INTEGRAL ORTHOGONAL BASES OF SMALL HEIGHT FOR REAL POLYNOMIAL SPACES

LENNY FUKSHANSKY

Abstract. Let $\mathcal{P}_N(\mathbb{R})$ be the space of all real polynomials in N variables with the usual inner product $\langle\ ,\ \rangle$ on it, given by integrating over the unit sphere. We start by deriving an explicit combinatorial formula for the bilinear form representing this inner product on the space of coefficient vectors of all polynomials in $\mathcal{P}_N(\mathbb{R})$ of degree $\leq M$. We exhibit two applications of this formula. First, given a finite dimensional subspace V of $\mathcal{P}_N(\mathbb{R})$ defined over $\mathbb{Q}$, we prove the existence of an orthogonal basis for $(V, \langle\ ,\ \rangle)$, consisting of polynomials of small height with integer coefficients, providing an explicit bound on the height; this can be viewed as a version of Siegel's lemma for real polynomial inner product spaces. Secondly, we derive a criterion for a finite set of points on the unit sphere in $\mathbb{R}^N$ to be a spherical M-design.

1. Introduction and notation

Siegel's lemma originated as an important combinatorial principle that a system of homogeneous linear equations with integer coefficients should have a nontrivial integral solution vector whose entries are comparable in size to the coefficients of the system. Although this observation was already made by Thue [15] in 1909, the first formal proof of such a result by an application of the pigeonhole principle appeared in the paper [12] of Siegel in 1929. In its modern formulation, Siegel's lemma is a statement about the existence of a "short" basis for a vector space over a global field, where the size of the vectors is measured with respect to a *height function*, a standard tool of Diophantine geometry which generalizes the naive sup-norm over integers. A general result like this was first proved over number fields by Bombieri and Vaaler [2] in 1983 with further extensions by a variety of authors following in the consequent years. In particular, given a symmetric bilinear space one may ask for a short *orthogonal* basis over a fixed field or ring. Results of this nature were recently obtained in [5] and [6], where the height of basis vectors in question were bounded in terms of the heights of the vector space and the coefficient vector of the bilinear form. One goal of the present note is to produce a similar result for real polynomial spaces. We start by setting up some notation.

Let $N \geq 2$ be an integer, and let us consider the algebra of all polynomials in N variables with real coefficients

$$\mathcal{P}_N(\mathbb{R}) := \mathbb{R}[X_1, ..., X_N]$$

1991 *Mathematics Subject Classification.* Primary 11C08, 11G50, 05B30.

Key words and phrases. polynomials, Siegel's lemma, heights, spherical designs.

as an infinite-dimensional real vector space with the standard inner product on it (see, for instance Chapter IV of [13]), given by

$$\langle F,G\rangle = \frac{1}{\alpha_N}\int_{\Sigma_{N-1}} F(\boldsymbol{x})G(\boldsymbol{x})d\boldsymbol{x}, \tag{1}$$

for each $F,G \in \mathcal{P}_N(\mathbb{R})$, where Σ_{N-1} is the unit sphere in $\mathbb{R}^N$, we integrate with respect to the usual Lebesgue measure on $\mathbb{R}^N$, and α_N is the generalized surface area of Σ_{N-1}:

$$\alpha_N = \begin{cases} \frac{(2\pi)^{N/2}}{2\times 4\times\cdots\times(N-2)} & \text{if } N \text{ is even} \\ \frac{2(2\pi)^{(N-1)/2}}{1\times 3\times\cdots\times(N-2)} & \text{if } N \text{ is odd.} \end{cases} \tag{2}$$

Let $M \geq 1$ be an integer, and write

$$\mathcal{M}(M,N) = \left\{ \boldsymbol{m} \in \mathbb{Z}^N_{\geq 0} : w(\boldsymbol{m}) := \sum_{i=1}^N m_i \leq M \right\} \tag{3}$$

for a set of multi-indexes, arranged in lexicographic order; we call $w(\boldsymbol{m})$ the *weight* of the index vector $\boldsymbol{m}$. Define $\mathcal{P}_N^M(\mathbb{R})$ to be the space of all polynomials in $\mathcal{P}_N(\mathbb{R})$ of degree $\leq M$, then each polynomial $F(X_1,...,X_N) \in \mathcal{P}_N^M(\mathbb{R})$ can be written as

$$F(\boldsymbol{X}) = \sum_{\boldsymbol{m}\in\mathcal{M}(M,N)} c_F(\boldsymbol{m})\boldsymbol{X}^{\boldsymbol{m}}, \tag{4}$$

where $\boldsymbol{X}^{\boldsymbol{m}} = X_1^{m_1}...X_N^{m_N}$, $c_F(\boldsymbol{m}) \in \mathbb{R}$ for each $\boldsymbol{m} \in \mathcal{M}(M,N)$; here and for the rest of the paper we adopt the convention that $X_i^0 = 1$, even when $X_i = 0$. We also write $\boldsymbol{c}_F = (c_F(\boldsymbol{m}))_{\boldsymbol{m}\in\mathcal{M}(M,N)} \in \mathbb{R}^{L(M,N)}$ for the vector of coefficients of F, where

$$L(M,N) := |\mathcal{M}(M,N)| = \dim_{\mathbb{R}} \mathcal{P}_N^M(\mathbb{R}) = \sum_{k=0}^M \binom{N+k-1}{k}. \tag{5}$$

An important tool we need is an explicit combinatorial formula for $\langle F,G\rangle$ in terms of the coefficients of polynomials $F(\boldsymbol{X})$ and $G(\boldsymbol{X})$.

Let us fix $M \geq 1$, and let $L = L(M,N)$ as given by (5). Let us also define the double factorial $m!!$ for any integer $m \geq -1$ to be

$$m!! = \begin{cases} m(m-2)(m-4)\dots 5\times 3\times 1 & \text{if } m>1 \text{ is odd} \\ m(m-2)(m-4)\dots 6\times 4\times 2 & \text{if } m>1 \text{ is even} \\ 1 & \text{if } m=-1,0,1. \end{cases} \tag{6}$$

For each $\boldsymbol{m} = (m_1,...,m_N) \in \mathcal{M}(M,N)$, define

$$P(\boldsymbol{m}) = \frac{\prod_{i=1}^N (2m_i-1)!!}{\prod_{k=1}^{w(\boldsymbol{m})}(N-2+2k)}, \tag{7}$$

where an empty product $\prod_{k=1}^0$ is interpreted as equal to 1. For each $\boldsymbol{a} \in \mathbb{R}^L$, we write $\boldsymbol{a} = (a(\boldsymbol{m}))_{\boldsymbol{m}\in\mathcal{M}(M,N)}$. Let

$$2\mathcal{M}(M,N) = \{2\boldsymbol{m} : \boldsymbol{m} \in \mathcal{M}(M,N)\},$$

and let

$$E(M,N) = \{(\boldsymbol{m}_1,\boldsymbol{m}_2) \in \mathcal{M}(M,N)\times\mathcal{M}(M,N) : \boldsymbol{m}_1+\boldsymbol{m}_2 \in 2\mathcal{M}(M,N)\}.$$

Define a bilinear form $\mathcal{L}_{M,N} \ : \mathbb{R}^L \times \mathbb{R}^L \longrightarrow \mathbb{R}$ by

$$\mathcal{L}_{M,N}(\boldsymbol{a},\boldsymbol{b}) = \sum_{(\boldsymbol{m}_1,\boldsymbol{m}_2)\in E(M,N)} P\left(\frac{\boldsymbol{m}_1+\boldsymbol{m}_2}{2}\right) a(\boldsymbol{m}_1)b(\boldsymbol{m}_2), \tag{8}$$

for each $(\boldsymbol{a},\boldsymbol{b}) \in \mathbb{R}^L \times \mathbb{R}^L$, and let $\mathcal{L}_{M,N}(\boldsymbol{a}) := \mathcal{L}_{M,N}(\boldsymbol{a},\boldsymbol{a})$ be the corresponding quadratic form. Notice in particular that if $(\boldsymbol{m}_1,\boldsymbol{m}_2) \in \mathcal{M}(M,N) \setminus E(M,N)$, then the coefficient of $\mathcal{L}_{M,N}(\boldsymbol{a},\boldsymbol{b})$ corresponding to the monomial $a(\boldsymbol{m}_1)b(\boldsymbol{m}_2)$ is equal to zero. Then we have the following result.

Theorem 1.1. *For each $F(\boldsymbol{X}), G(\boldsymbol{X}) \in \mathcal{P}_N^M(\mathbb{R})$,*

$$\langle F, G\rangle = \mathcal{L}_{M,N}(\boldsymbol{c}_F, \boldsymbol{c}_G), \tag{9}$$

where $\boldsymbol{c}_F, \boldsymbol{c}_G$ are coefficient vectors of F and G, respectively.

Remark 1.1. An immediate implication of (9) is that the quadratic form $\mathcal{L}_{M,N}(\boldsymbol{a})$ must be positive definite, since it is a norm form.

We prove Theorem 1.1 in section 2. Next, let V be a n-dimensional subspace of $\mathcal{P}_N(\mathbb{R})$ defined over $\mathbb{Q}$, $n \geq 1$, and define *degree* of V to be

$$d = \deg(V) := \min\left\{M \in \mathbb{Z} : V \subseteq \mathcal{P}_N^M(\mathbb{R})\right\}.$$

Then $(V, \langle\ ,\ \rangle)$ is a finite-dimensional $\mathbb{Q}$-inner product space, so there must exist an orthogonal basis for V consisting of polynomials with integer coefficients. We will prove the existence of a basis like this with each polynomial having relatively small height, which is a version of Siegel's lemma for polynomial spaces with additional orthogonality conditions.

For each polynomial $F(\boldsymbol{x}) \in \mathcal{P}_N(\mathbb{R})$, define the height of F by

$$H(F) = |\boldsymbol{c}_F| := \max_{\boldsymbol{m}\in\mathcal{M}(M,N)} |c_F(\boldsymbol{m})|, \tag{10}$$

where $M = \deg(F)$. Let $L = |\mathcal{M}(d,N)|$, and define an injective linear map $\varphi : V \to \mathbb{R}^L$ by $\varphi(F) = \boldsymbol{c}_F$. Let $f_1, \dots, f_k$ be a basis for V, and let $C = (\boldsymbol{c}_{f_1} \dots \boldsymbol{c}_{f_k})$ be the corresponding $L \times k$ basis matrix for $\varphi(V)$. Then define the height of V by

$$H(V) = D^{-1}\sqrt{|\det(C^tC)|},$$

where D is the greatest common divisor of the determinants of all $k \times k$ minors of C; $H(V)$ is well-defined, i.e. this definition does not depend on the choice of a basis for V. With this notation, we can now state our main result.

Theorem 1.2. *Let V be as above. Then there exists an orthogonal basis $g_1, \dots, g_n$ for $(V, \langle\ ,\ \rangle)$ consisting of polynomials with integer coefficients so that*

$$\prod_{i=1}^n H(g_i) \leq L^{\frac{3n(n+1)}{2}} H(V)^n. \tag{11}$$

We prove Theorem 1.2 in section 3. Our main tools are Theorem 1.1 and a version of Siegel's lemma due to Bombieri and Vaaler [2]. In fact, we prove a more general statement than Theorem 1.2, Theorem 3.6, where $\langle\ ,\ \rangle$ is replaced by an arbitrary bilinear form defined on V. Finally, in section 4 we derive an application of Theorem 1.1 to spherical designs, presenting a necessary and sufficient criterion for a finite set of points on the unit sphere in $\mathbb{R}^N$ to be a spherical M-design (see Theorem 4.1).

2. Proof of Theorem 1.1

Let us write $\mathcal{M}$ for $\mathcal{M}(M,N)$, E for $E(M,N)$, and $\mathcal{L}$ for $\mathcal{L}_{M,N}$. First notice that

$$\langle F,G\rangle = \sum_{\boldsymbol{m}_1\in\mathcal{M}}\sum_{\boldsymbol{m}_2\in\mathcal{M}} c_F(\boldsymbol{m}_1)c_G(\boldsymbol{m}_2)S(\boldsymbol{m}_1,\boldsymbol{m}_2), \tag{12}$$

where

$$S(\boldsymbol{m}_1,\boldsymbol{m}_2) = \frac{1}{\alpha_N}\int_{\Sigma_{N-1}} \boldsymbol{x}^{\boldsymbol{m}_1+\boldsymbol{m}_2}d\boldsymbol{x} = \frac{1}{\alpha_N}\int_{\Sigma_{N-1}}\prod_{i=1}^N x_i^{\varepsilon_i}d\boldsymbol{x}, \tag{13}$$

where the weight $w(\boldsymbol{m}_1+\boldsymbol{m}_2) = \sum_{i=1}^N \varepsilon_i \leq 2M$, $\varepsilon_i \in \mathbb{Z}_{\geq 0}$ for all $1 \leq i \leq N$. Consider a change to spherical coordinates (see, for instance, page 181 of [4]) $0 \leq \theta_i \leq \pi$ for all $1 \leq i \leq N-2$, $0 \leq \theta_{N-1} \leq 2\pi$, given by

$$x_i = \cos\ \theta_i \prod_{j=1}^{i-1} \sin\ \theta_j, \tag{14}$$

for all $1 \leq i \leq N-1$, and $x_N = \prod_{j=1}^{N-1}\sin\ \theta_j$. The Jacobian of this coordinate change is

$$J = \prod_{i=1}^{N-2} \sin^{N-1-i}\theta_i. \tag{15}$$

Then

$$\begin{aligned} S(\boldsymbol{m}_1,\boldsymbol{m}_2) &= \frac{1}{\alpha_N}\left(\prod_{i=1}^{N-2}\int_0^\pi \cos^{\varepsilon_i}\theta_i\ \sin^{\beta_i}\theta_i\ d\theta_i\right)\times \\ &\times \int_0^{2\pi}\cos^{\varepsilon_{N-1}}\theta_{N-1}\ \sin^{\beta_{N-1}}\theta_{N-1}\ d\theta_{N-1}, \end{aligned} \tag{16}$$

where $\beta_i = N-1-i+\sum_{j=i+1}^N \varepsilon_i$, for all $1 \leq i \leq N-1$; in particular, $\beta_{N-1} = \varepsilon_N$. For each $1 \leq i \leq N-2$,

$$\int_0^\pi \cos^{\varepsilon_i}\theta_i\ \sin^{\beta_i}\theta_i\ d\theta_i = (1+(-1)^{\varepsilon_i})\int_0^{\pi/2}\sin^{\varepsilon_i}\theta_i\ \cos^{\beta_i}\theta_i\ d\theta_i = 0, \tag{17}$$

unless ε_i is even. Similarly,

$$\begin{aligned} &\int_0^{2\pi}\cos^{\varepsilon_{N-1}}\theta_{N-1}\ \sin^{\varepsilon_N}\theta_{N-1}\ d\theta_{N-1} \\ &\quad= (-1)^{\varepsilon_{N-1}+\varepsilon_N}\int_{-\pi}^{\pi}\cos^{\varepsilon_{N-1}}\theta_{N-1}\ \sin^{\varepsilon_N}\theta_{N-1}\ d\theta_{N-1} \\ &\quad= (-1)^{\varepsilon_{N-1}}(1+(-1)^{\varepsilon_N})\int_0^{\pi}\cos^{\varepsilon_{N-1}}\theta_{N-1}\ \sin^{\varepsilon_N}\theta_{N-1}\ d\theta_{N-1} \\ &\quad= (-1)^{\varepsilon_{N-1}+\varepsilon_N}(1+(-1)^{\varepsilon_N})\int_{-\pi/2}^{\pi/2}\sin^{\varepsilon_{N-1}}\theta_{N-1}\ \cos^{\varepsilon_N}\theta_{N-1}\ d\theta_{N-1} \\ &\quad= (1+(-1)^{\varepsilon_{N-1}}+(-1)^{\varepsilon_N}+(1)^{\varepsilon_{N-1}+\varepsilon_N})\times \\ &\quad\times\int_0^{\pi/2}\sin^{\varepsilon_{N-1}}\theta_{N-1}\ \cos^{\varepsilon_N}\theta_{N-1}\ d\theta_{N-1} = 0, \end{aligned} \tag{18}$$

unless ε_{N-1} and ε_N are both even. So assume that for each $1 \leq i \leq N$, $\varepsilon_i = 2t_i$ for some $t_i \in \mathbb{Z}_+$; notice that in this case the weight $w(\boldsymbol{m}_1 + \boldsymbol{m}_2) = 2\sum_{i=1}^N t_i$, we will just call it w until further notice. Then $\beta_i = N - 1 - i + 2\sum_{j=i+1}^N t_j$, and so $(-1)^{\beta_i} = (-1)^{N-1-i}$. Putting things together, we see that $S(\boldsymbol{m}_1, \boldsymbol{m}_2) = 0$ unless $(\boldsymbol{m}_1, \boldsymbol{m}_2) \in E$, in which case combining (16), (17), (18) and using the standard integral formulas, as for instance (5-41) and (5-42) on page 182 of [4], produces

$$\begin{aligned} \alpha_N S(\boldsymbol{m}_1, \boldsymbol{m}_2) &= 2 \prod_{i=1}^{N-1} \left(2 \int_0^{\pi/2} \sin^{2t_i} \theta_i \ \cos^{\beta_i} \theta_i \ d\theta_i \right) \\ &= 2 \left(\prod_{i=1}^{N-1} \frac{\Gamma\left(\frac{2t_i+1}{2}\right) \Gamma\left(\frac{\beta_i+1}{2}\right)}{\Gamma\left(\frac{2t_i+\beta_i}{2} + 1\right)} \right) \end{aligned}$$

$$= 2 \left(\prod_{i=1}^{N-1} \frac{\sqrt{\pi}(2t_i - 1)!!\Gamma\left(\frac{\beta_i+1}{2}\right)}{2^{t_i}\Gamma\left(\frac{2t_i+\beta_i}{2} + 1\right)} \right), \tag{19}$$

where $\frac{2t_{i+1}+\beta_{i+1}}{2} + 1 = \frac{\beta_i+1}{2}$, and so

$$\begin{aligned} \alpha_N S(\boldsymbol{m}_1, \boldsymbol{m}_2) &= \frac{\Gamma\left(\frac{\beta_{N-1}+1}{2}\right)}{\Gamma\left(\frac{2t_1+\beta_1}{2} + 1\right)} 2\pi^{\frac{N-1}{2}} \prod_{i=1}^{N-1} \frac{(2t_i - 1)!!}{2^{t_i}} \\ &= \frac{2\pi^{\frac{N}{2}} \prod_{i=1}^N (2t_i - 1)!!}{2^{w/2}\Gamma\left(\frac{N+w}{2}\right)} \\ &= \begin{cases} \frac{2\pi^{\frac{N}{2}} \prod_{i=1}^N (2t_i-1)!!}{2^{w/2}\left(\frac{N-2+w}{2}\right)!} & \text{if } N \text{ is even} \\ \frac{2\pi^{\frac{N}{2}} \prod_{i=1}^N (2t_i-1)!!}{2^{w/2}\Gamma\left(\frac{N+w}{2}\right)} & \text{if } N \text{ is odd} \end{cases} \end{aligned}$$

$$= \frac{\alpha_N \prod_{i=1}^N (\varepsilon_i - 1)!!}{\prod_{k=1}^{w/2} (N - 2 + 2k)}. \tag{20}$$

The result of Theorem 1.1 now follows by combining (12) and (20).

Remark 2.1. Let K be a number field, and let $M(K)$ be its set of places. For each $v \in M(K)$, write K_v for the completion of K at v; in particular, if v is archimedean, then $K_v = \mathbb{R}$ or $\mathbb{C}$. Write Σ_{N-1}^v for the unit sphere centered at $\boldsymbol{0}$ in K_v^N. A standard norm on the space of homogeneous polynomials of degree M in N variables over K_v is usually defined by

$$\|F\|_v = \begin{cases} \left(\int_{\Sigma_{N-1}^v} |F(\boldsymbol{x})|_v^2 d\boldsymbol{x} \right)^{1/2} & \text{if } v \text{ is archimedean} \\ \sup\left\{ |F(\boldsymbol{x})|_v : \boldsymbol{x} \in \Sigma_{N-1}^v \right\} & \text{if } v \text{ is non-archimedean,} \end{cases} \tag{21}$$

where the measure $d\boldsymbol{x}$ in the archimedean case is normalized so that $\int_{\Sigma_{N-1}^v} d\boldsymbol{x} = 1$ (see, for instance, [1] and [9] for details). In case $K_v = \mathbb{C}$, a well-known identity (see [11], pp. 16-17) provides

$$\|F\|_v^2 = \binom{N+M}{N}^{-1} \sum_{\boldsymbol{m} \in \mathcal{M}(M,N)} \binom{M}{\boldsymbol{m}}^{-1} |c_F(\boldsymbol{m})|_v^2, \tag{22}$$

where $\binom{M}{\boldsymbol{m}} = \frac{M!}{m_1!...m_N!}$. If, on the other hand, $v \nmid \infty$ then we have (see [1]) an identity

$$\|F\|_v = \max_{\boldsymbol{m} \in \mathcal{M}(M,N)} |c_F(\boldsymbol{m})|_v. \tag{23}$$

Our Theorem 1.1 can be viewed as a counterpart of these formulas when $K_v = \mathbb{R}$.

3. Proof of Theorem 1.2

Unless stated otherwise, the notation in this section is as in the statement of Theorem 1.2. Our argument is similar to the proof of Theorem 2.4 of [5]. First we recall a version of Siegel's lemma, which is essentially Theorem 2 of [2].

Theorem 3.1. *Let V be as in Theorem 1.2. Then there exists a basis $f_1, \dots, f_k$ for V consisting of polynomials with integer coefficients so that*

$$\prod_{i=1}^{k} H(f_i) \leq H(V). \tag{24}$$

We will also need a few height-comparison lemmas. The first one is an immediate corollary of Theorem 1 of [14].

Lemma 3.2. *Let U_1 and U_2 be finite-dimensional subspaces of $\mathcal{P}_N(\mathbb{R})$. Then*

$$H(U_1 \cap U_2) \leq H(U_1)H(U_2).$$

Next let $\mathcal{M} = \mathcal{M}(d,N)$, $E = E(d,N)$, and $L = L(d,N) = |\mathcal{M}|$. Let us also write $\mathcal{L}$ for the bilinear form $\mathcal{L}_{d,N}$ and let $\mathfrak{L} = (l_{ij})_{1 \leq i,j \leq L}$ be the coefficient matrix of $\mathcal{L}$, so

$$\mathcal{L}(\boldsymbol{x}, \boldsymbol{y}) = \boldsymbol{x}^t \mathfrak{L} \boldsymbol{y},$$

for each $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^L$. Then diagonal entries of $\mathfrak{L}$ are equal to the corresponding coefficients of $\mathcal{L}$ while the off-diagonal entries are the corresponding coefficients of $\mathcal{L}$ multiplied by $1/2$. Let height of $\mathfrak{L}$, denoted by $H(\mathfrak{L})$, be the maximum of absolute values of entries of $\mathfrak{L}$, and let $H(\mathcal{L})$ be defined in the same way as height of a polynomial is defined in (10). Then we have the following simple bound.

Lemma 3.3. *Let the notation be as above, then*

$$H(\mathfrak{L}) \leq H(\mathcal{L}) = \max_{(\boldsymbol{m}_1, \boldsymbol{m}_2) \in E} P\left(\frac{\boldsymbol{m}_1 + \boldsymbol{m}_2}{2}\right) \leq \max_{\boldsymbol{m} \in \mathcal{M}} P(\boldsymbol{m}) \leq 1. \tag{25}$$

Proof. Notice that

$$\begin{aligned} H(\mathfrak{L}) \leq H(\mathcal{L}) &= \max_{(\boldsymbol{m}_1, \boldsymbol{m}_2) \in E} P\left(\frac{\boldsymbol{m}_1 + \boldsymbol{m}_2}{2}\right) \leq \max_{\boldsymbol{m} \in \mathcal{M}} P(\boldsymbol{m}) \\ &= \max_{\boldsymbol{m} \in \mathcal{M}} \frac{\prod_{i=1}^{N} (2m_i - 1)!!}{\prod_{k=1}^{w(\boldsymbol{m})} (N - 2 + 2k)} \leq \max_{\boldsymbol{m} \in \mathcal{M}} P(w(\boldsymbol{m}), 0, ..., 0) \\ &= \max_{\boldsymbol{m} \in \mathcal{M}} \frac{(2w(\boldsymbol{m}) - 1)!!}{\prod_{k=1}^{w(\boldsymbol{m})} (N - 2 + 2k)} \leq 1, \end{aligned}$$

which proves the lemma. □

Let us write $\| \ \|$ for the usual Euclidean norm on vectors. Let us also write $H(A) = \max_{1 \leq i,j \leq L} |a_{ij}|$ for every $L \times L$ matrix $A = (a_{ij})_{1 \leq i,j \leq L}$ with real coefficients.

Lemma 3.4. *Let $f \in \mathcal{P}_N^d(\mathbb{R})$, and let $A = (a_{ij})_{1 \leq i,j \leq L}$ be an $L \times L$ real matrix. Then*

$$\|\boldsymbol{c}_f^t A\| \leq L^3 H(f) H(A).$$

In particular,

$$\|\boldsymbol{c}_f^t \mathfrak{L}\| \leq L^3 H(f) H(\mathfrak{L}) \leq L^3 H(f), \tag{26}$$

where the second inequality follows by (25).

Proof. Recall that our indexing set $\mathcal{M} = \{\boldsymbol{m}_1, \dots, \boldsymbol{m}_L\}$ is lexicographically ordered, and hence

$$\boldsymbol{c}_f^t A = \left(\sum_{i=1}^L c_f(\boldsymbol{m}_i) a_{i1}, ..., \sum_{i=1}^L c_f(\boldsymbol{m}_i) a_{iL} \right).$$

Then, by Cauchy-Schwarz inequality

$$\begin{aligned} \|\boldsymbol{c}_f^t A\|^2 &= \sum_{j=1}^L \left\| \sum_{i=1}^L c_f(\boldsymbol{m}_i) a_{ij} \right\|^2 \\ &\leq \sum_{j=1}^L \left(\sum_{i=1}^L \|a_{ij}\|^2 \right) \left(\sum_{i=1}^L \|c_f(\boldsymbol{m}_i)\|^2 \right) \\ &= \|A\|^2 \|\boldsymbol{c}_f\|^2 \leq L^6 H(A)^2 H(f)^2, \end{aligned}$$

where $\|A\|^2 = \sum_{i=1}^L \sum_{j=1}^L |a_{ij}|^2$, and so (26) follows. □

The next lemma is a simple version of the well known Brill-Gordan duality principle [7] (also see Theorem 1 on p. 294 of [8]).

Lemma 3.5. *Let $f \in \mathcal{P}_N^d(\mathbb{R})$ be a polynomial with integer coefficients, and let*

$$U = \{t \in \mathcal{P}_N^d(\mathbb{R}) : \boldsymbol{c}_f^t A \boldsymbol{c}_t = 0\},$$

where A is as in Lemma 3.4 above. Let $\gamma(f)$ be the greatest common divisor of the coordinates of the vector $\boldsymbol{c}_f^t A$. Then

$$H(U) = \gamma(f)^{-1} \|\boldsymbol{c}_f^t A\|. \tag{27}$$

We will now state and prove a generalization of Theorem 1.2.

Theorem 3.6. *Let V be as in Theorem 1.2, and let B be a symmetric bilinear form on $\mathcal{P}_N^d(\mathbb{R})$ with $L \times L$ coefficient matrix $\mathcal{B}$, meaning that*

$$B(f,g) = \boldsymbol{c}_f^t \mathcal{B} \boldsymbol{c}_g, \ \forall \ f,g \in \mathcal{P}_N^d(\mathbb{R}).$$

Then there exists an orthogonal basis $g_1, \dots, g_n$ for (V, B) consisting of polynomials with relatively prime integer coefficients so that

$$\prod_{i=1}^n H(g_i) \leq \left(L^3 H(\mathcal{B})\right)^{\frac{n(n+1)}{2}} H(V)^n. \tag{28}$$

Proof. We argue by induction on n. First suppose that $n = 1$, then pick any nonzero polynomial $g_1 \in V$ with relatively prime integer coefficients, and observe that

$$H(g_1) = |\boldsymbol{c}_{g_1}| \leq \|\boldsymbol{c}_{g_1}\| = H(V),$$

where $\| \ \|$ is Euclidean norm. Next assume that $n > 1$ and the theorem is true for all $1 \leq j < n$. Let $0 \neq f_1 \in V$ be a vector guaranteed by Theorem 3.1 so that

$$H(f_1) \leq H(V)^{1/n}. \tag{29}$$

First assume that f_1 is a non-singular point in (V, B). Then

$$V_1 = \{t \in V : B(t, f_1) = 0\} = \{f_1\}^{\perp} \cap V$$

has dimension $n - 1$; here

$$\{f_1\}^{\perp} = \{t \in \mathcal{P}^d_N(\mathbb{R}) : B(t, f_1) = 0\} = \{t \in \mathcal{P}^d_N(\mathbb{R}) : \boldsymbol{c}^t_{f_1} \mathcal{B} \boldsymbol{c}_t = 0\}.$$

By Lemma 3.5, Lemma 3.4, and (29)

$$H\left(\{f_1\}^{\perp}\right) \leq L^3 H(\mathcal{B}) H(V)^{1/n}. \tag{30}$$

Then by Lemma 3.2 and (30) we obtain

$$H(V_1) \leq H\left(\{f_1\}^{\perp}\right) H(V) \leq L^3 H(\mathcal{B}) H(V)^{\frac{n+1}{n}}. \tag{31}$$

Since $\dim_{\mathbb{R}}(V_1) = n - 1$, the induction hypothesis implies that there exists a basis $f_2, \dots, f_n$ for V_1 of polynomials with relatively prime integer coefficients such that $\mathcal{B}(f_i, f_j) = 0$ for all $2 \leq i \neq j \leq n$, and

$$\begin{aligned} \prod_{i=2}^{n} H(f_i) \quad &\leq \quad \left(L^3 H(\mathcal{B})\right)^{\frac{n(n-1)}{2}} H(V_1)^{n-1} \\ &\leq \quad \left(L^3 H(\mathcal{B})\right)^{\frac{n^2+n-2}{2}} H(V)^{\frac{n^2-1}{n}}, \end{aligned} \tag{32}$$

where the last inequality follows by (31). Combining (29) and (32), we see that $f_1, \dots, f_n$ is a basis for V satisfying (28) so that $B(f_i, f_j) = 0$ for all $1 \leq i \neq j \leq n$.

Now assume that f_1 is a singular point in (V, B). Since $f_1 \neq 0,$, it must be true that $c_{f_1}(\boldsymbol{m}_j) \neq 0$ for some $\boldsymbol{m}_j \in \mathcal{M} = \{\boldsymbol{m}_1, \dots \boldsymbol{m}_L\}$. Let

$$T_j = \{t \in \mathcal{P}^d_N(\mathbb{R}) : c_t(\boldsymbol{m}_j) = 0\},$$

and define $V_1 = V \cap T_j$, then $f_1 \notin V_1$, $B(f_1, t) = 0$ for every $t \in V_1$, and

$$H(V_1) \leq H(V) H(T_j) = H(V), \tag{33}$$

by Lemma 3.2, since $H(T_j) = 1$ by Lemma 3.5. Since $\dim_{\mathbb{R}}(V_1) = n - 1$, we can apply induction hypothesis to V_1, and proceed the same way as in the non-singular case above. Since the upper bound of (33) is smaller than that of (31), the result follows. □

Proof of Theorem 1.2. Apply Theorem 3.6 with $B = \mathcal{L}$ and use Lemma 3.3. □

4. Spherical designs

In this section we apply Theorem 1.1 to obtain a criterion for spherical designs. Let $M, N, \mathcal{M}(M,N)$, and $\mathcal{P}_N^M(\mathbb{R})$ be as in section 1. A finite subset S of the unit sphere Σ_{N-1} is called a *spherical M-design* if for every $F(\boldsymbol{X}) \in \mathcal{P}_N^M(\mathbb{R})$,

$$\frac{1}{\alpha_N} \int_{\Sigma_{N-1}} F(\boldsymbol{x})\ d\boldsymbol{x} = \frac{1}{|S|} \sum_{\boldsymbol{y} \in S} F(\boldsymbol{y}). \tag{34}$$

Spherical designs have been extensively studied, in particular in the recent years in connection with lattices, the sphere packing problem, and minimization of Epstein zeta function (see [10] and [3] for details). For instance, recent results of B. Venkov on criteria for spherical designs and their applications are summarized in Chapter 16 of [10]. We use our Theorem 1.1 to give another criterion for a set to be a spherical design in the general spirit of Proposition 16.1.2 and Theorem 16.1.4 of [10].

Theorem 4.1. *Let $S \subset \Sigma_{N-1}$ be a finite set, write $S = \{\boldsymbol{x}_1, \dots, \boldsymbol{x}_k\}$, where $|S| = k$. Let*

$$\mathcal{M}^*(M,N) = \mathcal{M}(M,N) \cap 2\mathcal{M}(M,N).$$

Then S is a spherical M-design if and only if for every $\boldsymbol{m} \in \mathcal{M}(M,N)$,

$$\sum_{j=1}^k \boldsymbol{x}_j^{\boldsymbol{m}} = \begin{cases} kP\left(\frac{\boldsymbol{m}}{2}\right) & \text{if } \boldsymbol{m} \in \mathcal{M}^*(M,N) \\ 0 & \text{if } \boldsymbol{m} \in \mathcal{M}(M,N) \setminus \mathcal{M}^*(M,N). \end{cases} \tag{35}$$

Proof. Let us write $\mathbf{1} \in \mathcal{P}_N^M(\mathbb{R})$ for the constant polynomial equal to 1, i.e.

$$c_{\mathbf{1}}(\mathbf{0}) = 1,\ c_{\mathbf{1}}(\boldsymbol{m}) = 0\ \forall\ \mathbf{0} \neq \boldsymbol{m} \in \mathcal{M}(M,N).$$

Then for each

$$F(\boldsymbol{X}) = \sum_{\boldsymbol{m} \in \mathcal{M}(M,N)} c_F(\boldsymbol{m}) \boldsymbol{X}^{\boldsymbol{m}} \in \mathcal{P}_N^M(\mathbb{R}),$$

we have

$$\frac{1}{\alpha_N} \int_{\Sigma_{N-1}} F(\boldsymbol{x})\ d\boldsymbol{x} = \langle F, \mathbf{1} \rangle = \mathcal{L}_{M,N}(\boldsymbol{c}_F, \boldsymbol{c}_{\mathbf{1}}) = \sum_{\boldsymbol{m} \in \mathcal{M}^*(M,N)} P\left(\frac{\boldsymbol{m}}{2}\right) c_F(\boldsymbol{m}). \tag{36}$$

On the other hand, (34) implies that S is a spherical M-design if and only if

$$\begin{aligned} \frac{1}{\alpha_N} \int_{\Sigma_{N-1}} F(\boldsymbol{x})\ d\boldsymbol{x} &= \frac{1}{k} \sum_{j=1}^k \sum_{\boldsymbol{m} \in \mathcal{M}(M,N)} c_F(\boldsymbol{m}) \boldsymbol{x}_j^{\boldsymbol{m}} \\ &= \sum_{\boldsymbol{m} \in \mathcal{M}(M,N)} \left(\frac{1}{k} \sum_{j=1}^k \boldsymbol{x}_j^{\boldsymbol{m}} \right) c_F(\boldsymbol{m}). \end{aligned} \tag{37}$$

Hence we must have

$$\sum_{\boldsymbol{m} \in \mathcal{M}^*(M,N)} P\left(\frac{\boldsymbol{m}}{2}\right) c_F(\boldsymbol{m}) = \sum_{\boldsymbol{m} \in \mathcal{M}(M,N)} \left(\frac{1}{k} \sum_{j=1}^k \boldsymbol{x}_j^{\boldsymbol{m}} \right) c_F(\boldsymbol{m}), \tag{38}$$

for all $F(\boldsymbol{X}) \in \mathcal{P}_N^M(\mathbb{R})$, which means that the linear forms in the variables $\boldsymbol{c}_F$ on the right and left hand sides of (38) must be equal identically, i.e. their respective coefficients must be equal. Then (35) follows. □

References

[1] E. Bombieri, A. J. Van Der Poorten, and J. D. Vaaler. Effective measures of irrationality for cubic extensions of number fields. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 23(2):211–248, 1996.

[2] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[3] R. Coulangeon. Spherical designs and zeta functions of lattices. *Int. Math. Res. Not.*, Art. ID 49620:16 pp., 2006.

[4] W. H. Fleming. *Functions of several variables*. Addison-Wesley, 1965.

[5] L. Fukshansky. On effective Witt decomposition and Cartan-Dieudonné theorem. *Canad. J. Math.*, 59(6):1284–1300, 2007.

[6] L. Fukshansky. Small zeros of quadratic forms over $\overline{\mathbf{Q}}$. *Int. J. Number Theory*, 4(3):503–523, 2008.

[7] P. Gordan. Uber den grossten gemeinsamen Factor. *Math. Ann.*, 7:443–448, 1873.

[8] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1*. Cambridge Univ. Press, 1947.

[9] M. Laurent and D. Roy. Criteria of algebraic independence with multiplicities and approximation by hypersurfaces. *J. Reine Angew. Math.*, 538:65–114, 2001.

[10] J. Martinet. *Perfect lattices in Euclidean spaces*. Springer-Verlag, 2003.

[11] W. Rudin. *Function theory in the unit ball of* $\mathbb{C}^N$. Springer-Verlag, 1980.

[12] C. L. Siegel. Uber einige Anwendungen diophantischer Approximationen. *Abh. der Preuss. Akad. der Wissenschaften Phys.-math Kl.*, Nr. 1:209–266, 1929.

[13] E. Stein and G. Weiss. *Introduction to Fourier analysis on Euclidean spaces*. Princeton University Press, 1971.

[14] T. Struppeck and J. D. Vaaler. Inequalities for heights of algebraic subspaces and the Thue-Siegel principle. *Analytic number theory (Allerton Park, IL, 1989), Progr. Math.*, 85:493–528, 1990.

[15] A. Thue. Uber Annaherungswerte algebraischer Zahlen. *J. Reine Angew. Math.*, 135:284–305, 1909.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711

E-mail address: lenny@cmc.edu