MULTIVARIATE DISCRETE SPLINES
AND LINEAR DIOPHANTINE EQUATIONS

RONG-QING JIA

ABSTRACT. In this paper we investigate the algebraic properties of multivariate discrete splines. It turns out that multivariate discrete splines are closely related to linear diophantine equations. In particular, we use a solvability condition for a system of linear diophantine equations to obtain a necessary and sufficient condition for the integer translates of a discrete box spline to be linearly independent. In order to understand the local structure of discrete splines we develop a general theory for certain systems of linear partial difference equations. Using this theory we prove that the integer translates of a discrete box spline are locally linearly independent if and only if they are linearly independent.

1. INTRODUCTION

Multivariate discrete splines are closely related to linear diophantine equations. The close relationship between them was first revealed by Dahmen and Micchelli [12].

Let X be an $s \times n$ integer matrix. Given $\alpha \in \mathbb{Z}^s$, consider the following system of linear diophantine equations for $\beta \in \mathbb{Z}^n$,

$$X\beta = \alpha.$$

The number of nonnegative integer solutions β to this system is denoted by $t(\alpha|X)$. It is easily seen that $t(\alpha|X)$ is finite as long as the convex hull of X does not contain 0. It turns out that the sequence $(t(\alpha|X))_{\alpha \in \mathbb{Z}^s}$ is just the so-called *discrete truncated power* associated with X. In [12] Dahmen and Micchelli used the discrete truncated power as a tool to study linear diophantine equations. In particular, they reproved and extended certain results of Stanley [25, Chapter 4] about magic squares. Following their approach, the author in [17] solved a conjecture of Stanley about symmetric magic squares.

Let $H = \operatorname{diag}\{h_1, \dots, h_n\}$ be an $n \times n$ diagonal matrix with $N_j := 1/h_j$ being positive integers, $j = 1, \dots, n$. Such a matrix is called a *scaling matrix*. If all the diagonal entries in H are equal, then H is called a *simple scaling matrix*. Consider the following system of linear equations for $\beta \in \mathbb{Z}^n$,

$$XH\beta = \alpha.$$

Given $\alpha \in XH(\mathbb{Z}^n)$, the number of solutions $\beta \in \prod_{j=1}^{n}\{0, 1, \ldots, N_j - 1\}$ to the above system is denoted by $b_H(\alpha|X)$. It turns out that the sequence $(b_H(\alpha|X))_{\alpha \in XH(\mathbb{Z}^n)}$ is just the so-called *discrete box spline* associated with X and H. The discrete box spline plays an important role in applications such as computer generation of surfaces (see [4 and 8]). In the special case of simple scaling, Dahmen and Micchelli [11] established several algebraic properties for the discrete box spline, and they were wondering whether their results could be generalized to the discrete box spline with respect to arbitrary diagonal scaling. In this paper we shall give a comprehensive investigation of the algebraic properties of the discrete box spline in the general case. Even in the simple scaling case our results are much more satisfactory than the original results of Dahmen and Micchelli in [11]. Our results are based on a study of the solvability of linear diophantine equations. It is remarkable that a condition on the solvability of linear diophantine equations leads us to a necessary and sufficient condition under which the integer translates of a discrete box spline are linearly independent.

In order to study the local linear independence of the integer translates of a discrete box spline we need to understand the local structure of the discrete box spline. The local structure of the box spline was studied by de Boor and Höllig [3], and Dahmen and Micchelli [7]. Their study was related to certain systems of linear partial differential equations. In the discrete case the problem is related to certain systems of linear partial *difference equations* (see [10 and 12]). Following their lead we shall investigate certain systems of linear partial difference equations in a more general setting. This investigation enables us to prove that the integer translates of a discrete box spline are locally linearly independent if and only if they are linearly independent.

The paper is organized as follows: After reviewing some basic properties of multivariate discrete splines in §2 and some conditions on the solvability of linear diophantine equations in §3, we give in §4 a necessary and sufficient condition for the integer translates of a discrete box spline to be linearly independent. Section 5 is devoted to a study of certain linear partial difference equations arising from multivariate discrete splines. In §6 we give a satisfactory description of the local structure of the discrete box spline. The results of §§5 and 6 are then applied to the study of local linear independence in §7. Finally, in §8, we extend the previous results to multivariate discrete exponential splines.

2. Multivariate discrete splines

In this section, we review some basic properties of truncated powers and box splines and their discrete counterparts. Let us first introduce some notation. We view a real (complex) s-vector as a real (complex) $s \times 1$ matrix. Let $\mathbb{R}^s$ ($\mathbb{C}^s$) be the linear space of all real (complex) s-vectors. The *transpose* of a given matrix A is denoted by A^T. The *scalar product* of two vectors $x, y \in \mathbb{C}^s$ is defined to be $x^T y$. By $\mathbb{R}_+$ (resp. $\mathbb{Z}_+$) we denote the set of nonnegative real numbers (resp. nonnegative integers). Recall that a *distribution* on $\mathbb{R}^s$ is a continuous linear functional on the test function space $\mathscr{D}(\mathbb{R}^s)$ (e.g., see [22, Chapter 6]). The space of all distributions on $\mathbb{R}^s$ is denoted by $\mathscr{D}'(\mathbb{R}^s)$. The Fourier-Laplace transform of a test function ϕ is given by

$$\hat{\phi}(\xi) := \int_{\mathbb{R}^s} \phi(x) \exp(-i\xi^T x)\, dx\,, \qquad \xi \in \mathbb{C}^s.$$

The Fourier-Laplace transform of a distribution is defined accordingly.

Let X be an $s \times n$ real matrix. The *truncated power* $T(\cdot|X)$ *associated with* X was introduced by Dahmen [5]. If the convex hull of the column vectors of X does not contain 0, then $T(\cdot|X)$ is the distribution given by the rule

$$(2.1) \qquad T(\cdot|X)\colon \phi \mapsto \int_{\mathbb{R}^n_+} \phi(Xu)\, du\,, \qquad \phi \in \mathscr{D}(\mathbb{R}^s).$$

The *box spline* $B(\cdot|X)$ *associated with* X was introduced by de Boor and DeVore [2], and de Boor and Höllig [3]. It is the distribution given by the rule

$$(2.2) \qquad B(\cdot|X)\colon \phi \mapsto \int_{[0..1)^n} \phi(Xu)\, du\,, \qquad \phi \in \mathscr{D}(\mathbb{R}^s),$$

where $[0..1)$ denotes the interval $\{r \in \mathbb{R}\colon 0 \le r < 1\}$.

In what follows we assume that all the columns of X are nonzero integer vectors. Then it follows from (2.1) and (2.2) that for all $\phi \in \mathscr{D}(\mathbb{R}^s)$,

$$\begin{aligned}
\langle T(\cdot|X)\,, \phi \rangle &= \int_{\mathbb{R}^n_+} \phi(Xu)\, du \\
&= \sum_{\beta \in \mathbb{Z}^n_+} \int_{[0..1)^n} \phi(X(u + \beta))\, du \\
&= \sum_{\beta \in \mathbb{Z}^n_+} \langle B(\cdot - X\beta|X)\,, \phi \rangle.
\end{aligned}$$

Hence, with

$$t(\alpha|X) := \#\{\beta \in \mathbb{Z}^n_+\colon X\beta = \alpha\}\,, \qquad \alpha \in \mathbb{Z}^s,$$

where $\#E$ denotes the number of elements in a set E, we have

$$T(\cdot|X) = \sum_{\alpha \in \mathbb{Z}^s} t(\alpha|X) B(\cdot - \alpha|X).$$

This relation was established by Dahmen and Micchelli in [6]. The sequence

$$t(\cdot|X)\colon \alpha \mapsto t(\alpha|X) \qquad (\alpha \in \mathbb{Z}^s)$$

is called the *discrete truncated power* associated with X.

Let $H = \mathrm{diag}\{h_1, \ldots, h_n\}$ be a scaling matrix and set

$$(2.3) \qquad E_H := (H\mathbb{Z}^n) \cap [0..1)^n = \prod_{j=1}^{n} \{0, h_j, \ldots, 1 - h_j\}.$$

The box spline $B(\cdot|X)$ can be represented in terms of the integer translates of the box spline $B(\cdot|XH)$. More precisely, it follows from (2.2) that for all

$\phi \in \mathscr{D}(\mathbb{R}^s)$,

$$\langle B(\cdot|X), \phi \rangle = \int_{[0..1)^n} \phi(Xu)\, du$$

$$= (\det H) \int_{H^{-1}([0..1)^n)} \phi(XHv)\, dv$$

$$= (\det H) \sum_{\beta \in H^{-1}(E_H)} \int_{[0..1)^n} \phi(XH(v+\beta))\, dv$$

$$= (\det H) \sum_{\beta \in E_H} \langle B(\cdot - X\beta|XH), \phi \rangle.$$

Therefore, with

(2.4) $b_H(\alpha|X) := \#\{\beta \in E_H : X\beta = \alpha\}, \qquad \alpha \in X(E_H)$,

we have

(2.5) $B(\cdot|X) = (\det H) \sum_{\alpha \in X(E_H)} b_H(\alpha|X) B(\cdot - \alpha|XH).$

The sequence

$$b_H(\cdot|X): \alpha \mapsto b_H(\alpha|X) \qquad (\alpha \in X(E_H))$$

is called the *discrete box spline* associated with X and H. When $H = \mathrm{diag}\{h, \ldots, h\}$ is a simple scaling matrix we write $b_h(\cdot|X)$ for $b_H(\cdot|X)$. The discrete box spline was introduced by Cohen, Lyche, and Riesenfeld [4], and by Dahmen and Micchelli [8].

From (2.4) we see that $b_H(\cdot|X)$ is supported on the finite set $X(E_H)$. Thus we may view $b_H(\cdot|X)$ as a linear combination of Dirac measures

$$b_H(\cdot|X) = \sum_{\alpha \in X(E_H)} b_H(\alpha|X)\delta(\cdot - \alpha),$$

where δ is the distribution given by

$$\langle \delta, \phi \rangle = \phi(0), \quad \text{for all } \phi \in \mathscr{D}(\mathbb{R}^s).$$

Then (2.5) may be rewritten as

(2.6) $B(\cdot|X) = (\det H)b_H(\cdot|X) * B(\cdot|XH).$

In particular, in the simple scaling case, we have

(2.7) $B(\cdot|X) = h^n b_h(\cdot|X) * B(\cdot|hX).$

From (2.2) we see that $B(\cdot|hX)$ converges to δ in $\mathscr{D}'(\mathbb{R}^s)$ as $h \to 0$, hence (2.7) yields

$$\lim_{h \to 0} h^n b_h(\cdot|X) = B(\cdot|X).$$

Taking Fourier-Laplace transforms of both sides of (2.6), we obtain

$$B(\cdot|X)\hat{\ } = (\det H)b_H(\cdot|X)\hat{\ } B(\cdot|XH)\hat{\ }.$$

The Fourier-Laplace transform of $B(\cdot|X)$ is well known (see [3]):

(2.8) $B(\cdot|X)\hat{\ }(\xi) = \prod_{j=1}^{n} \dfrac{1 - \exp(-i\xi^T x_j)}{i\xi^T x_j}, \qquad \xi \in \mathbb{C}^s,$

where x_j denotes the jth column of X, $j = 1, \ldots, n$. It follows that

$$(2.9) \qquad b_H(\cdot|X)\hat{}(\xi) = \prod_{j=1}^{n} \frac{1 - \exp(-i\xi^T x_j)}{1 - \exp(-i\xi^T x_j h_j)}, \qquad \xi \in \mathbb{C}^s.$$

3. LINEAR DIOPHANTINE EQUATIONS

Let A be an $m \times n$ integer matrix and b an integer m-vector. In this section we are concerned with the following system of linear diophantine equations

$$(3.1) \qquad\qquad Ay = b.$$

We shall give a necessary and sufficient condition for the system (3.1) to have integer solutions for y. To this end we first recall some concepts from elementary matrix theory.

We use the usual notation for matrix partition. For example, if $a_1, \ldots, a_n$ are the columns of a matrix A, then we may write

$$A = [a_1, \ldots, a_n].$$

An $m \times n$ matrix with $m \leq n$ is said to be of *full row rank* if its rank equals m. An $m \times n$ integer matrix U of full row rank is said to be *unimodular*, if any $m \times m$ submatrix of U has determinant -1, 0 or 1. In particular, a square matrix U with integer entries is unimodular if and only if $|\det U| = 1$. Let A and B be two $m \times n$ integer matrices. We say that B is *left equivalent* to A if $B = UA$ for some $m \times m$ unimodular matrix U; B is *right equivalent* to A if $B = AV$ for some $n \times n$ unimodular matrix V.

For two integers p and q, we use the notation $p \mid q$ to indicate that q is an integer multiple of p. For a set E of integers we denote by g.c.d.(E) the *greatest common divisor* of the integers in E. If $E = \{0\}$, we adopt the convention that g.c.d.$(E) = 0$. Let A be an $m \times n$ integer matrix with $m \leq n$. We denote by d_A the g.c.d. of all $m \times m$ minors of A. For $J \subseteq \{1, \ldots, m\}$, we denote by $A(J)$ the matrix made up of the rows of A indicated by J. From the Laplace expansion of determinants we see that $d_{A(J)} | d_A$.

Lemma 3.1. *Let A and B be two $m \times n$ integer matrices with $m \leq n$. If there is an $n \times n$ integer matrix C such that $B = AC$, then $d_A | d_B$. Moreover, if B is right equivalent to A, then $d_A = d_B$.*

Proof. If $B = AC$ for some integer matrix C, then every column of B is an integer linear combination of the columns of A. Then every $m \times m$ minor of B is an integer linear combination of the $m \times m$ minors of A, which are integer multiples of d_A. This shows that $d_A | d_B$. Moreover, if C is unimodular, then $A = BC^{-1}$ and C^{-1} is also an integer matrix. Hence $d_B | d_A$, and so $d_A = d_B$, as desired. $\square$

The following theorem can be found in [24, p. 10]. However, for reader's convenience, we shall give a proof for it.

Theorem 3.2. *Let A be an integer matrix of full row rank. Then the system (3.1) has an integer solution for y if and only if $d_A = d_{[A,b]}$.*

Proof. Assume that A is an $m \times n$ matrix with $m \leq n$. From the very definition of d_A, we have $d_{[A,b]} | d_A$. Suppose that (3.1) has an integer solution

y. Then
$$[A, b] = A[I, y],$$
where I is the $n \times n$ identity matrix. By Lemma 3.1, $d_A | d_{[A,b]}$. Thus $d_A = d_{[A,b]}$, as desired.

Suppose conversely that $d_A = d_{[A,b]}$. We wish to prove that the system (3.1) has an integer solution for y. Every integer matrix is left equivalent to an integer matrix in *row-echelon form* (e.g., see [23, pp. 294–295]). Thus, A^T is left equivalent to an integer matrix whose last $n - m$ rows are all zero. After taking transpose, we find that there exists an $n \times n$ unimodular matrix U such that the last $n - m$ columns of the matrix $B := AU$ are all zero. It follows that

$$[B, b] = [A, b] \begin{bmatrix} U & 0 \\ 0 & 1 \end{bmatrix},$$

so $[B, b]$ is right equivalent to $[A, b]$. Hence by Lemma 3.1 and the assumption that $d_A = d_{[A,b]}$ we have

$$(3.2) \qquad\qquad d_B = d_A = d_{[A,b]} = d_{[B,b]}.$$

Let C be the matrix made up of the first m columns of B. Since the last $n - m$ columns of B are all zero, we deduce from (3.2) that

$$|\det C| = d_C = d_B = d_{[B,b]} = d_{[C,b]}.$$

By Cramer's rule the vector $C^{-1}b$ is an integer m-vector. Let z be the n-vector of which the first m components are those of $C^{-1}b$ and the remaining ones are zero. Then $y := Uz$ is an integer n-vector and satisfies

$$Ay = AUz = Bz = C(C^{-1}b) = b. \quad \square$$

Corollary 3.3. *The system* (3.1) *has integer solutions for any given integer vector b if and only if $d_A = 1$.*

Proof. The sufficiency of this corollary is a straightforward consequence of Theorem 3.2. For the necessity, let e_j be the jth column of the $m \times m$ identity matrix I ($j = 1, \dots, m$) and for each j let y_j be an integer solution to the system $Ay = e_j$. Set

$$Y = [y_1, y_2, \dots, y_m].$$

Then $AY = I$. By Lemma 3.1 we have $d_A | d_I$. But $d_I = 1$, hence $d_A = 1$. $\quad \square$

The following theorem relaxes the condition in Theorem 3.2 that A is of full row rank.

Theorem 3.4. *Let A be an $m \times n$ integer matrix. The system* (3.1) *has an integer solution for y if and only if the following two conditions hold.*

(i) $\mathrm{rank}(A) = \mathrm{rank}([A, b])$.

(ii) *There exists a subset J of $\{1, \dots, m\}$ such that* $\mathrm{rank}(A) = \mathrm{rank}(A(J)) = \# J$ *and* $d_{A(J)} = d_{[A,b](J)}$.

Proof. From linear algebra we know that the condition (i) is necessary. Theorem 3.2 tells us that the condition (ii) is also necessary. To prove the sufficiency, let J be a subset of $\{1, \dots, m\}$ such that $\mathrm{rank}(A) = \mathrm{rank}(A(J)) = \# J$ and $d_{A(J)} = d_{[A,b](J)}$. Denote by a_j the jth row of A, and by b_j the jth component of b, $j = 1, \dots, m$. By Theorem 3.2 one can find an integer vector y such that

$$(3.3) \qquad\qquad a_j y = b_j$$

for all $j \in J$. By virtue of the condition (i) we have

$$\text{rank}([A, b](J)) \geq \text{rank}(A(J)) = \text{rank}(A) = \text{rank}([A, b]) \geq \text{rank}([A, b](J)).$$

It follows that $\text{rank}([A, b](J)) = \text{rank}([A, b])$. This shows that any row of $[A, b]$ is a linear combination of the rows of $[A, b](J)$. But every row $[a_j, b_j]$ of $[A, b](J)$ satisfies (3.3), hence so does every row $[a_j, b_j]$ of $[A, b]$, $j = 1, \dots, m$. In other words, y satisfies the equation (3.1). $\square$

4. Linear independence of the integer translates of a discrete box spline

In this section we shall investigate the linear independence of the integer translates of the discrete box spline $b_H(\cdot|X)$. Here, $H = \text{diag}\{h_1, \dots, h_n\}$ is a scaling matrix with $N_j = 1/h_j$ being positive integers, $j = 1, \dots, n$, and X is an $s \times n$ integer matrix. Further, we assume that X is of full row rank. We denote by $\mathscr{B}(X)$ the collection of all $s \times s$ invertible submatrices of X.

Let ϕ be a distribution supported on a compact set in $\mathbb{R}^s$. For any $\beta \in \mathbb{Z}^s$, $\phi(\cdot - \beta)$ is called a (multi)integer translate of ϕ. Consider the nullspace $N(\phi)$, i.e., the set of those sequences $f: \mathbb{Z}^s \to \mathbb{C}$ for which

$$\sum_{\beta \in \mathbb{Z}^s} f(\beta)\phi(\cdot - \beta) = 0.$$

If $N(\phi)$ is trivial, i.e., $N(\phi) = \{0\}$, then we say that *the integer translates* $\phi(\cdot - \beta)$ $(\beta \in \mathbb{Z}^s)$ *are linearly independent.*

It was de Boor and Höllig [3] who first studied the linear independence problem for integer translates of a box spline. Given an integer matrix X of full row rank, they showed in [3] that the integer translates of the box spline $B(\cdot|X)$ are linearly independent only if the matrix X is unimodular. Dahmen and Micchelli [7], and Jia [15] independently, proved that this condition is also sufficient. For the discrete case, Dahmen and Micchelli [11] demonstrated that the condition that X is unimodular is also sufficient for the integer translates of $b_h(\cdot|X)$ to be linearly independent, but pointed out that this condition, in general, is not necessary. In this section, we shall give a complete characterization for the linear independence of the integer translates of $b_H(\cdot|X)$ in the general scaling case.

Our results are based on a characterization of the linear independence of the integer translates of a compactly supported distribution. Let

$$K(\phi) := \{z \in (\mathbb{C}\backslash\{0\})^s : (z^\beta)_{\beta \in \mathbb{Z}^s} \in N(\phi)\}.$$

When ϕ is a compactly supported continuous function, Dahmen and Micchelli [7] showed that $N(\phi)$ is trivial if and only if $K(\phi)$ is empty. Ron [21] extended their result to the case in which ϕ could be a compactly supported distribution and observed that for $\theta \in \mathbb{C}^s$, $e^{i\theta} \in K(\phi)$ if and only if $(\hat{\phi}(\theta + 2\pi\alpha))_{\alpha \in \mathbb{Z}^s} = 0$. Thus their result can be stated as follows.

Theorem 4.1. *Let ϕ be a distribution supported on a compact set in $\mathbb{R}^s$. Then the integer translates $\phi(\cdot - \beta)$ $(\beta \in \mathbb{Z}^s)$ are linearly independent if and only if for any $\theta \in \mathbb{C}^s$, there exists some $\alpha \in \mathbb{Z}^s$ such that $\hat{\phi}(\theta + 2\pi\alpha) \neq 0$.*

Let us apply this theorem to the study of linear independence of the integer translates of the discrete box spline $b_H(\cdot|X)$. Recall that the jth column of X

is denoted by x_j, $j = 1, \ldots, n$. The Fourier-Laplace transform of $b_H(\cdot|X)$ was given in (2.9), from which we find that

$$b_H(\cdot|X)\hat{\ }(\theta + 2\pi\alpha) \neq 0$$

if and only if

(4.1) $x_j^T(\theta + 2\pi\alpha) \notin 2\pi(\mathbb{Z}\backslash N_j\mathbb{Z})$

for all $j = 1, \ldots, n$. Given $\theta \in \mathbb{C}^s$, let J be the set of those indices j for which $x_j^T\theta \in 2\pi\mathbb{Z}$. Then for $j \notin J$, (4.1) holds automatically, while for $j \in J$, (4.1) is equivalent to $x_j^T\alpha - b_j \in N_j\mathbb{Z}$ where $b_j = -x_j^T\theta/2\pi$ is an integer. Note that the vector $b = (b_j)_{j\in J}$ lies in $\mathrm{span}(X^T(J))$, the real linear space spanned by the column vectors of $X^T(J)$. On the other hand, given an integer vector $b \in \mathrm{span}(X^T(J))$ one can find $\theta \in \mathbb{C}^s$ such that $X^T(J)\theta = b$. This motivates us to consider the $n \times (s + n)$ integer matrix

(4.2) $A := [X^T, \mathrm{diag}\{N_1, \ldots, N_n\}].$

From the above remarks we conclude that the integer translates of $b_H(\cdot|X)$ are linearly independent if and only if for any nonempty subset J of $\{1, \ldots, n\}$ and any integer vector $b \in \mathrm{span}(X^T(J))$ the system of linear diophantine equations

(4.3) $A(J)\alpha = b$

has an integer solution $\alpha \in \mathbb{Z}^{s+n}$. We are now in a position to prove the main result of this section.

Theorem 4.2. *The following statements are equivalent:*

   (i) *The integer translates $b_H(\cdot - \beta|X)$ ($\beta \in \mathbb{Z}^s$) are linearly independent.*

  (ii) *For any linearly independent set $\{x_j: j \in J\}$ of columns of X, $d_{A(J)} = 1$, where A is the matrix given in (4.2) and $J \subseteq \{1, \ldots, n\}$.*

 (iii) *For any linearly independent set $\{x_j: j \in J\}$ of columns of X,*

(4.4)   g.c.d.$\{d_{X^T(J)}, \text{g.c.d.}\{N_j: j \in J\}\} = 1.$

Proof. (i) $\Rightarrow$ (ii): Suppose that $\{x_j: j \in J\}$ is linearly independent. Then any vector $b \in \mathbb{Z}^J$ lies in $\mathrm{span}(X^T(J))$. Thus, if the integer translates of $b_H(\cdot|X)$ are linearly independent, then given any integer vector $b \in \mathbb{Z}^J$ the system (4.3) has integer solutions. Consequently, by Corollary 3.3 we have $d_{A(J)} = 1$, as desired.

    (ii) $\Rightarrow$ (iii). Denote by $c(J)$ the left-hand side of (4.4). Let B be an $l \times l$ submatrix of $A(J)$, where $l = \#J$. Then either B is a submatrix of $X^T(J)$, or $\det B$ is an integer multiple of some N_k, $k \in J$. In the former case, $d_{X^T}(J)|\det B$, while in the latter case, $N_k|\det B$. Hence in both cases, $c(J)|\det B$. The g.c.d. of the determinants of such submatrices B is $d_{A(J)}$, which is 1 by assumption. This shows that $c(J) = 1$.

    (iii) $\Rightarrow$ (ii). We prove this by induction on $l := \#J$. The case $l = 1$ is trivial. Suppose that $\{x_j: j \in J\}$ is linearly independent, where $J \subseteq \{1, \ldots, n\}$ has cardinality $l > 1$. To an index $j \in J$ and an $(l-1) \times (l-1)$ submatrix of $A(J\backslash j)$ there corresponds an $l \times l$ submatrix B of $A(J)$ such that $\det B = \pm(\det C)N_j$. The g.c.d. of the determinants of all such submatrices C is $d_{A(J\backslash j)}$, which is 1 by the induction hypothesis. This shows that $d_{A(J)}|N_j$ for

all $j \in J$. Moreover, $d_{A(J)}|d_{X^T(J)}$. It follows that $d_{A(J)}|c(J)$. But $c(J) = 1$ by assumption, hence $d_{A(J)} = 1$.

(ii) $\Rightarrow$ (i). We have demonstrated that (i) is true provided that for any nonempty subset J of $\{1, \ldots, n\}$ and any integer vector $b \in \operatorname{span}(X^T(J))$, the system (4.3) has integer solutions. To prove the existence of integer solutions of (4.3), by Theorem 3.2 it suffices to show that $d_{A(J)}|\det B$ for any $l \times l$ submatrix B of $[A(J), b]$, where $l = \# J$. Let B be such a matrix. Then there exists a subset K of J and a square matrix C consisting of some columns of $[X^T(J\backslash K), b(J\backslash K)]$ such that $\det B = \pm(\det C)N_K$ where $N_K := \prod_{k \in K} N_k$. In the case $K = \varnothing$ we adopt the convention that $N_K = 1$. If $\{x_j : j \in J\backslash K\}$ is *linearly dependent*, then the rows of $X^T(J\backslash K)$ are linearly dependent, therefore so are the rows of $[X^T(J\backslash K), b(J\backslash K)]$, because $b \in \operatorname{span}(X^T(J))$. Thus $\det C = 0$, and so $\det B = 0$ in this case. If $\{x_j : j \in J\backslash K\}$ is *linearly independent*, then $d_{A(J\backslash K)} = 1$ by assumption. For any square matrix Q consisting of some columns of $A(J\backslash K)$, one can find an $l \times l$ submatrix P of $A(J)$ such that $\det P = \pm(\det Q)N_K$. Since $d_{A(J)}|\det P$, and since the g.c.d. of the determinants of all such Q is $d_A(J\backslash K) = 1$, we have $d_{A(J)}|N_K$. Thus, in both cases, $d_{A(J)}|\det B$, thereby completing the proof. $\square$

Applying Theorem 4.2 to the simple scaling case, we obtain the following corollary. Note that the sufficiency of this corollary was first proved by Dahmen and Micchelli in [11] under an additional condition.

Corollary 4.3. *Let* N *be a positive integer and* $h = 1/N$. *Then the integer translates of* $b_h(\cdot|X)$ *are linearly independent if and only if* N *is relatively prime to* $|\det B|$ *for any* $B \in \mathscr{B}(X)$.

Proof. The necessity comes from Theorem 4.2 immediately. To prove the sufficiency, we pick a linear independent set $\{x_j : j \in J\}$ of columns of X. Then one can find an element $B \in \mathscr{B}(X)$ so that for every $j \in J$, x_j is a column of B. We have $d_{X^T(J)}|\det B$; hence

$$\text{g.c.d.}\{d_{X^T(J)}, N\}|\text{g.c.d.}\{\det B, N\}.$$

But the latter is 1 by assumption. Thus the sufficiency follows from Theorem 4.2. $\square$

5. PARTIAL DIFFERENCE EQUATIONS

Certain linear partial difference equations arise from the study of box splines. In this section we shall investigate these equations. Such an investigation is essential for our understanding of the local structure of discrete box splines.

For $y \in \mathbb{R}^s$ and a function f defined on $\mathbb{R}^s$, we denote by $D_y f$ the directional derivative of f in the direction y, and by $\nabla_y f$ the corresponding backward difference of f:

$$\nabla_y f := f - f(\cdot - y).$$

More generally, for a multiset Y of vectors in $\mathbb{R}^s$, let

$$D_Y := \prod_{y \in Y} D_y, \qquad \nabla_Y := \prod_{y \in Y} \nabla_y.$$

Here by a *multiset* we mean a set with possible repeated elements (see [25, p. 15]).

Let X be an $s \times n$ real matrix. We also view X as the multiset of its column vectors $x_1, \ldots, x_n$. The support of the box spline $B(\cdot|X)$ is

$$[\![X]\!] := \left\{ \sum_{j=1}^{n} t_j x_j : 0 \leq t_j \leq 1, \text{ all } j \right\},$$

which is also known as the *zonotope* spanned by $x_1, \ldots, x_n$.

The following differentiation formula was given in [3]:

$$(5.1) \qquad D_Y B(\cdot|X) = \nabla_Y B(\cdot|X \setminus Y) \quad \text{for } Y \subseteq X.$$

We assume that X spans $\mathbb{R}^s$ and use the abbreviation

$$\mathscr{Y}(X) := \{Y \subseteq X : \text{span}(X \setminus Y) \neq \mathbb{R}^s\},$$

where $\text{span}(X \setminus Y)$ denotes the linear span of $X \setminus Y$. Further, assume that X is an integer matrix. Then by (5.1) we find that for any $Y \in \mathscr{Y}(X)$, $D_Y B(\cdot|X)$ has its support in

$$(5.2) \qquad c(X) := \bigcup_{Y \in \mathscr{Y}(X)} (\text{span}(X \setminus Y) + \mathbb{Z}^s),$$

which is a union of hyperplanes in $\mathbb{R}^s$. A connected component of $[\![X]\!] \setminus c(X)$ is called a *fundamental X-region* (see [9]). Thus, on each fundamental X-region,

$$(5.3) \qquad D_Y B(\cdot|X) = 0 \quad \text{for all } Y \in \mathscr{Y}(X).$$

This motivates us to consider the following system of linear partial differential equations for $f \in \mathscr{D}'(\mathbb{R}^s)$:

$$D_Y f = 0, \qquad Y \in \mathscr{Y}(X).$$

The solutions to the above system form a linear space, which we shall denote by $D(X)$. It was proved in [3 and 7] that $D(X)$ is a finite dimensional linear space of polynomials provided X spans $\mathbb{R}^s$. From (5.3) we see that on each fundamental X-region, $B(\cdot|X)$ agrees with some element of $D(X)$.

Analogously, consider the following system of linear partial difference equations for $f \in S$, where S denotes the linear space of all mappings from $\mathbb{Z}^s$ to $\mathbb{C}$:

$$\nabla_Y f = 0, \qquad Y \in \mathscr{Y}(X).$$

The solutions to the above system form a linear space, which we shall denote by $\nabla(X)$. It was proved in [10] that $\nabla(X)$ is a finite dimensional space provided X spans $\mathbb{R}^s$.

In what follows, for a subset E of $\mathbb{R}^s$, we set

$$\nu(E|X) := (E - [\![X]\!]) \cap \mathbb{Z}^s.$$

When $E = \{y\}$ we denote this set by $\nu(y|X)$. Note that $\alpha \in \nu(E|X)$ if and only if the support of $B(\cdot - \alpha|X)$ intersects E. By the definition of $\nu(y|X)$, we see that the compact set $y - [\![X]\!]$ is disjoint from $\mathbb{Z}^s \setminus \nu(y|X)$, which is a closed set. Hence there exists an open neighborhood G_y of the origin such that $y - [\![X]\!] + G_y$ is disjoint from $\mathbb{Z}^s \setminus \nu(y|X)$. This shows that $\nu(y|X) =$

$\nu(y + G_y | X)$. More generally, for any nonempty subset E of $\mathbb{R}^s$, there exists an open set G containing E such that $\nu(E|X) = \nu(G|X)$.

Dahmen and Micchelli in [10] proved that for a point $y \in \mathbb{R}^s \backslash c(X)$, any mapping from $\nu(y|X)$ to $\mathbb{C}$ has a unique extension to an element of $\nabla(X)$. They used this result in [12] to study the piecewise structure of discrete truncated powers. This result, however, is not adequate to give a satisfactory description of the local structure of discrete box splines (see [11]). To this end, we extend their results as follows.

Theorem 5.1. *Let* Ω *be a nonempty connected subset of* $\mathbb{R}^s$, *and* X *a multiset of nonzero integer vectors in* $\mathbb{R}^s$ *such that* $\mathrm{span}(X) = \mathbb{R}^s$. *Let* g *be a sequence on* $\nu(\Omega|X)$, *i.e., a mapping from* $\nu(\Omega|X)$ *to* $\mathbb{C}$, *which satisfies the following condition: For any* $Y \in \mathscr{Y}(X)$,

$$(5.4) \qquad \nabla_Y g(\alpha) = 0 \quad \text{for all } \alpha \in \nu(\Omega|X \backslash Y).$$

Then there exists a unique element $f \in \nabla(X)$ *such that* f *agrees with* g *on* $\nu(\Omega|X)$.

Of particular interest is the case in which X is a basis for $\mathbb{R}^s$. In such a case, we can prove the following stronger result concerning nonhomogeneous partial difference equations. For some related results, see [18, §4] and [19].

Theorem 5.2. *Let* V *be an* $s \times s$ *integer matrix whose columns form a basis for* $\mathbb{R}^s$. *Associate to each column vector* $v \in V$ *a sequence* $a_v \in S$. *Then the system of linear partial difference equations*

$$(5.5) \qquad \nabla_v f = a_v, \quad v \in V,$$

has a solution f *in* S *if and only if*

$$(5.6) \qquad \nabla_u a_v = \nabla_v a_u \quad \text{for } u \neq v.$$

Moreover, given a point $y \in \mathbb{R}^s \backslash c(V)$ *and a mapping* g *from* $\nu(y|V)$ *to* $\mathbb{C}$, *the system* (5.5) *has a unique solution* f *satisfying the initial condition*

$$(5.7) \qquad f(\gamma) = g(\gamma) \quad \text{for all } \gamma \in \nu(y|V),$$

provided the compatibility condition (5.6) *holds.*

Proof. Evidently, the compatibility condition (5.6) is necessary for the system (5.5) to have a solution. Let us prove that (5.6) is also sufficient. We observe that $\mathbb{R}^s$ is the disjoint union of $y - V([0..1)^s) + V\beta$, $\beta \in \mathbb{Z}^s$. Since $y \in \mathbb{R}^s \backslash c(V)$, we have

$$(y - V([0..1)^s) + V\beta) \cap \mathbb{Z}^s = \nu(y|V) + V\beta \quad \text{for } \beta \in \mathbb{Z}^s.$$

Hence $\mathbb{Z}^s$ is the disjoint union of $\nu(y|V) + V\beta$, $\beta \in \mathbb{Z}^s$. Thus any $\alpha \in \mathbb{Z}^s$ has a unique representation as follows:

$$(5.8) \qquad \alpha = \gamma + \sum_{v \in V} \beta_v v,$$

where $\gamma \in \nu(y|V)$ and $\beta_v \in \mathbb{Z}$, all $v \in V$. For $m = 0, 1, \ldots$, let

$$G_m := \bigcup_{|\beta| = m} (\nu(y|V) + V\beta),$$

where $|\beta| := \sum_{v \in V} |\beta_v|$. Note that $G_0 = \nu(y|V)$.

Suppose $f \in S$ is a solution to the system (5.5) satisfying (5.7). Then for any $v \in V$ and all $\alpha \in \mathbb{Z}^s$,

(5.9) $$f(\alpha) = f(\alpha - v) + a_v(\alpha),$$

(5.10) $$f(\alpha) = f(\alpha + v) - a_v(\alpha + v).$$

From the representation (5.8) of α we see that if $\alpha \in G_{m+1}$, then $\alpha - v \in G_m$ whenever $\beta_v > 0$, and $\alpha + v \in G_m$ whenever $\beta_v < 0$. Thus the values of f on $\mathbb{Z}^s$ are uniquely determined by (5.9) and (5.10) together with (5.7). This proves the uniqueness of the solution.

Furthermore, (5.9) and (5.10) together with (5.7) give an inductive way to define f on G_m $(m = 0, 1, \ldots)$. We only have to verify that f is well defined. For this, we argue by induction on m. Suppose f is well defined on $\bigcup_{j=0}^m G_j$ and satisfies (5.7), (5.9) and (5.10). We wish to prove that the same is true for G_{m+1}. Pick $\alpha \in G_{m+1}$. Suppose in the representation (5.8) of α, $\beta_u \neq 0$, $\beta_v \neq 0$, for $u, v \in V$, $u \neq v$. We shall only deal with the case $\beta_u > 0$ and $\beta_v > 0$, since the other cases can be treated in the same way. In such a case, $\alpha - u - v \in G_{m-1}$. Since (5.9) is true by the induction hypothesis when α is replaced by $\alpha - u \in G_m$, we obtain

$$
\begin{aligned}
f(\alpha - u) + a_u(\alpha) &= f(\alpha - u - v) + a_v(\alpha - u) + a_u(\alpha) \\
&= f(\alpha - u - v) + a_u(\alpha - v) + a_v(\alpha) \\
&= f(\alpha - v) + a_v(\alpha),
\end{aligned}
$$

where we have used the condition (5.6) to derive the second equality. This finishes the induction step. The sequence f so constructed is a solution to the system (5.5) due to (5.9) and (5.10), and satisfies the initial condition (5.7). $\square$

We are now in a position to prove Theorem 5.1. Our proof follows along the lines of the paper [15].

Proof of Theorem 5.1. The proof proceeds by induction on $\# X$. First, consider the case $\# X = s$, i.e., the columns of X form a basis for $\mathbb{R}^s$. By the remark made before the statement of Theorem 5.1, there exists a connected open set G containing Ω such that $\nu(G|Y) = \nu(\Omega|Y)$ for all $Y \subseteq X$. Thus, without loss of generality, we assume that Ω itself is a connected open set. Pick $y \in \Omega \backslash c(X)$. By Theorem 5.2, there exists an element $f \in \nabla(X)$ such that f agrees with g on $\nu(y|X)$. We shall demonstrate that f agrees with g on $\nu(\Omega|X)$. For this purpose, it suffices to show that f agrees with g on $\nu(z|X)$ for all $z \in \Omega$. Let $z \in \Omega$. Since Ω is open and connected, we can find a finite sequence of points $y_0, \ldots, y_m$ satisfying the following conditions: (a) $y_0 = y$ and $y_m = z$; (b) for every $j \in \{1, \ldots, m\}$, the segment connecting y_{j-1} with y_j lies in Ω; (c) for each $j \in \{1, \ldots, m\}$, $y_j - y_{j-1} = ax$ for some $a \in (-1/2..1/2)$ and $x \in X$. Knowing that f agrees with g on $\nu(y_0|X)$, we shall prove by induction on j that f agrees with g on $\nu(y_j|X)$, $j = 1, \ldots, m$. Let $j > 0$ and assume that f agrees with g on $\nu(y_{j-1}|X)$. Suppose $y_j - y_{j-1} = ax$ for some $x \in X$ and $a \in (-1/2..1/2)$. Pick $\alpha \in \nu(y_j|X)$. Then

(5.11) $$y_j - \alpha \in tx + [\![X \backslash x]\!]$$

for some $t \in [0..1]$. It follows that

(5.12) $$y_{j-1} - \alpha = (y_j - ax) - \alpha \in (t - a)x + [\![X \backslash x]\!].$$

We have $t - a \in (-1/2..3/2)$. If $t - a \in [0..1]$, then α also belongs to $\nu(y_{j-1}|X)$ by (5.12); hence $f(\alpha) = g(\alpha)$ by the induction hypothesis. If $t - a \in (-1/2..0)$, then

$$y_{j-1} - (\alpha - x) \in (1 + t - a)x + [\![X \backslash x]\!] \subseteq [\![X]\!],$$

and therefore $\alpha - x \in \nu(y_{j-1}|X)$. Moreover, $t - a \in (-1/2..0)$ and $t \in [0..1]$ imply $0 \leq t < a$, hence $y_j - tx$ lies in the segment from $y_{j-1} = y_j - ax$ to y_j, and therefore lies in Ω. By (5.11) this shows that $\alpha \in \nu(\Omega|X\backslash x)$. Thus it follows from (5.4) that $g(\alpha) = g(\alpha - x)$. By the induction hypothesis and the fact that $f \in \nabla(X)$ we obtain

$$f(\alpha) = f(\alpha - x) = g(\alpha - x) = g(\alpha).$$

In the case $t - a \in (1..3/2)$, one can prove $f(\alpha) = g(\alpha)$ in the same way. This shows that f agrees with g on $\nu(y_j|X)$ and finishes the induction step. Thus Theorem 5.1 is true for the case $\#X = s$.

Now let $\#X > s$. Suppose the theorem is true for any multiset X' of vectors with $\mathrm{span}(X') = \mathbb{R}^s$ and $\#X' < \#X$. Let $V \subseteq X$ be a basis for $\mathbb{R}^s$.

First, we associate to each $v \in V$ a sequence $a_v \in S$ as follows. If $X\backslash v$ does not span $\mathbb{R}^s$, then we set $a_v = 0$. If $X\backslash v$ spans $\mathbb{R}^s$, then we choose a_v to be an element of $\nabla(X\backslash v)$ such that

$$(5.13) \qquad a_v(\alpha) = \nabla_v g(\alpha) \quad \text{for all } \alpha \in \nu(\Omega|X\backslash v).$$

The existence of a_v is guaranteed by the induction hypothesis, since for any $Y \in \mathscr{Y}(X\backslash v)$ we have $\mathrm{span}(X\backslash v\backslash Y) \neq \mathbb{R}^s$ and hence by (5.4)

$$\nabla_Y \nabla_v g(\alpha) = \nabla_{Y \cup v} g(\alpha) = 0 \quad \text{for all } \alpha \in \nu(\Omega|X\backslash v\backslash Y).$$

Next, consider the system (5.5) with the sequences a_v chosen as above. Let $u, v \in V$, $u \neq v$. If $X\backslash u\backslash v$ spans $\mathbb{R}^s$, then we have

$$\nabla_u a_v(\alpha) = \nabla_u \nabla_v g(\alpha) = \nabla_v \nabla_u g(\alpha) = \nabla_v a_u(\alpha) \quad \text{for all } \alpha \in \nu(\Omega|X\backslash u\backslash v).$$

Therefore by the uniqueness part of the induction hypothesis, $\nabla_v a_u = \nabla_u a_v$ everywhere. If $X\backslash u\backslash v$ does not span $\mathbb{R}^s$, then both $\nabla_v a_u$ and $\nabla_u a_v$ vanish on $\mathbb{Z}^s$. This verifies the compatibility condition (5.6). Thus by Theorem 5.2 there exists a solution $f \in S$ to the system (5.5). We claim that $f \in \nabla(X)$. Indeed, any $Y \in \mathscr{Y}(X)$ contains an element $v \in V$, for otherwise $X\backslash Y$ would contain V, which is a basis of $\mathbb{R}^s$. For this v, $Y\backslash v \in \mathscr{Y}(X\backslash v)$. If $X\backslash v$ does not span $\mathbb{R}^s$, then $a_v = 0$; otherwise $a_v \in \nabla(X\backslash v)$. In both cases we have

$$\nabla_Y f = \nabla_{Y\backslash v} \nabla_v f = \nabla_{Y\backslash v} a_v = 0.$$

This verifies our claim.

Let $\Omega' := \Omega - [\![X\backslash V]\!]$. Then Ω' is also a connected set and $\nu(\Omega'|V) = \nu(\Omega|X)$. Since $\nabla_v f = a_v$ for $v \in V$, it follows from (5.13) that

$$\nabla_v(g - f)(\alpha) = 0 \quad \text{for all } \alpha \in \nu(\Omega|X\backslash v) = \nu(\Omega'|V\backslash v).$$

Hence by what has been proved before one can find an $h \in \nabla(V) \subseteq \nabla(X)$ such that h agrees with $g - f$ on $\nu(\Omega'|V)$. Let $\tilde{f} := f + h$. Then $\tilde{f} \in \nabla(X)$ is an extension of g.

To prove the uniqueness it suffices to show that any $f \in \nabla(X)$ vanishing on $\nu(\Omega|X)$ must be identically zero. Let $v \in V$. If $X\backslash v$ does not span $\mathbb{R}^s$, then $\nabla_v f = 0$; otherwise $\nabla_v f \in \nabla(X\backslash v)$. In the latter case, $\nabla_v f = 0$ on

$\nu(\Omega|X\backslash v)$. Hence by the induction hypothesis we have $\nabla_v f = 0$. Thus $f \in$ $\nabla(V)$ and $f = 0$ on $\nu(\Omega'|V)$. By Theorem 5.2 we conclude that $f = 0$. $\square$

Remark. Our proof of Theorem 5.1 is self-contained. In contrast to Dahmen and Micchelli's method [9], our method does not rely on any information about the volume of the zonotope of $[\![X]\!]$. In fact, it is easily derived from Theorem 5.1 that the volume of $[\![X]\!]$ equals $\dim(\nabla(X))$. Thus one can find the volume of $[\![X]\!]$ by computing the dimension of $\nabla(X)$.

6. THE LOCAL STRUCTURE OF A DISCRETE BOX SPLINE

To study the local structure of a discrete box spline we need to consider partial difference equations on a *lattice*. Here by a lattice in $\mathbb{R}^s$ we mean a free $\mathbb{Z}$-module of dimension s generated by finitely many rational vectors in $\mathbb{R}^s$. (A vector is called a rational vector if all its components are rational numbers.)

Let M be a lattice, and let $S(M)$ be the linear space of all mappings from M to $\mathbb{C}$. Let X be a finite multiset of vectors in M such that $\text{span}(X) = \mathbb{R}^s$. Then for any $x \in X$ the difference operator ∇_x maps $S(M)$ into itself. Consider the system of linear partial difference equations for $f \in S(M)$,

$$\nabla_Y f = 0 \quad \text{for all } Y \in \mathscr{Y}(X).$$

The solutions to this system form a linear subspace of $S(M)$, which we shall denote by $\nabla_M(X)$.

Theorem 6.1. *Let Ω be a nonempty connected subset of $\mathbb{R}^s$, M a lattice in $\mathbb{R}^s$, and X a finite multiset of vectors in M such that $\text{span}(X) = \mathbb{R}^s$. Let g be a mapping from $(\Omega - [\![X]\!]) \cap M$ to $\mathbb{C}$ having the property that for any $Y \in \mathscr{Y}(X)$,*

$$(6.1) \qquad \nabla_Y g(\alpha) = 0 \quad \text{for all } \alpha \in (\Omega - [\![X\backslash Y]\!]) \cap M.$$

Then there exists a unique element $f \in \nabla_M(X)$ such that f agrees with g on $(\Omega - [\![X]\!]) \cap M$.

Proof. The free $\mathbb{Z}$-module M has a basis, say $\{v_1, \ldots, v_s\}$ (e.g., see [14, §IV.2]). Let A be the linear transform on $\mathbb{R}^s$ determined by $Av_j = e_j$, $j = 1, \ldots, s$, where e_j is the jth column of the $s \times s$ identity matrix. Then $AM = \mathbb{Z}^s$ and $AX \subset \mathbb{Z}^s$. The linear transform A induces a mapping $f \mapsto f \circ A^{-1}$ which is an isomorphism between $S(M)$ and S. We observe that $f \in \nabla_M(X)$ if and only if $f \circ A^{-1} \in \nabla(AX)$. Moreover, for any $Y \in \mathscr{Y}(X)$, (6.1) is equivalent to

$$\nabla_{AY}(g \circ A^{-1})(\alpha) = 0 \quad \text{for all } \alpha \in (A\Omega - [\![A(X\backslash Y)]\!]) \cap \mathbb{Z}^s.$$

Thus the present theorem reduces to Theorem 5.1. $\square$

Let now X be an $s \times n$ integer matrix of full row rank with columns $x_1, \ldots, x_n$ and let $H = \text{diag}\{h_1, \ldots, h_n\}$ be a scaling matrix. If x is a column of X, we write h_x for h_j in the case $x = x_j$. Given $Y \subseteq X$, by YH we denote the multiset $\{h_y y : y \in Y\}$. The discrete box spline $b_H(\cdot|Y)$ can be defined in terms of its Fourier transform (see (2.9)):

$$b_H(\cdot|Y)\hat{}(\xi) = \prod_{y \in Y} \frac{1 - \exp(-i\xi^T y)}{1 - \exp(-i\xi^T y h_y)}, \qquad \xi \in \mathbb{R}^s.$$

It follows that

$$(6.2) \qquad \nabla_{YH} b_H(\cdot|X) = \nabla_Y b_H(\cdot|X\backslash Y),$$

which is obtained by comparing the Fourier transforms of both members.

Let M be a lattice in $\mathbb{R}^s$ containing both XH and $\mathbb{Z}^s$. We view the discrete box spline $b_H(\cdot|X)$ as a mapping from M to $\mathbb{C}$ by defining $b_H(\alpha|X) = 0$ for $\alpha \in M \backslash \mathrm{supp}(b_H(\cdot|X))$.

The following theorem describes the local structure of the discrete box spline $b_H(\cdot|X)$.

Theorem 6.2. *For each fundamental X-region Γ, there exists a unique element $f_\Gamma \in \nabla_M(XH)$ which agrees with $b_H(\cdot|X)$ on $(\Gamma - [\![XH]\!]) \cap M$.*

Proof. Any element in $\mathscr{Y}(XH)$ is of the form YH, where $Y \in \mathscr{Y}(X)$. By Theorem 6.1, it suffices to prove that for any $Y \in \mathscr{Y}(X)$,

$$(6.3) \qquad \nabla_{YH} b_H(\alpha|X) = 0 \quad \text{for all } \alpha \in (\Gamma - [\![(X\backslash Y)H]\!]) \cap M.$$

Since Γ is a fundamental X-region, we have $\Gamma \cap c(X) = \varnothing$, where $c(X)$ is given by (5.2). Moreover, $Y \in \mathscr{Y}(X)$ implies that $[\![(X\backslash Y)H]\!] \subset \mathrm{span}(X\backslash Y) \subset c(X)$. Hence

$$\alpha \in (\Gamma - [\![(X\backslash Y)H]\!]) \cap M \Rightarrow \alpha \notin c(X).$$

Since $\nabla_Y b_H(\cdot|X\backslash Y)$ is supported in $c(X)$, it follows that

$$\nabla_Y b_H(\alpha|X\backslash Y) = 0 \quad \text{for all } \alpha \in (\Gamma - [\![(X\backslash Y)H]\!]) \cap M.$$

This together with (6.2) verifies (6.3), as desired. □

7. LOCAL LINEAR INDEPENDENCE

Given a subset Ω of $\mathbb{R}^s$, we observed before that the support of the box spline $B(\cdot - j|X)$ $(j \in \mathbb{Z}^s)$ intersects Ω if and only if $j \in \nu(\Omega|X)$. Thus we say that the integer translates of $B(\cdot|X)$ are *locally linearly independent* if, for any open subset Ω of $\mathbb{R}^s$, the translates $B(\cdot - j|X)$, $j \in \nu(\Omega|X)$, are linearly independent over Ω. It was proved in [9 and 16] independently that the integer translates of $B(\cdot|X)$ are locally linearly independent if and only if they are linearly independent.

One would attempt to define in the same fashion the local linear independence of the integer translates of a discrete box spline. However, such a definition is inappropriate, as the following example illustrates. Let $s = 1$, $X = [1, 1]$, and $h = 1/2$. Then the discrete box spline $b_h(\cdot|X)$ is supported on $\{0, 1/2, 1\}$, and takes value $1/2$ at 0 and 1, and 1 at $1/2$. Let $\Omega = (1/2 .. 3/2)$. Then

$$\mathrm{supp}(b_h(\cdot - j)) \cap \Omega = \begin{cases} \{1\}, & \text{if } j = 0 \text{ or } 1; \\ \varnothing, & \text{otherwise}. \end{cases}$$

Clearly, the integer translates of $b_h(\cdot|X)$ are (globally) linearly independent, but the translates $b_h(\cdot - j|X)$ $(j = 0, 1)$ are linearly *dependent* on Ω. Consequently, we have to modify the definition of local linear independence to suit our purpose.

We point out that for $j \in \mathbb{Z}^s$,

$$(7.1) \qquad \mathrm{supp}(b_H(\cdot - j|X)) \cap (\Omega - [\![XH]\!]) \neq \varnothing$$

if and only if $j \in \nu(\Omega|X)$. Indeed, (7.1) is equivalent to

$$(\mathrm{supp}(b_H(\cdot - j|X)) + [\![XH]\!]) \cap \Omega \neq \varnothing.$$

But the support of $b_H(\cdot - j|X)$ is $j + X(E_H)$, where E_H is given by (2.3); hence

$$\mathrm{supp}(b_H(\cdot - j|X)) + [\![XH]\!] = j + X(E_H) + [\![XH]\!] = j + [\![X]\!],$$

while $(j + [\![X]\!]) \cap \Omega \neq \varnothing$ if and only if $j \in \nu(\Omega|X)$. Thus, we say that the integer translates of $b_H(\cdot|X)$ are locally linearly independent if, for any nonempty subset Ω of $\mathbb{R}^s$, the translates $b_H(\cdot - j|X)$, $j \in \nu(\Omega|X)$, are linearly independent over $\Omega - [\![XH]\!]$.

Theorem 7.1. *The integer translates of $b_H(\cdot|X)$ are locally linearly independent if and only if they are linearly independent.*

Proof. Choosing $\Omega = \mathbb{R}^s$ in the above definition, we see that local linear independence implies linear independence. To prove the converse, we assume that the integer translates of $b_H(\cdot|X)$ are linearly independent and let Ω be a nonempty subset of $\mathbb{R}^s$. We wish to show that the translates $b_H(\cdot - j|X)$ $(j \in \nu(\Omega|X))$ are linearly independent over $(\Omega - [\![XH]\!]) \cap M$, where M is a fixed lattice in $\mathbb{R}^s$ containing both XH and $\mathbb{Z}^s$. As was done in the beginning of §5, one can find an open set G containing Ω such that $\nu(G|X) = \nu(\Omega|X)$ and $(G - [\![XH]\!]) \cap M = (\Omega - [\![XH]\!]) \cap M$. Moreover, we have

$$(7.2) \qquad \nu(G|X) = \nu(G \backslash c(X)|X).$$

Indeed, $j \in \nu(G|X)$ implies that $j + [\![X]\!]$ intersects G; hence one can find $u \in G \backslash c(X)$ such that $j + [\![X]\!] \ni u$. It follows that $j \in \nu(u|X)$. This verifies (7.2). Thus the theorem will be proved if we can show that for any $u \in \mathbb{R}^s \backslash c(X)$, the translates $b_H(\cdot - j|X)$ $(j \in \nu(u|X))$ are linearly independent over $u - [\![XH]\!]$. If this were not true, then there would exist a nonzero mapping g from $\nu(u|X)$ to $\mathbb{C}$ such that

$$(7.3) \qquad \sum_{j \in \nu(u|X)} g(j)b_H(\alpha - j|X) = 0 \quad \text{for all } \alpha \in (u - [\![XH]\!]) \cap M.$$

Since $u \notin c(X)$, the condition (5.4) is vacuously true for $\Omega = \{u\}$; hence by Theorem 5.1, g can be extended to an element of $\nabla(X)$, which we shall still denote by g. Then $g \neq 0$. Let f be the sequence on M given by

$$(7.4) \qquad f(\alpha) = \sum_{j \in \mathbb{Z}^s} g(j)b_H(\alpha - j|X), \quad \alpha \in M.$$

We claim that $f \in \nabla_M(XH)$. Indeed, for any $Y \in \mathscr{Y}(X)$, $\nabla_Y g = 0$, and by (6.2) we have

$$\nabla_{YH} f = \sum_{j \in \mathbb{Z}^s} g(j)\nabla_{YH} b_H(\cdot - j|X)$$

$$= \sum_{j \in \mathbb{Z}^s} g(j)\nabla_Y b_H(\cdot - j|X \backslash Y)$$

$$= \sum_{j \in \mathbb{Z}^s} (\nabla_Y g)(j)b_H(\cdot - j|X \backslash Y) = 0.$$

But for $\alpha \in (u - [\![XH]\!]) \cap M$, $b_H(\alpha - j|X) \neq 0$ if and only if $j \in \nu(u|X)$. Thus it follows from (7.3) and (7.4) that

$$f(\alpha) = 0 \quad \text{for all } \alpha \in (u - [\![XH]\!]) \cap M.$$

Applying Theorem 6.1 to f, we conclude that $f = 0$. Since $g \neq 0$, (7.4) means that the integer translates of $b_H(\cdot|X)$ are linearly dependent, which is a contradiction. $\square$

8. Multivariate discrete exponential splines

In this section we extend the results in the previous sections to discrete exponential box splines. Exponential box splines were introduced by Ron [20]. See [1 and 13] for various properties of them. The following exposition of discrete exponential box splines is taken from [13].

Let X be an $s \times n$ integer matrix of full row rank. Associate to each row x_j of X a complex number μ_j, $j = 1, \ldots, n$, and let μ be the vector in $\mathbb{C}^n$ with μ_j as its jth component. We write μ_x for μ_j in the case $x = x_j$. The exponential box spline $B_\mu(\cdot|X)$ is the distribution given by the rule

$$B_\mu(\cdot|X): \phi \mapsto \int_{[0..1)^n} e^{-\mu^T u} \phi(Xu)\,du, \quad \phi \in \mathscr{D}(\mathbb{R}^s).$$

When $\mu = 0$, $B_\mu(\cdot|X)$ reduces to the box spline $B(\cdot|X)$.

Let $H = \mathrm{diag}\{h_1, \ldots, h_n\}$ be a scaling matrix. The exponential box spline $B_\mu(\cdot|X)$ is related to $B_{H_\mu}(\cdot|XH)$ in the following way:

$$B_\mu(\cdot|X) = (\det H) \sum_{\alpha \in X(E_H)} b_{\mu,H}(\alpha|X) B_{H\mu}(\cdot - \alpha|XH),$$

where E_H is given by (2.3) and

$$(8.1) \qquad b_{\mu,H}(\alpha|X) = \sum_{\beta \in E_H,\, X\beta = \alpha} e^{-\mu^T \beta}, \qquad \alpha \in X(E_H).$$

The sequence $(b_{\mu,H}(\alpha|X))_{\alpha \in X(E_H)}$ is called the *discrete exponential box spline* associated with μ, X, and H. We also view $b_{\mu,H}(\cdot|X)$ as a linear combination of Dirac measures. The Fourier-Laplace transform of $b_{\mu,H}(\cdot|X)$ is computed from (8.1) to be

$$(8.2) \qquad b_{\mu,H}(\cdot|X)\hat{}(\xi) = \prod_{j=1}^{n} \frac{1 - \exp(-(\mu_j + i\xi^T x_j))}{1 - \exp(-h_j(\mu_j + i\xi^T x_j))}, \qquad \xi \in \mathbb{C}^s.$$

For simplicity, we shall investigate linear independence of the integer translates of $b_{\mu,H}(\cdot|X)$ only for the simple scaling case, i.e., $H = \mathrm{diag}\{h, \ldots, h\}$. In this case, we write $b_{\mu,h}(\cdot|X)$ for $b_{\mu,H}(\cdot|X)$, and write N for $1/h$. Then N is a positive integer. Let

$$X_\xi := \{x \in X : \mu_x + i\xi^T x \in 2\pi i N\mathbb{Z}\} \quad \text{for } \xi \in \mathbb{C}^s$$

and

$$A_{\mu,h}(X) := \{\xi \in \mathbb{C}^s : \mathrm{span}(X_\xi) = \mathbb{R}^s\}.$$

Theorem 8.1. *Let X be an $s \times n$ integer matrix of full row rank. The integer translates of the discrete exponential box spline $b_{\mu,h}(\cdot|X)$ are linearly independent if and only if the following two conditions are satisfied:*
   (i) $b_{\mu,h}(\cdot|X)^{\wedge}(\xi) \neq 0$ *for any* $\xi \in A_{\mu,h}(X)$;
   (ii) N *is relatively prime to* $\det V$ *for every* $V \in \mathscr{B}(X)$.

Proof. The sufficiency of this theorem was established by Dahmen and Micchelli (see [13, Corollary 9.4]). To prove the necessity we assume that the integer translates of $b_{\mu,h}(\cdot|X)$ are linearly independent. Then the condition (ii) can be established by an argument analogous to that used in the proof of Theorem 4.2. It remains to prove (i). If (i) were not true, then there would be some $\xi \in A_{\mu,h}(X)$ such that $b_{\mu,h}(\cdot|X)^{\wedge}(\xi) = 0$. We claim that in this case for some $x \in X_{\xi}$ and all $\alpha \in \mathbb{Z}^s$

$$(8.3) \qquad \mu_x + ix^T(\xi + 2\pi\alpha) \in 2\pi i(\mathbb{Z}\backslash N\mathbb{Z}).$$

This in connection with (8.2) would imply that

$$b_{\mu,h}(\cdot|X)^{\wedge}(\xi + 2\pi\alpha) = 0 \quad \text{for all } \alpha \in \mathbb{Z}^s,$$

which, by Theorem 4.1, contradicts the assumption that the integer translates of $b_{\mu,h}(\cdot|X)$ are linearly independent.

Let $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s$. There are two possible cases: Either $x^T\alpha \notin N\mathbb{Z}$ for some $x \in X_{\xi}$, or $x^T\alpha \in N\mathbb{Z}$ for all $x \in X_{\xi}$. In the former case, we have $x^T\alpha \in \mathbb{Z}\backslash N\mathbb{Z}$. But $x \in X_{\xi}$ implies that $\mu_x + ix^T\xi \in 2\pi iN\mathbb{Z}$. Therefore (8.3) follows. In the latter case, $x^T\alpha \in N\mathbb{Z}$ for all $x \in X_{\xi}$. Since $\xi \in A_{\mu,h}(X)$, X_{ξ} spans $\mathbb{R}^s$. Let V be a basis of $\mathbb{R}^s$ contained in X_{ξ}. One can find integers k_x ($x \in V$) such that

$$x^T\alpha = k_x N \quad \text{for all } x \in V.$$

Applying Cramer's rule to the above system of linear equations, we obtain

$$\alpha_r = Nm_r/\det V, \qquad r = 1, \ldots, s,$$

where $m_1, \ldots, m_s$ are integers. Since N is relatively prime to $\det V$, $\det V$ must divide m_r. It follows that $\alpha_r \in N\mathbb{Z}$, $r = 1, \ldots, s$. Moreover, in view of (8.2), $b_{\mu,h}(\cdot|X)^{\wedge}(\xi) = 0$ implies

$$\mu_x + ix^T\xi \in 2\pi i(\mathbb{Z}\backslash N\mathbb{Z}),$$

for some $x \in X$. But $x^T\alpha \in N\mathbb{Z}$, hence (8.3) is valid for this x. $\square$

Let us now consider certain linear partial difference equations arising from exponential box splines. Given μ and X as before, we define $\nabla_{\mu,v}f := \nabla_v f + \mu_v f$ for $v \in X$ and $f \in S$. For $Y \subseteq X$, let $\nabla_{\mu,Y} := \prod_{y \in Y} \nabla_{\mu,y}$. Denote by $\nabla_{\mu}(X)$ the linear space of those sequences $f \in S$ for which

$$\nabla_{\mu,Y}f = 0 \quad \text{for all } Y \in \mathscr{Y}(X).$$

The following theorem can be proved in the same way as Theorem 5.1 was.

Theorem 8.2. *Let Ω be a nonempty connected subset of $\mathbb{R}^s$. Let g be a mapping from $\nu(\Omega|X)$ to $\mathbb{C}$ satisfying the condition that for any $Y \in \mathscr{Y}(X)$,*

$$\nabla_{\mu,Y}g(\alpha) = 0 \quad \text{for all } \alpha \in \nu(\Omega|X\backslash Y).$$

Then there exists a unique element $f \in \nabla_\mu(X)$ such that f agrees with g on $\nu(\Omega|X)$.

Let M be a lattice in $\mathbb{R}^s$ containing both XH and $\mathbb{Z}^s$. Denote by $\nabla_{\mu,M}(XH)$ the linear space of those mappings f from M to $\mathbb{C}$ for which

$$\nabla_{\mu,Y} f = 0 \quad \text{for all } Y \in \mathscr{Y}(XH).$$

The following theorem describes the local structure of $b_{\mu,H}(\cdot|X)$.

Theorem 8.3. *Let M be a lattice in $\mathbb{R}^s$ containing XH and $\mathbb{Z}^s$. For any fundamental X-region Γ, there exists a unique element $f_\Gamma \in \nabla_{\mu,M}(XH)$ which agrees with $b_{\mu,H}(\cdot|X)$ on $(\Gamma - [\![XH]\!]) \cap M$.*

We can define local linear independence of the integer translates of the discrete exponential box spline in the same way as we did for the discrete box spline in §7. We state the following theorem about local linear independence to conclude this paper.

Theorem 8.4. *The integer translates of $b_{\mu,h}(\cdot|X)$ are locally linearly independent if and only if they are linearly independent.*

Acknowledgment

References

1. A. Ben-Artzi and A. Ron, *Translates of exponential box splines and their related spaces*, Trans. Amer. Math. Soc. **309** (1988), 683–710.

2. C. de Boor and R. DeVore, *Approximation by smooth multivariate splines*, Trans. Amer. Math. Soc. **276** (1983), 775–788.

3. C. de Boor and K. Höllig, *B-splines from parallelepipeds*, J. Analyse Math. **42** (1982/83), 99–115.

4. E. Cohen, T. Lyche, and R. Riesenfeld, *Discrete box splines and refinement algorithms*, Computer Aided Geometric Design **1** (1984), 131–148.

5. W. Dahmen, *On multivariate B-splines*, SIAM J. Numer. Anal. **17** (1980), 179–191.

6. W. Dahmen and C. A. Micchelli, *Recent progress in multivariate splines*, Approximation Theory IV (C. K. Chui, L. L. Schumaker, and J. Ward, eds.), Academic Press, New York, 1983, pp. 27–121.

7. ____, *Translates of multivariate splines*, Linear Algebra Appl. **52/53** (1983), 217–234.

8. ____, *Subdivision algorithms for the generation of box spline surfaces*, Computer Aided Geometric Design **1** (1984), 115–129.

9. ____, *On the local linear independence of translates of a box spline*, Studia Math. **82** (1985), 243–263.

10. ____, *On the solution of certain systems of partial difference equations and linear dependence of translates of box splines*, Trans. Amer. Math. Soc. **292** (1985), 305–320.

11. ____, *Algebraic properties of discrete box splines*, Constr. Approx. **3** (1987), 209–221.

12. ____, *The number of solutions to linear diophantine equations and multivariate splines*, Trans. Amer. Math. Soc. **308** (1988), 509–532.

13 ____, *Multivariate E-splines*, Adv. in Math. **76** (1989), 33–93.

14. T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

15. R. Q. Jia, *Linear independence of translates of a box spline*, J. Approx. Theory **40** (1984), 158–160.

16. ____, *Local linear independence of the translates of a box spline*, Constr. Approx. **1** (1985), 175–182.

17. ____, *Symmetric magic squares and multivariate splines*, preprint 1991.

18. R. Q. Jia, S. D. Riemenschneider, and Z. W. Shen, *Dimension of kernels of linear operators*, Amer. J. Math. **114** (1992), 157–184.

19. ____, *Solvability of systems of linear operator equations*, preprint 1991.

20. A. Ron, *Exponential box splines*, Constr. Approx. **4** (1988), 357–378.

21. ____, *A necessary and sufficient condition for the linear independence of the integer translates of a compactly supported distribution*, Constr. Approx. **5** (1989), 297–308.

22. W. Rudin, *Functional analysis*, McGraw-Hill, New York, 1973.

23. C. C. Sims, *Abstract algebra*, Wiley, New York, 1984.

24. Th. Skolem, *Diophantine Gleichungen*, Chelsea, New York, 1950.

25. R. Stanley, *Enumerative combinatorics*, Vol. 1, Wadsworth, Belmont, Calif., 1986.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALBERTA, EDMONTON, CANADA T6G 2G1
E-mail address: jia@xihu.math.ualberta.ca