2}, \quad d(V_r, \mathbf{F}_{m,r+1}) = b_{m,r}^{1/2}, \quad 0 \leq r \leq m-1.$$

These are [BL, Lemmas 2.2 and 2.4].

LEMMA 2.3. Let $r \geq 0$ and $n \geq 2r+1$. Then

$$d(S_r, \mathbf{P}_{n,r+1}) = d(T_r, \mathbf{P}_{n,r+1}) = c_{n,r}^{1/2}.$$

Proof. We give the proof for n even; the proof for n odd is similar. So, let $n = 2m$ and $0 \leq r \leq m-1$. Then $d(S_r, \mathbf{P}_{n,r+1}) \stackrel{(1.6)}{=} d(T_r, \mathbf{P}_{n,r+1})$ and

$$\begin{aligned} d(S_r, \mathbf{P}_{n,r+1})^2 &\stackrel{(1.6)}{=} \|S_{n,r}\|^2 = \left\| \frac{U_{m,r} + V_{m-1,r}}{2} \right\|^2 \\ &= \frac{\|U_{m,r}\|^2 + \|V_{m-1,r}\|^2}{4} = \frac{a_{m,r} + b_{m-1,r}}{4} \stackrel{(1.11)}{=} c_{n,r}. \end{aligned}$$

The second equality follows from Lemma 2.1(a). The fourth one follows from (1.4) and Lemma 2.2. ■

LEMMA 2.4. Let $r \geq 0$ and $n \geq 2r+1$. Then

$$\cos \varphi_{n,r} = (-1)^{n+1} \cdot \frac{2r+1}{n+1}.$$

Consequently, if $n \geq 6r+2$, then $|\cos \varphi_{n,r}| \leq 1/3$.

Proof. We give the proof for n even; for n odd the proof is analogous. Let $n = 2m$ and $0 \leq r \leq m-1$. By definition, $\varphi_{n,r}$ is the angle between $S_{n,r}$ and $T_{n,r}$, so that

$$\cos \varphi_{n,r} = \frac{(S_{n,r} | T_{n,r})}{\|S_{n,r}\| \cdot \|T_{n,r}\|}.$$

From (1.6) and Lemma 2.3 it follows that $\|S_{n,r}\| \cdot \|T_{n,r}\| = c_{n,r}$. Lemma 2.1(a) yields

$$(S_{n,r} | T_{n,r}) = \left(\frac{U_{m,r} + V_{m-1,r}}{2} \left| \frac{U_{m,r} - V_{m-1,r}}{2} \right. \right) = \frac{\|U_{m,r}\|^2 - \|V_{m-1,r}\|^2}{4}.$$

From (1.4) and Lemma 2.2 it follows that $\|U_{m,r}\|^2 = a_{m,r}$ and $\|V_{m-1,r}\|^2 = b_{m-1,r}$. Consequently, we may write

$$\cos \varphi_{n,r} = \frac{a_{m,r} - b_{m-1,r}}{4c_{n,r}}.$$

Finally, from (1.8)–(1.10) after direct calculations we obtain

$$\frac{a_{m,r} - b_{m-1,r}}{4c_{n,r}} = -\frac{2r+1}{n+1}. \quad \blacksquare$$

Let us denote

$$\gamma_{n,r} := c_{n,r}^{-1} \left(\frac{1}{2} a_{m,m} + \sum_{k=r+1}^{m-1} c_{n,k} \right), \quad n = 2m, 0 \leq r \leq m-2,$$

$$\gamma_{n,r} := c_{n,r}^{-1} \sum_{k=r+1}^m c_{n,k}, \quad n = 2m+1, 0 \leq r \leq m-1.$$

LEMMA 2.5. *Let $r \geq 0$ and $n \geq 6r + 6$. Then $\gamma_{n,r} < 0.026$.*

The proof is similar to the proofs of [BL, Lemmas 2.11 and 2.13].

LEMMA 2.6. *Let $r \geq 0$ and $n \geq 6r + 12$. Then $\gamma_{n,r} < 1.026\chi_{n,r+1}$.*

The proof is similar to the proofs of [BL, Lemmas 2.12 and 2.14].

We will denote by P_0, P_1, P_2, \dots the Legendre polynomials on $[0, 1]$:

$$P_n(x) = \frac{1}{n!} \frac{d^n (x^n (x-1)^n)}{dx^n}.$$

The polynomials P_n can be defined by

$$P_n(x) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} \binom{n+k}{k} x^k.$$

Hence

$$(2.1) \quad P'_n(x) = \sum_{k=0}^{n-1} (-1)^{n-k+1} (k+1) \binom{n}{k+1} \binom{n+k+1}{k+1} x^k.$$

LEMMA 2.7. *Let $m \geq 0$. Then*

$$(2.2) \quad U_{m,0} = \frac{P'_{2m+1}}{(2m+1)(2m+2)},$$

$$(2.3) \quad V_{m,0} = \frac{P'_{2m+2}}{(2m+2)(2m+3)}.$$

Proof. We will prove (2.2); the proof of (2.3) is analogous. Let

$$Q := \frac{P'_{2m+1}}{(2m+1)(2m+2)}.$$

By definition, $U_0 \equiv 1$ and $U_{m,0}$ is the intersection point of the hyperplane $\mathbf{E}_{m,1} + U_0$ and the subspace $(\mathbf{E}_{m,1})^\perp$. Therefore, we need to prove that (a) $Q \in \mathbf{E}_{m,1} + U_0$ and (b) Q is orthogonal to $\mathbf{E}_{m,1}$.

To prove (a) we have to show that $Q - U_0 \in \mathbf{E}_{m,1} \equiv \mathbf{E}_m \cap \mathbf{M}_1$, i.e. that (c) $Q - U_0 \in \mathbf{E}_m$ and (d) $Q - U_0 \in \mathbf{M}_1$. It is clear that $P_{2m+1} \in \mathbf{P}_{2m+1}$ and $P_{2m+1} \in \mathbf{F}$. Therefore $P'_{2m+1} \in \mathbf{P}_{2m}$ and $P'_{2m+1} \in \mathbf{E}$. So, $Q \in \mathbf{P}_{2m} \cap \mathbf{E} \equiv \mathbf{E}_m$, whence (c) follows.

To prove (d) we have to show that $Q(0) = Q(1) = 1$. Replacing n by $2m + 1$ in (2.1), we obtain

$$(2.4) \quad P'_{2m+1}(x) = \sum_{k=0}^{2m} (-1)^k (k+1) \binom{2m+1}{k+1} \binom{2m+k+2}{k+1} x^k.$$

In particular $P'_{2m+1}(0) = (2m+1)(2m+2)$. Hence $Q(0) = 1$, and consequently $Q(1) = 1$, because $Q \in \mathbf{E}$.

To prove (b), take any $R \in \mathbf{E}_{m,1}$. We have to show that $(Q | R) = 0$, i.e. $(P'_{2m+1} | R) = 0$. Integrating by parts we obtain

$$\int_0^1 P'_{2m+1}(x)R(x) dx = [P_{2m+1}(x)R(x)]_0^1 - \int_0^1 P_{2m+1}(x)R'(x) dx.$$

Since $R \in \mathbf{E}_{m,1} \subset \mathbf{M}_1$, we have $R(0) = R(1) = 0$, so that the first component on the right-hand side vanishes. The second one also vanishes: since $R \in \mathbf{E}_{m,1} \subset \mathbf{P}_{2m}$, we have $R' \in \mathbf{P}_{2m-1}$, and P_{2m+1} is obviously orthogonal to \mathbf{P}_{2m-1} . ■

REMARK 2.8. Lemma 2.7 has the following generalization. Let us denote

$$\sigma_{r,i} = (2r+1)! P_r^{(i-1)}(0) = (-1)^{r-i+1} \frac{(2r+1)!}{(i-1)!} \cdot \frac{(r+i-1)!}{(r-i+1)!}$$

for $r \geq 0$ and $1 \leq i \leq r+1$. It can be shown that

$$U_{m,r} = (2m-2r)! \sum_{i=1}^{r+1} \frac{\sigma_{r,i}}{(2m+2i)!} P_{2m+i}^{(i)},$$

$$V_{m,r} = (2m-2r+1)! \sum_{i=1}^{r+1} \frac{\sigma_{r,i}}{(2m+2i+1)!} P_{2m+i+1}^{(i)}$$

for $m \geq 0$ and $0 \leq r \leq m$.

The derivatives of Legendre polynomials can be represented as linear combinations of Legendre polynomials themselves:

$$P_{2m+i}^{(i)} = 2 \sum_{j=1}^i (-1)^j P_{2m+i}^{(i-j)}(0) \sum_{k=0}^m (4k+1) P_{2k}^{(j-1)}(0) P_{2k},$$

$$P_{2m+i+1}^{(i)} = 2 \sum_{j=1}^i (-1)^j P_{2m+i+1}^{(i-j)}(0) \sum_{k=0}^m (4k+3) P_{2k+1}^{(j-1)}(0) P_{2k+1}$$

for $m \geq 0$ and $i \geq 1$. Consequently, the polynomials $U_{m,r}$ and $V_{m,r}$ can be represented as linear combinations of Legendre polynomials. Thus, in particular,

$$\begin{aligned}
U_{m,0} &= \frac{2}{(2m+1)(2m+2)} \sum_{k=0}^m (4k+1)P_{2k}, \\
V_{m,0} &= \frac{2}{(2m+2)(2m+3)} \sum_{k=0}^m (4k+3)P_{2k+1}, \\
U_{m,1} &= \frac{12(2m)(2m+3)}{(2m-1)\cdots(2m+4)} \sum_{k=0}^m (4k+1)P_{2k} \\
&\quad - \frac{24}{(2m-1)\cdots(2m+4)} \sum_{k=0}^m (2k)(2k+1)(4k+1)P_{2k}, \\
V_{m,1} &= \frac{12(2m+1)(2m+4)}{(2m)\cdots(2m+5)} \sum_{k=0}^m (4k+3)P_{2k+1} \\
&\quad - \frac{24}{(2m)\cdots(2m+5)} \sum_{k=0}^m (2k+1)(2k+2)(4k+3)P_{2k+1}.
\end{aligned}$$

We do not prove these facts because we are not going to use them.

PROPOSITION 2.9. *The polynomials $U_{m,0}$ and $V_{m,0}$ ($m \geq 0$) have integer coefficients.*

Proof. Fix $m \geq 0$. We will prove that $U_{m,0} \in \mathbf{P}^{\mathbb{Z}}$; for $V_{m,0}$ the proof is analogous. Let $U_{m,0}(x) = \sum_{k=0}^{2m} a_k x^k$. We are to prove $a_0, a_1, \dots, a_{2m} \in \mathbb{Z}$. We have $a_0 = U_{m,0}(0) = 1$, therefore it is enough to prove that $a_k - a_{k-1} \in \mathbb{Z}$ for $k = 1, \dots, 2m$.

From (2.2) and (2.4) it follows that

$$\begin{aligned}
a_k &= \frac{(-1)^k(k+1)}{(2m+1)(2m+2)} \binom{2m+1}{k+1} \binom{2m+k+2}{k+1} \\
&= \frac{(-1)^k}{k+1} \binom{2m}{k} \binom{2m+k+2}{k}, \quad k = 0, 1, \dots, 2m.
\end{aligned}$$

So, for each $k = 1, \dots, 2m$ the difference $a_k - a_{k-1}$ is equal to

$$\begin{aligned}
&\frac{(-1)^k}{k+1} \binom{2m}{k} \binom{2m+k+2}{k} - \frac{(-1)^{k-1}}{k} \binom{2m}{k-1} \binom{2m+k+1}{k-1} \\
&= \frac{(-1)^k}{k+1} \binom{2k}{k} \binom{2m+k+1}{2k} = (-1)^k C_k \binom{2m+k+1}{2k},
\end{aligned}$$

where C_k is the k th Catalan number. ■

REMARK 2.10. In a similar way one can show that the polynomials $S_{2m+1,0}$ and $T_{2m+1,0}$ ($m \geq 0$) have integer coefficients. The coefficients of the polynomials $S_{2m,0}$ and $T_{2m,0}$ ($m \geq 1$) need not be integers.

3. Auxiliary lemmas. In this section $m \geq 1$ is a fixed integer and $w, x_1, y_1, \dots, x_m, y_m$ is some fixed sequence of linearly independent vectors in $L_2(0, 1)$. We assume that

$$(3.1) \quad \Phi(w) = w \quad \text{and} \quad \Phi(x_i) = y_i \quad \text{for } i = 1, \dots, m.$$

Let us denote

$$L_0 := \mathbb{Z}w, \quad M_0 := \text{span } L_0 \equiv \mathbb{R}w, \quad h_0 := \|w\|, \quad s_0 := h_0$$

and, for $i = 1, \dots, m$,

$$\begin{aligned} L_i &:= \mathbb{Z}w + \mathbb{Z}x_1 + \mathbb{Z}y_1 + \dots + \mathbb{Z}x_i + \mathbb{Z}y_i, \\ M_i &:= \text{span } L_i \equiv \text{span}\{w, x_1, y_1, \dots, x_i, y_i\}, \\ h_i &:= d(x_i, M_{i-1}), \\ s_i &:= (h_0^2 + 2h_1^2 + \dots + 2h_i^2)^{1/2}. \end{aligned}$$

From (3.1) it follows that

$$(3.2) \quad \Phi(L_i) = L_i, \quad \Phi(M_i) = M_i, \quad i = 0, 1, \dots, m.$$

Hence, for each $i = 1, \dots, m$,

$$d(y_i, M_{i-1}) = d(\Phi(x_i), \Phi(M_{i-1})) = d(x_i, M_{i-1}) = h_i.$$

For $i = 1, \dots, m$ let u_i (resp. v_i) be the shortest vector in the hyperplane $M_{i-1} + x_i$ (resp. in $M_{i-1} + y_i$). If there are two or more such vectors, we fix any of them. Since Φ is an isometry, $\Phi(u_i)$ is the shortest vector in the hyperplane

$$\Phi(M_{i-1} + x_i) = \Phi(M_{i-1}) + \Phi(x_i) \stackrel{(3.2), (3.1)}{=} M_{i-1} + y_i.$$

Therefore $\Phi(u_i) = v_i$. Note that $\|u_i\| = \|v_i\| = h_i$. Let $K_i := \mathbb{Z}u_i + \mathbb{Z}v_i$ and let $K_0 := L_0 = \mathbb{Z}w$.

For $i = 1, \dots, m$ let \tilde{u}_i (resp. \tilde{v}_i) be the shortest vector in the coset $L_{i-1} + x_i$ (resp. in $L_{i-1} + y_i$). Since Φ is an isometry, $\Phi(\tilde{u}_i)$ is the shortest vector in the coset

$$\Phi(L_{i-1} + x_i) = \Phi(L_{i-1}) + \Phi(x_i) \stackrel{(3.2), (3.1)}{=} L_{i-1} + y_i.$$

Therefore we may and will assume that $\Phi(\tilde{u}_i) = \tilde{v}_i$; hence, in particular, $\|\tilde{u}_i\| = \|\tilde{v}_i\|$. Observe that $w, \tilde{u}_1, \tilde{v}_1, \dots, \tilde{u}_i, \tilde{v}_i$ is a basis of the lattice L_i .

For $i = 1, \dots, m$ let $N_i := M_i \ominus M_{i-1}$ be the orthogonal complement of M_{i-1} in M_i . Thus

$$u_i = \pi(x_i; N_i) = \pi(\tilde{u}_i; N_i), \quad v_i = \pi(y_i; N_i) = \pi(\tilde{v}_i; N_i), \quad K_i = \pi(L_i; N_i).$$

For $i = 1, \dots, m$ let ξ_i (resp. $\tilde{\xi}_i$) be the angle between u_i and v_i (resp. between \tilde{u}_i and \tilde{v}_i).

LEMMA 3.1. *Let $0 \leq i \leq m$. Then*

$$(3.3) \quad \mu(K_i) \leq \mu(L_i) \leq \left(\sum_{j=0}^i \mu(K_j)^2 \right)^{1/2}.$$

Proof. For $i=0$ there is nothing to prove because $K_0 = L_0$. Assume $i \geq 1$. The first inequality in (3.3) is obvious: $K_i = \pi(L_i; N_i)$ and the orthogonal projection does not increase distances. We prove the second one by induction on i . It is enough to show that $\mu(L_i)^2 \leq \mu(L_{i-1})^2 + \mu(K_i)^2$ for $i = 1, \dots, m$.

Let $x \in M_i$. We have to show that $d(x, L_i)^2 \leq \mu(L_{i-1})^2 + \mu(K_i)^2$. There is some $y \in K_i$ with

$$(3.4) \quad \|\pi(x; N_i) - y\| \leq \mu(K_i).$$

We have $y = \pi(z; N_i)$ for some $z \in L_i$. Next, there is some $t \in L_{i-1}$ with

$$(3.5) \quad \|\pi(x - z; M_{i-1}) - t\| \leq \mu(L_{i-1}).$$

Then

$$\begin{aligned} d(x, L_i)^2 &\leq \|x - (z + t)\|^2 = \|\pi(x - z - t; M_{i-1})\|^2 + \|\pi(x - z - t; N_i)\|^2 \\ &= \|\pi(x - z; M_{i-1}) - t\|^2 + \|\pi(x; N_i) - y\|^2 \stackrel{(3.5), (3.4)}{\leq} \mu(L_{i-1})^2 + \mu(K_i)^2. \blacksquare \end{aligned}$$

LEMMA 3.2. *Let $u, v \in L_2(0, 1)$ be linearly independent vectors with $\|u\| = \|v\| = h$ and let ξ be the angle between u and v . Let then K be the lattice generated by u and v .*

(a) *One has*

$$\mu(K) = \frac{h}{\sqrt{2(1 + |\cos \xi|)}}.$$

Consequently, $\frac{1}{2}h < \mu(K) \leq \frac{\sqrt{2}}{2}h$.

(b) *Assume that $|\cos \xi| \leq 1/2$. Then $\lambda_1(K) = \lambda_2(K) = h$.*

(c) *Assume that $|\cos \xi| \leq 1/3$ and let $p, q \in \mathbb{Z}$ be such that $|p| + |q| \geq 2$. Then $\|pu + qv\| \geq \frac{2\sqrt{3}}{3}h$.*

The proof is an elementary exercise in plane geometry. If $0 < \xi \leq \pi/2$, then $\mu(K)$ is equal to the circumradius of the triangle with vertices $0, u, v$.

LEMMA 3.3. *Let $0 \leq i \leq m$. Then $\mu(L_i) \leq \frac{1}{2}s_i$.*

Proof. First observe that $\mu(L_0) = \mu(K_0) = \mu(\mathbb{Z}w) = \frac{1}{2}\|w\| = \frac{1}{2}h_0 = \frac{1}{2}s_0$. Assume $i \geq 1$. By Lemma 3.2(a) we have $\mu(K_j) \leq \frac{\sqrt{2}}{2}h_j$ for $j = 1, \dots, i$. Hence, by Lemma 3.1,

$$\mu(L_i) \leq \left(\sum_{j=0}^i \mu(K_j)^2 \right)^{1/2} \leq \left(\frac{1}{4}h_0^2 + \frac{1}{2} \sum_{j=1}^i h_j^2 \right)^{1/2} = \frac{1}{2}s_i. \blacksquare$$

LEMMA 3.4. *Let $1 \leq i \leq m$. Then*

$$\frac{h_i}{\sqrt{2(1+|\cos \xi_i|)}} \leq \mu(L_i) < \frac{h_i}{\sqrt{2(1+|\cos \xi_i|)}} \left(1 + \frac{s_{i-1}^2}{2h_i^2}\right).$$

Proof. Let us write $\mu_0 = \frac{1}{2}h_0$ and

$$\mu_j = \frac{h_j}{\sqrt{2(1+|\cos \xi_j|)}}, \quad j = 1, \dots, i.$$

Observe that

$$(3.6) \quad h_j^2/4 < \mu_j^2 \leq h_j^2/2, \quad j = 1, \dots, i.$$

We have $\mu(K_0) = \mu_0$ and $\mu(K_j) = \mu_j$ for $j = 1, \dots, i$ according to Lemma 3.2. Hence

$$\mu_i \leq \mu(L_i) \leq \left(\sum_{j=0}^i \mu_j^2\right)^{1/2}$$

by Lemma 3.1. Next, we may write

$$\begin{aligned} \sum_{j=0}^i \mu_j^2 &= \mu_i^2 \left(1 + \frac{1}{\mu_i^2} \sum_{j=0}^{i-1} \mu_j^2\right) = \mu_i^2 \left(1 + \frac{1}{\mu_i^2} \left(\mu_0^2 + \sum_{j=1}^{i-1} \mu_j^2\right)\right) \\ &\stackrel{(3.6)}{<} \mu_i^2 \left(1 + \frac{4}{h_i^2} \left(\frac{h_0^2}{4} + \frac{1}{2} \sum_{j=1}^{i-1} h_j^2\right)\right) = \mu_i^2 \left(1 + \frac{s_{i-1}^2}{h_i^2}\right) \end{aligned}$$

(if $i = 1$, the sum $\sum_{j=1}^{i-1}$ is treated as 0). Hence

$$\left(\sum_{j=0}^i \mu_j^2\right)^{1/2} < \mu_i \left(1 + \frac{s_{i-1}^2}{h_i^2}\right)^{1/2} < \mu_i \left(1 + \frac{s_{i-1}^2}{2h_i^2}\right). \quad \blacksquare$$

LEMMA 3.5. *Let L be a lattice in $L_2(0, 1)$ and let $M = \text{span } L$. Let $x \in L_2(0, 1) \setminus M$ and let $h = d(x, M)$. Let u (resp. \tilde{u}) be the shortest vector in $M + x$ (resp. in $L + x$), let $a = \pi(\tilde{u}; M)$ and let η be the angle between \tilde{u} and M . Then $\tilde{u} = u + a$,*

$$(3.7) \quad \|a\| \leq \mu(L),$$

$$(3.8) \quad h \leq \|\tilde{u}\| \leq (h^2 + \mu(L)^2)^{1/2} < h \left(1 + \frac{\mu(L)^2}{2h^2}\right)$$

and $\cot \eta \leq \mu(L)/h$.

Proof. By assumption, u is the orthogonal projection of 0 onto the hyperplane $M + x$; therefore $u \perp M$ and $\|u\| = h$. Since $u \in M + x$ and $\tilde{u} \in L + x \subset M + x$, it follows that $\tilde{u} - u \in M$; hence

$$\tilde{u} - u = \pi(\tilde{u} - u; M) = \pi(\tilde{u}; M) - \pi(u; M) = a.$$

Since \tilde{u} is the shortest vector in $L+x$ and $u \perp M$, it follows that $a = \tilde{u} - u$ is the shortest vector in $L+x-u$. This implies (3.7) (the length of the shortest vector in a shifted lattice does not exceed the covering radius of the lattice; observe that $x-u \in \text{span } L$).

The first inequality in (3.8) is obvious: $\|\tilde{u}\| \geq \|u\| = h$. As $\tilde{u} = u + a$ and $u \perp a$, we have $\|\tilde{u}\|^2 = \|u\|^2 + \|a\|^2 \leq h^2 + \mu(L)^2$ by (3.7). The last inequality in (3.8) is immediate:

$$(h^2 + \mu(L)^2)^{1/2} = h \left(1 + \frac{\mu(L)^2}{h^2} \right)^{1/2} < h \left(1 + \frac{\mu(L)^2}{2h^2} \right).$$

Finally, $\cot \eta = \|a\|/\|u\| \leq \mu(L)/h$ by (3.7). ■

For $i = 1, \dots, m$ let η_i be the angle between \tilde{u}_i and M_{i-1} ; naturally, it is the same as the angle between \tilde{v}_i and M_{i-1} , because $\Phi(\tilde{u}_i) = \tilde{v}_i$ and $\Phi(M_{i-1}) = M_{i-1}$.

LEMMA 3.6. *Let $1 \leq i \leq m$. Then:*

- (a) $h_i \leq \|\tilde{u}_i\| = \|\tilde{v}_i\| \leq \left(h_i^2 + \frac{s_{i-1}^2}{4} \right)^{1/2} < h_i \left(1 + \frac{s_{i-1}^2}{8h_i^2} \right)$;
- (b) $\cot \eta_i \leq s_{i-1}/(2h_i)$;
- (c) $|\cos \tilde{\xi}_i| \leq |\cos \xi_i| + s_{i-1}^2/(4h_i^2)$.

Proof. From Lemma 3.3 we obtain

$$(3.9) \quad \mu(L_{i-1}) \leq s_{i-1}/2.$$

By Lemma 3.5 we have

$$h_i \leq \|\tilde{u}_i\| = \|\tilde{v}_i\| \leq (h_i^2 + \mu(L_{i-1})^2)^{1/2} < h_i \left(1 + \frac{\mu(L_{i-1})^2}{2h_i^2} \right)$$

and $\cot \eta_i \leq \mu(L_{i-1})/h_i$, so that (a) and (b) follow from (3.9).

(c) Denote $a = \pi(\tilde{u}_i; M_{i-1})$ and $b = \pi(\tilde{v}_i; M_{i-1})$. By Lemma 3.5 we have $\tilde{u}_i = u_i + a$ and $\tilde{v}_i = v_i + b$; moreover $a, b \perp u_i, v_i$. Hence

$$|(\tilde{u}_i | \tilde{v}_i)| = |(u_i + a | v_i + b)| \leq |(u_i | v_i)| + |(a | b)| \leq |(u_i | v_i)| + \|a\| \cdot \|b\|.$$

By (a) we have $\|\tilde{u}_i\| = \|\tilde{v}_i\| \geq h_i$; from Lemma 3.5 and (3.9) we obtain $\|a\|, \|b\| \leq \mu(L_{i-1}) \leq \frac{1}{2}s_{i-1}$. Consequently,

$$|\cos \tilde{\xi}_i| = \frac{|(\tilde{u}_i | \tilde{v}_i)|}{\|\tilde{u}_i\| \cdot \|\tilde{v}_i\|} \leq \frac{|(u_i | v_i)|}{\|u_i\| \cdot \|v_i\|} + \frac{\|a\| \cdot \|b\|}{\|u_i\| \cdot \|v_i\|} \leq |\cos \xi_i| + \frac{s_{i-1}^2}{4h_i^2}. \quad \blacksquare$$

LEMMA 3.7. *Let $0 \leq i \leq m$. Then $\lambda_{2i+1}(L_i) \leq s_i$.*

Proof. We have $\lambda_1(L_0) = \|w\| = h_0 = s_0$. Let $i \geq 1$. Then $w, \tilde{u}_1, \tilde{v}_1, \dots, \tilde{u}_i, \tilde{v}_i$ are linearly independent vectors in L_i . According to Lemma 3.6(a), for $j = 1, \dots, i$ we have

$$\|\tilde{u}_j\|^2 = \|\tilde{v}_j\|^2 \leq h_j^2 + s_{j-1}^2/4 < 2h_j^2 + s_{j-1}^2 = s_j^2 \leq s_i^2,$$

so that $\|\tilde{u}_j\|, \|\tilde{v}_j\| < s_i$. ■

Let B (resp. \overline{B}) denote the open (resp. closed) unit ball in $L_2(0, 1)$.

LEMMA 3.8. *Let $1 \leq i \leq m$ and $s_{i-1} \leq h_i$. Then $\lambda_{2i+1}(L_i) \leq \|\tilde{u}_i\|$.*

Proof. Denote $r = \|\tilde{u}_i\|$. We may write $\lambda_{2i-1}(L_{i-1}) \leq s_{i-1} \leq h_i \leq \|\tilde{u}_i\| = r$; the first inequality follows from Lemma 3.7, the third one follows from Lemma 3.6(a). So, the ball $r\overline{B}$ contains $2i - 1$ linearly independent elements of L_{i-1} . Moreover, $r\overline{B}$ contains the vectors $\tilde{u}_i, \tilde{v}_i \in L_i \setminus M_{i-1}$. Thus $\lambda_{2i+1}(L_i) \leq r$. ■

LEMMA 3.9. *Let $1 \leq i \leq m$. Assume that*

$$(3.10) \quad \|\tilde{u}_i\| \leq \frac{2\sqrt{3}}{3}h_i,$$

$$(3.11) \quad \|\tilde{u}_i\| \leq h_j, \quad i + 1 \leq j \leq m,$$

$$(3.12) \quad |\cos \xi_i| \leq 1/3,$$

$$(3.13) \quad |\cos \xi_j| \leq 1/2, \quad i + 1 \leq j \leq m.$$

Then $\lambda_{2i}(L_m) \geq \|\tilde{u}_i\|$.

Proof. Denote $r = \|\tilde{u}_i\|$. It is enough to show that $rB \cap L_m \subset M_{i-1}$. First we prove that

$$(3.14) \quad rB \cap L_m \subset rB \cap L_i.$$

If $i = m$, there is nothing to prove. Assume $i < m$. From (3.11) we get $r \leq h_m$, whence $rB \subset h_mB$. From (3.13) we get $|\cos \xi_m| \leq 1/2$, whence $\lambda_1(K_m) = h_m$ due to Lemma 3.2(b). Next, it is not hard to see that $\lambda_1(K_m)B \cap L_m \subset L_{m-1}$. Consequently,

$$rB \cap L_m \subset h_mB \cap L_m = \lambda_1(K_m)B \cap L_m \subset L_{m-1},$$

and therefore $rB \cap L_m \subset rB \cap L_{m-1}$.

If $i < m - 1$, we can repeat the above argument, with m replaced by $m - 1$, to get $rB \cap L_{m-1} \subset rB \cap L_{m-2}$; and so on. After $m - 1$ such steps we obtain (3.14).

It remains to show that $rB \cap L_i \subset M_{i-1}$. Let $x \in L_i \setminus M_{i-1}$. We have to show that $\|x\| \geq r$. We may write

$$L_i = L_{i-1} + \mathbb{Z}x_i + \mathbb{Z}y_i = \bigcup_{p,q \in \mathbb{Z}} (L_{i-1} + px_i + qy_i).$$

So, $x \in L_{i-1} + px_i + qy_i$ for some $p, q \in \mathbb{Z}$ with $|p| + |q| \geq 1$. If $p = 1$ and $q = 0$, then $\|x\| \geq \|\tilde{u}_i\| = r$, because \tilde{u}_i is, by definition, the shortest vector in $L_{i-1} + x_i$. If $p = -1$ and $q = 0$, then $-x \in L_{i-1} + x_i$, so that $\|x\| = \|-x\| \geq r$. In the same way we prove that $\|x\| \geq r$ if $p = 0$ and $q = \pm 1$. Finally, if $|p| + |q| \geq 2$, then, by (3.12) and Lemma 3.2(c), we have $\|pu_i + qv_i\| \geq \frac{2\sqrt{3}}{3}h_i$. Thus

$$\|x\| \geq \|\pi(x; N_i)\| = \|pu_i + qv_i\| \geq \frac{2\sqrt{3}}{3}h_i \stackrel{(3.10)}{\geq} r. \quad \blacksquare$$

4. The proofs. We will prove Theorems 1.1 and 1.2 for n even. For n odd the proofs are almost the same and need only minor modifications; one needs analogues of the lemmas from Section 3. The difference between the two cases is the following. If $n = 2m$, then in the proofs below we consider the lattice $\mathbf{P}_n^{\mathbb{Z}}$ with the basis $S_0, T_0, \dots, S_{m-1}, T_{m-1}, U_m$. For $n = 2m + 1$ one should consider the basis $S_0, T_0, \dots, S_m, T_m$ instead.

In this section $m \geq 1$ is a fixed integer and $n = 2m$. We set $w := U_m \equiv U_{m,m}$ and

$$x_i := S_{m-i}, \quad y_i := T_{m-i}, \quad i = 1, \dots, m.$$

Let then $L_i, M_i, h_i, s_i, u_i, v_i, \tilde{u}_i, \tilde{v}_i$ and ξ_i be defined as in Section 3. Thus

$$L_0 = \mathbb{Z}U_m, \quad M_0 = \text{span } L_0 = \mathbb{R}U_m, \quad h_0 = s_0 = \|U_m\|$$

and, for $i = 1, \dots, m$,

$$L_i = \mathbb{Z}U_m + \mathbb{Z}S_{m-1} + \mathbb{Z}T_{m-1} + \dots + \mathbb{Z}S_{m-i} + \mathbb{Z}T_{m-i} = \mathbf{P}_{n,m-i}^{\mathbb{Z}},$$

$$M_i = \text{span}\{U_m, S_{m-1}, T_{m-1}, \dots, S_{m-i}, T_{m-i}\} = \mathbf{P}_{n,m-i},$$

$$h_i = d(S_{m-i}, \mathbf{P}_{n,m-i+1}),$$

$$s_i = \left(\|U_m\|^2 + 2 \sum_{j=1}^i d(S_{m-j}, \mathbf{P}_{n,m-j+1})^2 \right)^{1/2},$$

$$u_i = S_{n,m-i}, \quad v_i = T_{n,m-i}, \quad \tilde{u}_i = \tilde{S}_{n,m-i}, \quad \tilde{v}_i = \tilde{T}_{n,m-i}, \quad \xi_i = \varphi_{n,m-i}.$$

By Lemma 2.2 we have $\|U_m\| = a_{n,m}^{1/1}$. By Lemma 2.4, for $i = 1, \dots, m$ we have $d(S_{m-i}, \mathbf{P}_{n,m-i+1}) = c_{n,m-i}^{1/2}$, so that $h_i = c_{n,m-i}^{1/2}$ and

$$s_i = \left(a_{m,m} + 2 \sum_{j=1}^i c_{n,m-j} \right)^{1/2} = \left(a_{m,m} + 2 \sum_{k=m-i}^{m-1} c_{n,k} \right)^{1/2}.$$

Therefore for $i \geq 2$ we may write

$$\frac{s_{i-1}^2}{2h_i^2} = c_{n,m-i}^{-1} \left(\frac{a_{m,m}}{2} + \sum_{k=m-i+1}^{m-1} c_{n,k} \right) = \gamma_{n,m-i}.$$

Lemma 2.6 says that $\gamma_{n,r} < 0.026$ if $3r + 3 \leq m$. In other words, we have $s_{j-1}^2/h_j^2 < 0.052$ if $3j \geq 2m + 3$, which implies in particular that

$$(4.1) \quad s_{j-1} < h_j \quad \text{if } 3j \geq 2m + 3.$$

Proof of Theorems 1.1 and 1.2. By assumption we have

$$(4.2) \quad r \leq n/6 - 2,$$

i.e. $n \geq 6r + 12$. Hence, by Lemma 2.7,

$$(4.3) \quad \gamma_{n,r} < 1.026\chi_{n,r+1}.$$

Condition (4.2) implies that $2(r+1)/n < 1/3$, whence

$$(4.4) \quad \chi_{n,r+1} = \left[\frac{(2(r+1)/n)^2}{1 - (2(r+1)/n)^2} \right]^2 < \left(\frac{1/9}{1 - 1/9} \right)^2 = \frac{1}{64}.$$

Let us denote $i = m - r$. Then $n - 2r = 2i$ and

$$\begin{aligned} c_{n,r}^{1/2} &= h_i, & \mathbf{P}_{n,r}^{\mathbb{Z}} &= L_i, & \mathbf{P}_n^{\mathbb{Z}} &\equiv \mathbf{P}_{n,0}^{\mathbb{Z}} = L_m, \\ \tilde{S}_{n,r} &= \tilde{u}_i, & \tilde{T}_{n,r} &= \tilde{v}_i, & \gamma_{n,r} &= \frac{s_{i-1}^2}{2h_i^2}. \end{aligned}$$

We begin with the proof of Theorem 1.1. Condition (4.2) may be written as $3r \leq m - 6$, whence

$$(4.5) \quad 3i = 3m - 3r \geq 2m + 6.$$

Now from (4.1) it follows that

$$(4.6) \quad s_{i-1} < h_i.$$

Hence, by Lemma 3.8, we obtain $\lambda_{2i+1}(L_i) \leq \|\tilde{u}_i\|$, i.e.

$$(4.7) \quad \lambda_{n-2r+1}(\mathbf{P}_{n,r}^{\mathbb{Z}}) \leq \|\tilde{S}_{n,r}\|.$$

To apply Lemma 3.9 we have to verify (3.10)–(3.13). Lemma 3.6(a) yields

$$\|\tilde{u}_i\|^2 \leq h_i^2 + s_{i-1}^2/4 \stackrel{(4.6)}{<} h_i^2 + h_i^2/4 < \frac{4}{3}h_i^2,$$

which proves (3.10). To prove (3.11) suppose that $i + 1 \leq j \leq m$. Then $3j > 3i \stackrel{(4.5)}{\geq} 2m + 6$ and, by (4.1),

$$(4.8) \quad s_{j-1} < h_j.$$

Now, by Lemma 3.6(a),

$$\|\tilde{u}_i\|^2 \leq h_i^2 + s_{i-1}^2/4 < h_i^2 + s_{i-1}^2/2 = s_i^2/2 \leq s_{j-1}^2/2 \stackrel{(4.8)}{<} h_j^2/2 < h_j^2,$$

which proves (3.11). Finally, if $j \geq i$, then (4.5) implies $3j > 2m + 1$, which may be written as $3(m - j) + 1 < m$. Hence, by Lemma 2.5, $|\cos \xi_j| = |\cos \varphi_{n,m-j}| \leq 1/3$. This proves (3.12) and (3.13). Thus, by Lemma 3.9, $\lambda_{2i}(L_m) \geq \|\tilde{u}_i\|$, i.e.

$$(4.9) \quad \lambda_{n-2r}(\mathbf{P}_{n,0}^{\mathbb{Z}}) \geq \|\tilde{S}_{n,r}\|.$$

Now, as $0 \leq s \leq r$, we may write

$$\begin{aligned} \|\tilde{S}_{n,r}\| &\stackrel{(4.9)}{\leq} \lambda_{n-2r}(\mathbf{P}_{n,0}^{\mathbb{Z}}) \leq \lambda_{n-2r}(\mathbf{P}_{n,s}^{\mathbb{Z}}) \\ &\leq \lambda_{n-2r+1}(\mathbf{P}_{n,s}^{\mathbb{Z}}) \leq \lambda_{n-2r+1}(\mathbf{P}_{n,r}^{\mathbb{Z}}) \stackrel{(4.7)}{\leq} \|\tilde{S}_{n,r}\|, \end{aligned}$$

which gives

$$\lambda_{n-2r}(\mathbf{P}_{n,s}^{\mathbb{Z}}) = \lambda_{n-2r+1}(\mathbf{P}_{n,s}^{\mathbb{Z}}) = \|\tilde{S}_{n,r}\|.$$

From Lemma 3.6(a) we obtain

$$h_i \leq \|\tilde{u}_i\| < \left(1 + \frac{s_{i-1}^2}{8h_i^2}\right) h_i,$$

which means that

$$c_{n,r}^{1/2} \leq \|\tilde{S}_{n,r}\| < \left(1 + \frac{\gamma_{n,r}}{4}\right) c_{n,r}^{1/2}.$$

To complete the proof of Theorem 1.1 it remains to observe that

$$1 + \gamma_{n,r}/4 \stackrel{(4.3)}{<} 1 + 0.26\chi_{n,r+1} \stackrel{(4.4)}{<} 1.0041.$$

The proof of Theorem 1.2 is very short. From Lemma 2.5 we get

$$\kappa_{n,r} = \sqrt{2(1 + |\cos \varphi_{n,r}|)} = \sqrt{2(1 + |\cos \xi_i|)}.$$

So, according to Lemma 3.4,

$$\frac{c_{n,r}^{1/2}}{\kappa_{n,r}} \leq \mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) < (1 + \gamma_{n,r}) \frac{c_{n,r}^{1/2}}{\kappa_{n,r}}.$$

To complete the proof it remains to observe that

$$1 + \gamma_{n,r} \stackrel{(4.3)}{<} 1 + 1.026\chi_{n,r+1} \stackrel{(4.4)}{<} 1.0161. \blacksquare$$

REMARK 4.1. The sequence

$$(4.10) \quad \tilde{S}_{n,0}, \tilde{T}_{n,0}, \tilde{S}_{n,1}, \tilde{T}_{n,1}, \dots, \tilde{S}_{n,m-1}, \tilde{T}_{n,m-1}, U_m$$

is a basis of the lattice $\mathbf{P}_n^{\mathbb{Z}}$. Let $\tilde{\varphi}_{n,r}$ denote the angle between $\tilde{S}_{n,r}$ and $\tilde{T}_{n,r}$. Next, let $\tilde{\psi}_{n,r}$ denote the angle between $\tilde{S}_{n,r}$ (or $\tilde{T}_{n,r}$) and the subspace $\mathbf{P}_{n,r+1}$. From the above proof and from Lemma 3.6(b),(c) one can deduce that if $0 \leq r \leq n/6 - 2$, then

$$\begin{aligned} \cot \tilde{\psi}_{n,r} &\leq (\gamma_{n,r}/2)^{1/2} < \sqrt{0.513} \chi_{n,r+1}^{1/2} < 0.09, \\ |\cos \tilde{\varphi}_{n,r}| &\leq |\cos \varphi_{n,r}| + \frac{\gamma_{n,r}}{2} < \frac{2r+1}{n+1} + 0.513\chi_{n,r+1} < \frac{1}{3} + \frac{0.513}{64} < 0.342. \end{aligned}$$

So, if r is small compared to n , then the polynomial $\tilde{S}_{n,r}$ (resp. $\tilde{T}_{n,r}$) is almost orthogonal to the other polynomials of the basis (4.10).

REMARK 4.2. Let $m \geq 1$. From Proposition 2.9 it follows that the lattice $\mathbf{E}_m^{\mathbb{Z}} \equiv \mathbf{E}_{m,0}^{\mathbb{Z}}$ is the orthogonal direct sum of the m -dimensional lattice $\mathbf{E}_{m,1}^{\mathbb{Z}}$ and the 1-dimensional lattice $\mathbb{Z}U_{m,0}$. Similarly, $\mathbf{F}_m^{\mathbb{Z}}$ is the orthogonal direct sum of $\mathbf{F}_{m,1}^{\mathbb{Z}}$ and $\mathbb{Z}V_{m,0}$.

REMARK 4.3. Little is known about the successive minima $\lambda_i(\mathbf{P}_n^{\mathbb{Z}})$ for $i \lesssim 2n/3$. The only exception is the first minimum, $\lambda_1(\mathbf{P}_n^{\mathbb{Z}})$. By definition we have

$$\lambda_1(\mathbf{P}_n^{\mathbb{Z}}) = \min\{\|P\|_{L_2(0,1)} : 0 \neq P \in \mathbf{P}_n^{\mathbb{Z}}\}.$$

Let us denote

$$\varrho_n := \min\{\|P\|_{C[0,1]} : 0 \neq P \in \mathbf{P}_n^{\mathbb{Z}}\}.$$

The limit

$$t_{\mathbb{Z}}([0, 1]) := \lim_{n \rightarrow \infty} \varrho_n^{1/n}$$

is called the *integer Chebyshev constant* for the interval $[0, 1]$ and was investigated in many papers; see e.g. [P1, P2] for historical and bibliographical information. The best known bounds are

$$0.4213 < t_{\mathbb{Z}}([0, 1]) < 0.42291334$$

(see [P2, p. 3]). It is a standard fact that

$$\|P\|_{L_2(0,1)} \leq \|P\|_{C[0,1]} \leq (n+1)\|P\|_{L_2(0,1)}$$

for $P \in \mathbf{P}_n$. Hence it follows that $\lim_{n \rightarrow \infty} \lambda_1(\mathbf{P}_n^{\mathbb{Z}})^{1/n} = t_{\mathbb{Z}}([0, 1])$.

5. Dual lattices and transference theorems. Let L be a lattice in $L_2(0, 1)$. By the *dual lattice* we mean the set

$$L^* := \{P \in \text{span } L : (P | Q) \in \mathbb{Z} \text{ for all } Q \in L\}.$$

THEOREM 5.1.

(a) Let $r \geq 0$ and $r \leq n/6$. Then

$$\lambda_1((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) = \lambda_2((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) = \frac{c_{n,r}^{-1/2}}{\sin \varphi_{n,r}}.$$

(b) Let $r \geq 0$, $s \geq 1$ and $r + s \leq n/6$. Then

$$\begin{aligned} \frac{c_{n,r+s}^{-1/2}}{\sin \varphi_{n,r+s}} &\leq \lambda_{2s+1}((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) = \lambda_{2s+2}((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) \\ &< \left[1 + \frac{1}{4} \cdot \frac{\chi_{n,r+s}}{1 - \chi_{n,r+s}} \right] \frac{c_{n,r+s}^{-1/2}}{\sin \varphi_{n,r+s}} \leq \frac{253}{252} \cdot \frac{c_{n,r+s}^{-1/2}}{\sin \varphi_{n,r+s}}. \end{aligned}$$

Note that, by Lemma 2.5,

$$\sin \varphi_{n,r+s} = \sqrt{1 - \left(\frac{2r + 2s + 1}{n + 1} \right)^2}.$$

Theorem 5.1 is a relatively simple consequence of the estimates of the quantities $c_{n,r}$ and $\gamma_{n,r}$ which we used in the proof of Theorem 1.1. We omit the proof; it is long and consists in labourious calculations. In some sense it is dual to the proof of Theorem 1.1.

Let L be a d -dimensional lattice. Then the following transference theorems are valid:

$$(5.1) \quad 1 \leq \lambda_{d+1-i}(L) \cdot \lambda_i(L^*) \leq d, \quad i = 1, \dots, d,$$

$$(5.2) \quad \frac{1}{2} \leq \mu(L) \cdot \lambda(L^*) \leq \frac{1}{2}d.$$

The lower bounds are trivial and the upper bounds were obtained in [B]; see also [G, Sect. 5, p. 751]. A result of Conway and Thompson (see [MH]) shows that there exist d -dimensional (even self-dual) lattices L_d such that $\lambda_1(L_d) \cdot \lambda_1(L_d^*) \geq \gamma d$, where $\gamma > 0$ is some numerical constant. This means that the upper bounds in (5.1) and (5.2) are the best possible up to some multiplicative constants.

The 2-dimensional lattice $\mathbf{P}_1^{\mathbb{Z}} \equiv \mathbf{P}_{1,0}^{\mathbb{Z}}$ is a hexagonal lattice generated by the polynomials x and $1 - x$ of the same length $\sqrt{3}/3$; the angle between them is equal to $\pi/6$. It is easy to see that $\lambda_1((\mathbf{P}_1^{\mathbb{Z}})^*) = 2$, so that $\lambda_1(\mathbf{P}_n^{\mathbb{Z}}) \cdot \lambda_1((\mathbf{P}_1^{\mathbb{Z}})^*) = 2\sqrt{3}/3$, and this is the maximal possible value of this product for 2-dimensional lattices. This observation led to the following questions: how ‘twisted’ (far from orthogonal) can the lattices $\mathbf{P}_n^{\mathbb{Z}}$ be and how big can the products $\lambda_{n-2r+2-i}(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_i((\mathbf{P}_{n,r}^{\mathbb{Z}})^*)$ and $\mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_1((\mathbf{P}_{n,r}^{\mathbb{Z}})^*)$ be? (The dimension of the lattice $\mathbf{P}_{n,r}^{\mathbb{Z}}$ is equal to $n - 2r + 1$.)

Let us replace r by $r + s$ and s by r in Theorem 1.1. Then we get

$$c_{n,r+s}^{1/2} \leq \lambda_{n-2r-2s}(\mathbf{P}_{n,r}^{\mathbb{Z}}) = \lambda_{n-2r-2s+1}(\mathbf{P}_{n,r}^{\mathbb{Z}}) < [1 + 0.26\chi_{n,r+s+1}]c_{n,r+s}^{1/2}$$

provided that $r + s \leq n/6 - 2$. Combined with Theorem 5.1, this yields

$$\begin{aligned} \frac{1}{\sin \varphi_{n,r+s}} &\leq \lambda_{n-2r-i+2}(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_i((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) \\ &< [1 + 0.26\chi_{n,r+s+1}] \cdot \left[1 + \frac{1}{4} \cdot \frac{\chi_{n,r+s}}{1 - \chi_{n,r+s}}\right] \cdot \frac{1}{\sin \varphi_{n,r+s}} \end{aligned}$$

for $i = 2s + 1, 2s + 2$. Hence it follows that if i and r are small compared to n , then the product $\lambda_{n-2r-i+2}(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_i((\mathbf{P}_{n,r}^{\mathbb{Z}})^*)$ is close to 1. In particular, if $2r + i \leq n/3 - 2$, it is less than 1.07.

Theorem 1.2 combined with Theorem 5.1 yields

$$\begin{aligned} \frac{1}{\sin \varphi_{n,r} \cdot \sqrt{2(1 + |\cos \varphi_{n,r}|)}} &\leq \mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_1((\mathbf{P}_{n,r}^{\mathbb{Z}})^*) \\ &< [1 + 1.026\chi_{n,r+1}] \cdot \frac{1}{\sin \varphi_{n,r} \cdot \sqrt{2(1 + |\cos \varphi_{n,r}|)}}. \end{aligned}$$

So, if r is small compared to n , then the product $\mu(\mathbf{P}_{n,r}^{\mathbb{Z}}) \cdot \lambda_1((\mathbf{P}_{n,r}^{\mathbb{Z}})^*)$ is close to $\sqrt{2}/2$.

The above remarks show that if r is small compared to n , then from the point of view of transference theorems the lattices $\mathbf{P}_{n,r}^{\mathbb{Z}}$ are not especially

interesting. This is due to the fact that in a certain sense they are almost orthogonal (see Remark 4.1). It is not clear what happens for $r \gtrsim n/3$.

References

- [B] W. Banaszczyk, *New bounds in some transference theorems in the geometry of numbers*, Math. Ann. 296 (1993), 625–635.
- [BL] W. Banaszczyk and A. Lipnicki, *On the lattice of polynomials with integer coefficients*, Ann. Polon. Math. 115 (2015), 123–144.
- [G] P. M. Gruber, *Geometry of numbers*, in: Handbook of Convex Geometry, Vol. B, P. M. Gruber and J. M. Wills (eds.), North-Holland, Amsterdam, 1993, 739–763.
- [MH] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, Berlin, 1973.
- [P1] I. E. Pritsker, *Small polynomials with integer coefficients*, J. Anal. Math. 96 (2005), 151–190.
- [P2] I. E. Pritsker, *Polynomials with integer coefficients and their zeros*, J. Math. Sci. (N.Y.) 183 (2012), 810–822.

Wojciech Banaszczyk
Faculty of Mathematics and Computer Science
University of Lodz
Banacha 22
90-238 Łódź, Poland
E-mail: wojciech.banaszczyk@wmii.uni.lodz.pl