

REFINEMENT EQUATIONS AND SPLINE FUNCTIONS

Artūras Dubickas

Department of Mathematics and Informatics, Vilnius University,
Naugarduko 24, Vilnius LT-03225, Lithuania
Email: arturas.dubickas@mif.vu.lt
and

Institute of Mathematics and Informatics,
Akademijos 4, Vilnius LT-08663, Lithuania

Zhiqiang Xu

Institute of Computational Math. and Sci. and Eng. Computing,
Academy of Mathematics and System Sciences,
Chinese Academy of Sciences, Beijing, 100080 China
Email: xuzq@lsec.cc.ac.cn

In this paper, we exploit the relation between the regularity of refinable functions with non-integer dilations and the distribution of powers of a fixed number modulo 1, and show the nonexistence of a non-trivial \mathbf{C}^∞ solution of the refinement equation with non-integer dilations. Using this, we extend the results on the refinable splines with non-integer dilations and construct a counterexample to some conjecture concerning the refinable splines with non-integer dilations. Finally, we study the box splines satisfying the refinement equation with non-integer dilation and translations. Our study involves techniques from number theory and harmonic analysis.

Key Words: Refinement equation, multivariate spline, Fourier transform, distribution modulo 1.

Mathematics Subject Classification (2000): 41A15, 05A17, 11J71.

1 Introduction

The *refinement equation* is a functional equation of the form

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j), \quad (1)$$

where $\lambda > 1$ and all the c_j, d_j are real numbers. For the refinement equation (1), the value λ is called a *dilation*, whereas the numbers $\{d_j\}$ are referred to as *translations*. Throughout this paper, we suppose that $d_0 < d_1 < \dots < d_N$ and

define the Fourier transform of $f(x)$ by the formulae

$$\widehat{f}(w) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i w x} dx.$$

Taking the Fourier transform of both sides of (1) we obtain

$$\widehat{f}(w) = H(\lambda^{-1}w) \widehat{f}(\lambda^{-1}w), \quad (2)$$

where $H(w) = \lambda^{-1} \sum_{j=0}^N c_j e^{-2\pi i d_j w}$ is called the *mask polynomial* of the refinement equation. Setting $w = 0$ into (2), we obtain $\sum_{j=0}^N c_j = \lambda$ provided that $\widehat{f}(0) \neq 0$. For simplicity, we shall call the function $f(x)$ satisfying (1) with $\widehat{f}(0) = 1$ a λ -*refinable function* with translations $\{d_j \mid 0 \leq j \leq N\}$. It plays a fundamental role in the construction of compactly supported wavelets and in the study of subdivision schemes in CAGD ([2, 7]).

The existence and regularity of the refinable function are of some interest. These questions were studied on several occasions. In [6], Daubechies and Lagarias showed that up to a scalar multiple the refinement equation (1) has a unique distribution solution f satisfying $\text{supp } f \subset [d_0(\lambda - 1)^{-1}, d_N(\lambda - 1)^{-1}]$. Moreover, they also showed the nonexistence of a \mathbf{C}^∞ -refinable function with compact support in one dimension when the number λ and all the d_j are integers. In [2], Cavaretta et al. extended this result to higher dimensions by a matrix method. When λ is non-integer, ‘the regularity question becomes more complicated and perhaps more interesting from the viewpoint of pure analysis’ [4]. Moreover, the refinable functions with non-integer dilations play an important role in the construction of wavelets with non-integer dilations [1]. Hence, it has attracted a considerable attention. For example, the regularity of Bernoulli convolutions, which are solutions to

$$f(x) = \frac{\lambda}{2} f(\lambda x) + \frac{\lambda}{2} f(\lambda x - 1),$$

was already studied in [12, 14, 22, 25]. In general, one characterizes the regularity of $f(x)$ by considering the decay of $\widehat{f}(w)$. In [4], Dai et al. considered

the uniform decay of the Fourier transform of the refinable functions with non-integer λ . In particular, they give an elegant answer to the following question: *for any given dilation factor $\lambda > 1$ and a positive integer k , can one construct a λ -refinable function $f \in \mathbf{C}^k$?* In this paper, we reverse the question: *can one find a dilation factor $\lambda > 1$ such that there exists a compactly supported λ -refinable function $f \in \mathbf{C}^\infty$?*

This question is interesting for two reasons. First, when λ and all the d_j are integers, the regularity of refinable functions is related to the spectrum of a certain matrix that is constructed by the refinement coefficients c_j . In this case, a negative answer to this question was given in [6]. However, the matrix can only be constructed in the case when λ and all the d_j are integers. Therefore, it is not clear whether there exists a non-integer refinable function which is compactly supported and belongs to \mathbf{C}^∞ . Second, as pointed out in Section 3, the regularity of refinable functions is closely related to the distribution of powers of a fixed number modulo 1, which is a classical problem in number theory. Hence, overlooking the regularity of refinable functions with non-integer dilations one will miss out on the beautiful connection between analysis and number theory.

In this paper, combining the tools of number theory with some results of harmonic analysis, we extend the result of Daubechies and Lagarias to the general case, thus giving a negative answer to the above question when all the d_j are rational numbers and $\lambda > 1$ is a real number.

Theorem 1.1. *Let $d_j \in \mathbf{Q}$ and $\lambda > 1$. Then the refinement equation*

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j),$$

has only the trivial compactly supported \mathbf{C}^∞ solution, i.e., $f \equiv 0$.

The proof of Theorem 1.1 is based on a purely number-theoretic statement

concerning the distribution of powers of a fixed number modulo 1 (see Theorem 3.1 below).

Remark 1. *It should be noted that any translate of a refinable function is refinable. If $f(x)$ satisfies (1) then $g(x) = f(x - b/(\lambda - 1))$ satisfies the refinement equation*

$$g(x) = \sum_{j=0}^N c_j g(\lambda x - d_j + b),$$

which has the same dilation, but a different translation set $\{d_j - b \mid 0 \leq j \leq N\}$.

In Section 2, using Theorem 1.1, we extend the results of [3] concerning the refinable splines with non-integer dilations. We also construct a counterexample to the conjecture about the refinable spline with non-integer translations. The box spline $B(x|M)$ associated with the $s \times n$ matrix M is considered as multivariate generalization of the univariate B spline and have become ‘one of the most dramatic success of multivariate splines’ [10]. It is well-known that the box spline is a λ -refinable function for any positive integer $\lambda > 1$. Hence, box splines play an important role in the subdivision algorithm and wavelets. Moreover, one is also interested in the question when a refinable distribution is essentially a box spline [15, 26]. However, very little is known about box splines satisfying the refinement equations with non-integer dilations. In Section 2, we give a characterization of refinable box splines with non-integer dilations.

The proof of Theorem 1.1 will be given in Section 3. Other proofs concerning refinable splines will be given in Sections 4 and 5.

2 Refinable Spline Functions

In this section, we study one of the most interesting refinable functions, so-called spline function. Firstly, let us recall the definition of spline functions, B splines and box splines.

Definition 2.1. The spline function $f(x)$ is a piecewise polynomial function. More precisely, there are some points $-\infty = x_0 < x_1 < \cdots < x_M < x_{M+1} = +\infty$ and polynomials $P_j(x)$ such that $f(x) = P_j(x)$ for $x \in [x_{j-1}, x_j)$ for each $j = 1, \dots, M+1$.

We call the points x_j , $j = 1, \dots, M$, the *knots* of $f(x)$ and $\max_j \{\deg(P_j)\}$ the *degree* of $f(x)$. Splines are widely used in the approximation theory and in computer aided geometric design. The spline functions satisfying a refinement equation are the most useful ones. A special class of refinable splines are so-called *cardinal B splines* which are defined by induction as

$$B_0(x) = \begin{cases} 1 & \text{if } x \in [0, 1), \\ 0 & \text{otherwise,} \end{cases}$$

and for $k \geq 1$

$$B_k = B_{k-1} * B_0,$$

where $*$ denotes the operation of convolution. By the definition of cardinal B splines, the Fourier transform of B splines is given by the formulae

$$\widehat{B}_k(w) = \left(\frac{1 - \exp(-2\pi i w)}{2\pi i w} \right)^{k+1}.$$

A simple observation is that B_0 is m -refinable for any integer $m > 1$ and satisfies

$$B_0(x) = \sum_{j=0}^{m-1} B_0(mx - j).$$

Since $B_k = B_0 * B_0 * \cdots * B_0$, the B spline B_k is also m -refinable for any integer $m > 1$.

The *box spline* $B(x|M)$ is defined using Fourier transform by the formulae

$$\widehat{B}(\xi|M) = \prod_{j=1}^n \frac{1 - \exp(-2\pi i \xi^T m_j)}{2\pi i \xi^T m_j}, \quad \xi \in \mathbf{C}^s, \quad (3)$$

where $M = (m_1, \dots, m_n)$ is an $s \times n$ real matrix of (full) rank s . In particular, for $M = (1, \dots, 1) \in \mathbf{Z}^{k+1}$, the box spline $B(x|M)$ is reduced to the univariate B spline B_k .

Next, we turn to the general refinable spline function. In [21], Lawton et al. gave the characterization of compactly supported refinable univariate splines $f(x)$ with the additional assumption that the dilation factor is an integer and all the translations are integers. They proved the following theorem:

Theorem 2.2. ([21]) *Suppose that $f(x)$ is a compactly supported spline function of degree d . Then $f(x)$ satisfies the refinement equation*

$$f(x) = \sum_{j=0}^N c_j f(mx - d_j), \quad m > 1, d_j \in \mathbf{Z},$$

if and only if $f(x) = \sum_{n=0}^K p_n B_d(x - n - d_0/(m-1))$ for some $K \geq 0$ and $\{p_n\}$ such that the polynomial $Q(z) = (z-1)^{d+1} \sum_{n=0}^K p_n z^n$ satisfies $Q(z)|Q(z^m)$.

Here and below, $Q(z)|Q(z^m)$ means $Q(z)$ divides $Q(z^m)$, namely, that the quotient $Q(z^m)/Q(z)$ is a polynomial. (In case the notation $a|b$ is used for integers a and b , it means that the quotient b/a is an integer.)

Remark 2. *Theorem 2.2 was extended to higher dimensions by Sun [26]. Moreover, in [21], the authors also gave a characterization of compactly supported univariate refinable splines whose shifts form a Riesz sequence. This was generalized to higher dimensions in [16]. In [5], the authors gave complete characterization of the structure of refinable splines. In [15], Goodman gave a review on refinable splines (including refinable vector splines).*

However, as pointed out in [3], refinable splines do not have to have integer dilations or integer translations. In this case, Dai et al. proved the following theorem:

Theorem 2.3. ([3]) *Suppose that $f(x)$ is a compactly supported spline satisfying the refinement equation*

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j), \quad \sum_{j=0}^N c_j = \lambda \tag{4}$$

such that $\lambda \in \mathbf{R}$ and $d_j \in \mathbf{Z}$. Then

(A) There exists an integer $l > 0$ such that $\lambda^l \in \mathbf{Z}$.

(B) Let k be the smallest positive integer such that $\lambda^k \in \mathbf{Z}$. Then the compactly supported distribution solution $\phi(x)$ of the refinement equation

$$\phi(x) = \sum_{j=0}^n c_j \lambda^{k-1} \phi(\lambda^k x - d_j) \quad (5)$$

is a spline.

(C) There exists a constant α such that the spline $f(x)$ is expressible as

$$f(x) = \alpha \phi(x) * \phi(\lambda^{-1}x) * \cdots * \phi(\lambda^{-(k-1)}x), \quad (6)$$

where $\phi(x)$ is the spline given by (5).

Conversely, if the refinement equation (4) satisfies (A) and (B) then the compactly supported distribution solution f is a spline given in (6).

By Theorem 1.1, we can prove Theorem 2.3 under weaker conditions. A compactly supported function on \mathbf{R} is *piecewise smooth* if there exist an integer M and some real numbers $a_1 < a_2 < \cdots < a_M$ such that $f \in \mathbf{C}^\infty(a_j, a_{j+1})$ for $j = 1, 2, \dots, M-1$ and $\text{supp } f \subset [a_1, a_M]$.

Theorem 2.4. *Let f be a piecewise smooth function with compact support satisfying the refinement equation*

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j), \quad \sum_{j=0}^N c_j = \lambda, \quad (7)$$

where $\lambda > 1$ and $d_j \in \mathbf{Z}$. Then $f(x)$ is a spline function. Hence, (A), (B) and (C) in Theorem 2.3 hold.

To deal with non-integer translations, in [3], the authors raised the following conjecture. Suppose that $f(x)$ is a λ -refinable spline that is λ -indecomposable. Then the translation set for f must be contained in a lattice, i.e., a set of

the form $a\mathbf{Z} + b$ for some $a \neq 0$. Here, we call a λ -refinable spline $f(x)$ λ -*indecomposable* if it cannot be written as the convolution of two λ -refinable splines. As stated in [3], if this conjecture is true, then one can classify all refinable splines by Theorem 2.3. However, we construct a counterexample to the conjecture.

Consider the spline function $f(x) = B(x|(1, \sqrt{5/2}))$. Using the Fourier transform

$$\widehat{f}(w) = \frac{1 - e^{-2\pi i w}}{2\pi i w} \frac{1 - e^{-2\pi i \sqrt{5/2} w}}{2\pi i \sqrt{5/2} w},$$

we have $H(w) = \widehat{f}(\sqrt{10}w)/\widehat{f}(w) = \frac{1}{10} \sum_{j=0}^9 e^{-2\pi i d_j w}$, where the numbers d_0, \dots, d_9 are equal to $0, 1, 2, 3, 4, 5/\sqrt{10}, 1 + 5/\sqrt{10}, 2 + 5/\sqrt{10}, 3 + 5/\sqrt{10}, 4 + 5/\sqrt{10}$, respectively. Hence, the spline $f(x)$ is $\sqrt{10}$ -refinable and satisfies the refinement equation

$$f(x) = \frac{1}{10} \left(\sum_{j=0}^9 f(\sqrt{10}x - d_j) \right)$$

with the translation set $\{0, 1, 2, 3, 4, 5/\sqrt{10}, 1 + 5/\sqrt{10}, 2 + 5/\sqrt{10}, 3 + 5/\sqrt{10}, 4 + 5/\sqrt{10}\}$, which is not contained in a lattice. Moreover, we have the following proposition:

Proposition 2.5. *The univariate box spline $B(x|(1, \sqrt{5/2}))$ is $\sqrt{10}$ -indecomposable.*

The proof of this proposition is non-trivial. It is postponed to Section 4.

Motivated by this counterexample, we shall study the refinable Box spline function with non-integer dilation and translations. It is not only helpful in the study of general refinable splines with non-integer translations, but also useful in understanding of the box splines associated with non-integer matrixes.

It is well-known that the box spline $B(x|M)$, with an additional assumption that M is an $s \times n$ integer matrix, satisfies some higher dimension refinement

equation with an integer $m > 1$, i.e.,

$$B(x|M) = \sum_{j \in \mathbf{Z}^s} c_j^{(m)} B(mx - j|M), \quad (8)$$

where $c_j^{(m)} = m^{s-n} \#\{\alpha \in \mathbf{Z}^n | M\alpha = mj\}$ (see [9]). For this reason, box splines are widely used in computer aided geometry design and wavelets.

The box splines associated with the non-integer matrix are also of interest. In [18, 27], the authors discuss linearly independent integral lattice translates of the box splines associated with a non-integer matrix. Here, we shall characterize the box splines associated to a non-integer matrix satisfying the refinement equation with some non-integer dilation and non-integer translations.

Theorem 2.6. *Suppose that the univariate box spline $B(x|A)$ satisfies the refinement equation*

$$B(x|A) = \sum_{j=0}^N c_j B(\lambda x - d_j|A),$$

where $\lambda > 1$, $\lambda \notin \mathbf{Z}$ and $d_j \in \mathbf{R}$. Then

- (A) *There exists a positive integer l such that $\lambda^l \in \mathbf{Z}$.*
- (B) *For each element $m_0 \in A$, there exists an element $m \in A$ and an integer p such that $m = pm_0/\lambda$.*
- (C) *The vector A contains a sub-vector of the form*

$$(m_0, m_0 p_1 \lambda^{-1}, \dots, m_0 p_{l-1} \lambda^{-l+1}),$$

where l is a positive integer such that $\lambda^l \in \mathbf{Z}$, and $p_j, j = 1, \dots, l-1$, are integers satisfying $p_j | p_{j+1}$, $j = 1, 2, \dots, l-2$, and $p_{l-1} | \lambda^l$.

- (D) *If all the $d_j \in \mathbf{Z}$, then the vector A can be represented as the union of the vectors of the form $(m_0, \lambda m_0, \dots, \lambda^{k-1} m_0)$, where k is the smallest positive integer for which $\lambda^k \in \mathbf{Z}$ and $m_0 \in \mathbf{Z} \setminus 0$.*

Moreover, using the technique of dimensional reduction, we can extend the above results to higher dimensions.

Theorem 2.7. *Suppose that the s -variable box spline $B(x|M)$ satisfies the refinement equation*

$$B(x|M) = \sum_{j=0}^N c_j B(\lambda x - d_j|M),$$

where $\lambda > 1$, $\lambda \notin \mathbf{Z}$ and $d_j \in \mathbf{R}^s$. Then

- (A) *There exists a positive integer l such that $\lambda^l \in \mathbf{Z}$.*
- (B) *For each column m_0 in M , there exists a column m in M and an integer p such that $m = pm_0/\lambda$.*
- (C) *The matrix M contains a sub-matrix of the form*

$$(m_0, m_0 p_1 \lambda^{-1}, \dots, m_0 p_{l-1} \lambda^{-l+1}) \in \mathbf{R}^{s \times l},$$

where l is a positive integer such that $\lambda^l \in \mathbf{Z}$, and $p_j, j = 1, \dots, l-1$, are integers satisfying $p_j | p_{j+1}$, $j = 1, 2, \dots, l-2$, and $p_{l-1} | \lambda^l$.

- (D) *If all the $d_j \in \mathbf{Z}^s$, then the matrix M can be represented as a disjoint union of matrices of the form $(m_0, \lambda m_0, \dots, \lambda^{k-1} m_0) \in \mathbf{R}^{s \times k}$, where k is the smallest positive integer such that $\lambda^k \in \mathbf{Z}$ and $m_0 \in \mathbf{Z}^s \setminus 0$.*

We conclude this section by stating a conjecture which classifies all refinable splines in terms of box splines. A function $P(w)$ is a *real quasi-trigonometric polynomial* if it is of the form of $\sum_{j=0}^N c_j e^{-2\pi i d_j w}$, where $c_j, d_j \in \mathbf{R}$. The real quasi-trigonometric polynomial $P(w)$ is λ -closed if $P(\lambda w)/P(w)$ is also a real quasi-trigonometric polynomial.

Conjecture 2.8. *The spline $f(x)$ satisfies the refinement equation*

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j), \quad \sum_{j=0}^N c_j = \lambda,$$

if and only if $\widehat{f}(w)$, i.e., the Fourier transform of $f(x)$, can be expressed in terms of box splines as follows:

$$\widehat{f}(w) = e^{2\alpha\pi i w} P(w) \widehat{B}(w|A),$$

where α is some constant, $\widehat{B}(w|A)$ is the Fourier transform of a λ -refinable box spline $B(x|A)$, and $P(w)$ is a λ -closed quasi-trigonometric polynomial with $P(0) = 1$.

Remark 3. Throughout the paper, we only consider the case where $\lambda > 0$. However, as pointed out in [3], if $f(x)$ is a λ -refinable spline then it is also a $(-\lambda)$ -refinable spline. Hence, the case, where $\lambda < 0$, can be also studied using the results of this paper.

3 Proof of Theorem 1.1

Before giving the proof of the theorem, we need a theorem of purely number-theoretic nature which plays an important role in the proofs below. For any $x \in \mathbf{R}$, let $\|x\|_{\mathbf{Z}}$ denote the distance from x to the nearest integer in \mathbf{Z} .

Theorem 3.1. Suppose that $\lambda > 1$ and r_1, \dots, r_m are real numbers. Then there exists a positive number ξ and a positive number $c = c(\lambda, r_1, \dots, r_m)$ such that

$$\|\xi\lambda^j - r_i\|_{\mathbf{Z}} \geq c$$

for every $i = 1, \dots, m$ and every $j = 0, 1, 2, \dots$

Proof. For each $\tau > 0$, put

$$S_\tau := \cup_{k \in \mathbf{Z}} \cup_{i=1}^m (k + r_i - \tau, k + r_i + \tau).$$

Then $\|x - r_i\|_{\mathbf{Z}} \geq \tau$ for every $i = 1, \dots, m$ if and only if $x \in \mathbf{R} \setminus S_\tau$. This implies that $\|\xi\lambda^n - r_i\|_{\mathbf{Z}} \geq c$ (for every $i = 1, \dots, m$ and every integer $n \geq 0$) if and only if $\xi \notin S_c \lambda^{-n}$ for $n \geq 0$.

We will construct a sequence of closed nested intervals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$ (where $I_0 \subset (0, 1)$) of length $|I_M| = \sqrt{2\lambda c}/\lambda^{gM}$, where $M = 0, 1, 2, \dots$, such that $\zeta\lambda^n \notin S_c$ for every $\zeta \in I_M$ and every $n = -1, 0, \dots, gM - 1$. (Here, for convenience, we start with $n = -1$, so the final result holds for every $i = 1, \dots, m$

and every $n = -1, 0, 1, \dots$) Also, here $g = g(\lambda, m)$ is the least positive integer satisfying

$$\lambda^g \geq 2(1 + gm).$$

Then, for the common point $\xi \in \cap_{M=0}^{\infty} I_M$, the inequalities $\|\xi \lambda^n - r_i\|_{\mathbf{Z}} \geq c$ will be satisfied for each $i = 1, \dots, m$ and each integer $n \geq -1$.

The proof is by induction on M . We begin with $M = 0$. Evidently, $S_c \cap (0, 1)$ is a union of at most $m + 1$ intervals of total length $2cm$. Thus $S_c \lambda \cap (0, 1)$ is a union of $\leq m + 1$ intervals of total length $2\lambda cm$. The set $(0, 1) \setminus S_c \lambda$ is thus a union of at most $m + 2$ intervals whose lengths sum to a number $\geq 1 - 2\lambda cm$. It contains a closed interval of length $\sqrt{2\lambda c}$ if $1 - 2\lambda cm > (m + 2)\sqrt{2\lambda c}$. So the required closed interval $I_0 \subset (0, 1)$ of length $\sqrt{2\lambda c}$ exists if

$$2\lambda cm + (m + 2)\sqrt{2\lambda c} < 1.$$

This inequality clearly holds if c is less than a certain constant depending on λ and m only. Let us start with this I_0 .

For the induction step $M \mapsto M + 1$, we assume that there exist closed intervals $I_M \subset I_{M-1} \subset \dots \subset I_0$ with required lengths such that $I_M \subset (0, 1) \setminus S_c \lambda^{-n}$ for each $n = -1, 0, \dots, gM - 1$. We need to show that I_M contains a subinterval I_{M+1} of length $\sqrt{2\lambda c}/\lambda^{g(M+1)}$ such that $I_{M+1} \subset (0, 1) \setminus S_c \lambda^{-n}$ for each $n = gM, gM + 1, \dots, g(M + 1) - 1$.

Fix $n \in \{gM, gM + 1, \dots, g(M + 1) - 1\}$. At most $m(1 + \lambda^n |I_M|)$ points of the form $(k + r_i)\lambda^{-n}$, where $k \in \mathbf{Z}$ and $i = 1, \dots, m$, lie in I_M . So the intersection of $S_c \lambda^{-n}$ and I_M consists of at most $m(1 + \lambda^n |I_M|)$ open intervals of length $2c/\lambda^n$ (or less) each plus at most two intervals of length c/λ^n (or less) each at both ends of I_M . As n runs through $gM, \dots, g(M + 1) - 1$ the total length of such intervals is at most

$$\ell_M = \sum_{n=gM}^{g(M+1)-1} (m(1 + \lambda^n |I_M|) 2c\lambda^{-n} + 2c\lambda^{-n}) = \sum_{n=gM}^{g(M+1)-1} (2cm|I_M| + 2c(m+1)\lambda^{-n}).$$

Using $\sum_{n=gM}^{g(M+1)-1} \lambda^{-n} < \sum_{n=gM}^{\infty} \lambda^{-n} = \lambda^{1-gM}/(\lambda-1) = \lambda|I_M|/(\sqrt{2\lambda c}(\lambda-1))$,
we find that

$$\ell_M < 2cmg|I_M| + 2c(m+1)\lambda|I_M|/(\sqrt{2\lambda c}(\lambda-1)) = |I_M|(2cmg + \sqrt{2\lambda c}(m+1)/(\lambda-1)).$$

The remaining part in I_M is of length at least

$$|I_M| - |I_M|(2cmg + \sqrt{2\lambda c}(m+1)/(\lambda-1)) = |I_M|(1 - 2cmg - \sqrt{2\lambda c}(m+1)/(\lambda-1)).$$

It consists of at most

$$1 + \sum_{n=gM}^{g(M+1)-1} m(1 + \lambda^n|I_M|) < 1 + gm + |I_M|\lambda^{g(M+1)}/(\lambda-1) = 1 + gm + \sqrt{2\lambda c}\lambda^g/(\lambda-1)$$

closed (possibly degenerate $[u, u]$) intervals. In order to show that one of these closed intervals is of length at least $\sqrt{2\lambda c}/\lambda^{g(M+1)}$ (so that we can take it as I_{M+1}) we need to check that

$$|I_M|(1 - 2cmg - \sqrt{2\lambda c}(m+1)/(\lambda-1)) \geq |I_{M+1}|(1 + gm + \sqrt{2\lambda c}\lambda^g/(\lambda-1))$$

for c small enough. Indeed, using $|I_{M+1}|/|I_M| = \lambda^{-g}$, we can rewrite this inequality as

$$2cmg + (1 + gm)\lambda^{-g} + \sqrt{2\lambda c}(m+2)/(\lambda-1) < 1.$$

Since $\lambda^g \geq 2(1 + gm)$, the required inequality would follow from

$$2cmg + \sqrt{2\lambda c}(m+2)/(\lambda-1) < 1/2.$$

Clearly, g depends on λ and m only. So this inequality holds for some positive c depending on λ and m only. This completes the proof of the theorem. \square

Remark 4. The $m = 1$ case of this theorem with some explicit constant c was recently obtained by the first named author in [11]. The existence of such a positive number $c := c(\lambda)$ for $m = 1$ was conjectured by Erdős [13] and then proved independently by de Mathan [8] and Pollington [23]. In fact, this result

was proved already by Khintchine in 1926 (see Hilfssatz III in [19]), but then forgotten.

Remark 5. By estimating g from above and by some standard calculations, one can see that the inequalities $2\lambda cm + (m+2)\sqrt{2\lambda c} < 1$ (corresponding to the $M = 0$ case) and $2cmg + \sqrt{2\lambda c}(m+2)/(\lambda-1) < 1/2$ (corresponding to the induction step $M \mapsto M+1$ case) both hold if, for instance, $c := (\lambda-1)^2/(20(m+2)^2\lambda^3)$. This gives an explicit expression for c in Theorem 3.1 for each $\lambda > 1$. The main part for the “difficult” case when λ is close to 1 is the factor $(\lambda-1)^2$. It is essentially the same factor as that in the proof of a similar result obtained by the first named author in the $m = 1$ case [11].

We now can give the proof of Theorem 1.1.

Proof of Theorem 1.1. Suppose that $f \in \mathbf{C}^\infty$ is the solution of

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j)$$

with compact support. Take the Fourier transform of its both sides. We obtain

$$\widehat{f}(\xi) = H(\xi/\lambda)\widehat{f}(\xi/\lambda), \quad (9)$$

where $H(\xi) = \lambda^{-1} \sum_{j=0}^N c_j e^{-2\pi i d_j \xi}$. By Paley and Wiener theorem, $\widehat{f}(\xi)$ is an entire function satisfying $\widehat{f}(\xi) \leq C_k |\xi|^{-k}$ for any positive integer k and $\xi \in \mathbf{R}$, where C_k is a constant.

By (9), for any $M \in \mathbf{N}$, taking the product $\widehat{f}(\lambda\xi)\widehat{f}(\lambda^2\xi)\cdots\widehat{f}(\lambda^M\xi)$, we deduce that

$$|\widehat{f}(\lambda^M\xi)| = |\widehat{f}(\xi)| \prod_{j=0}^{M-1} |H(\lambda^j\xi)|. \quad (10)$$

Suppose that the zero points of $H(\xi)$ on $[0, D_0]$ are $\{r_1, \dots, r_m\}$, where D_0 is the least common multiple of the denominators of d_j . Hence, each nonnegative root of $H(\xi)$ has the form of $r_i + kD_0$ with some $k \in \mathbf{Z}$. By Theorem 3.1, we

can select a positive number ξ_0 such that there exists a $c > 0$ for which

$$\|\xi_0 \lambda^j - r_i - k D_0\|_{\mathbf{Z}} = \|\xi_0 \lambda^j - r_i\|_{\mathbf{Z}} \geq c$$

for every $i = 1, \dots, m$, and every $j = 0, 1, 2, \dots$. Therefore, there exists an $\varepsilon_0 > 0$ such that $H(\lambda^j \xi_0) > \varepsilon_0$ for all j . So, by (10),

$$|\widehat{f}(\lambda^M \xi_0)| \geq |\widehat{f}(\xi_0)| \varepsilon_0^M.$$

Moreover, since $f \in \mathbf{C}^\infty$, for any integer k , we can find a constant C_k such that

$$C_k (\lambda^M \xi_0)^{-k} \geq |\widehat{f}(\lambda^M \xi_0)| \geq |\widehat{f}(\xi_0)| \varepsilon_0^M.$$

It follows that

$$|\widehat{f}(\xi_0)| \leq C_k (\lambda^{-k})^M \xi_0^{-k} \varepsilon_0^{-M}.$$

We can select k so large that $\lambda^{-k} < \varepsilon_0$. Letting $M \rightarrow \infty$, we deduce that $\widehat{f}(\xi_0) = 0$.

Consider the derivative of $\widehat{f}(\xi)$ at ξ_0 . Note that

$$\lambda \widehat{f}'(\lambda \xi) = H(\xi) \widehat{f}'(\xi) + H'(\xi) \widehat{f}(\xi).$$

Since $\widehat{f}(\xi_0) = 0$, we have

$$\lambda \widehat{f}'(\lambda \xi_0) = H(\xi_0) \widehat{f}'(\xi_0).$$

It follows that

$$|\lambda^M \widehat{f}'(\lambda^M \xi_0)| = |\widehat{f}'(\xi_0)| \prod_{j=0}^{M-1} |H(\lambda^j \xi_0)|.$$

Using essentially the same argument, we deduce that $\widehat{f}'(\xi_0) = 0$. By induction, it follows that $\frac{d^k \widehat{f}(\xi)}{d\xi^k} \big|_{\xi=\xi_0} = 0$ for any integer $k \geq 0$. Since $\widehat{f}(\xi)$ is an entire function, this yields $\widehat{f}(\xi) \equiv 0$ and hence $f(x) \equiv 0$. This completes the proof. \square

4 Proofs of Theorem 2.4 and Proposition 2.5

To prove Theorem 2.4, we first prove a lemma, which shows that the regularity of a refinable function can be determined by a certain smoothness property near the endpoints of the support.

Lemma 4.1. *Let f be a compactly supported solution of*

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j), \quad (11)$$

with $\text{supp } f = [A, B]$. Suppose that there exist a $u_0 \in [A, B]$ and $m \in \mathbf{N}$ such that $f^{(m)}(x)$ either does not exist or is discontinuous at u_0 . Then for any $\varepsilon > 0$ there are $x_0 \in [A, A + \varepsilon)$ and $x_1 \in (B - \varepsilon, B]$ such that $f^{(m)}(x)$ either does not exist or is discontinuous at x_0 and x_1 .

Proof. We first consider the case, where $x_0 \in [A, A + \varepsilon)$. Without loss of generality, we may suppose that $d_0 = 0$ (see Remark 1). By the result of [6] (which was stated in Section 1), we have $\text{supp } f \subset [0, d_N(\lambda - 1)^{-1}]$. To prove the lemma, note that

$$f(\lambda^{-1}x) = \sum_{j=0}^N c_j f(x - d_j).$$

Hence

$$f(x) = c_0^{-1} f(\lambda^{-1}x) - c_0^{-1} \sum_{j=1}^N c_j f(x - d_j). \quad (12)$$

Consider the set

$$S := \{y \mid f^{(m)}(x) \text{ either does not exist or is discontinuous at } y\}.$$

Since $f \notin \mathbf{C}^m$, the set S is nonempty. We choose an element $y_1 \in S$. By (12), $\{y_1/\lambda, y_1 - d_1, \dots, y_1 - d_N\} \cap S$ is nonempty. Therefore, we can find a $y_2 \in \{y_1/\lambda, y_1 - d_1, \dots, y_1 - d_N\} \cap S$ such that $0 \leq y_2 \leq y_1$. By induction, there is a sequence y_k such that $y_k \in S$ and $0 \leq y_k \leq y_{k-1}$. If this sequence contains 0, then the lemma is proved. Suppose that 0 is not an element of the

sequence. By the construction of y_k , there exists a k_0 such that $y_{k_0} < d_1$. We have $y_{k_0}/\lambda \in S$, since $y_{k_0} - d_j < 0$ for $1 \leq j \leq N$. Thus, for $k > k_0$, we can take $y_k = y_{k-1}/\lambda$. It is clear that, for any $\varepsilon > 0$, we can find an integer k so large that $x_0 := y_{k_0}/\lambda^k < \varepsilon$.

In case $x_1 \in (B - \varepsilon, B]$, we can suppose that $d_N = 0$. By the same method as above, the conclusion follows. \square

Next, we give the proof of Theorem 2.4.

Proof of Theorem 2.4. We suppose that $f(x)$ is smooth on (a_j, a_{j+1}) where $1 \leq j \leq M$ and $\text{supp} f \subset [a_1, a_{M+1}]$. Without loss of generality, we can suppose that $d_0 = 0$, and hence $a_1 = 0$. Let us define

$$\left(\frac{d}{dx}\right)^k f_-(a_j) = \lim_{x \rightarrow a_j^-} \left(\frac{d}{dx}\right)^k f(x), \quad \left(\frac{d}{dx}\right)^k f_+(a_j) = \lim_{x \rightarrow a_j^+} \left(\frac{d}{dx}\right)^k f(x),$$

and $f_k(a_j) = \left(\frac{d}{dx}\right)^k f_+(a_j) - \left(\frac{d}{dx}\right)^k f_-(a_j)$. We shall prove that either $f_k(a_j) = 0$ or $\lim_{x \rightarrow a_j} \left(\frac{d}{dx}\right)^k f(x)$ exists for all a_j except when $k = k_0$ for some nonnegative integer k_0 . Note that $\text{supp} f \subset [0, a_{M+1}]$. Then the function $f(x)$ satisfies

$$f(x) = c_0 f(\lambda x - d_0) = c_0 f(\lambda x), \quad x \in [0, \varepsilon] \quad (13)$$

for a sufficiently small $\varepsilon > 0$.

We claim that there exists a nonnegative integer k_0 such that $f_+^{(k_0)}(0) \neq 0$. For a contradiction, assume that $f_+^{(k)}(0) = 0$ for any nonnegative integer k . Note that $f_-^{(k)}(0) = 0$ for each $k \geq 0$, since $f(x) = 0$ for $x < 0$. So $f^{(k)}(x)|_{x=0}$ exists for any nonnegative integer k . Since $f(x)$ is the piecewise smooth function, there exists a positive number ε_1 such that $f(x) \in \mathbf{C}^\infty[0, \varepsilon_1)$. According to Lemma 4.1, we have $f(x) \in \mathbf{C}^\infty$. But then Theorem 1.1 implies that $f(x) \equiv 0$, a contradiction.

According to (13), we have $f_+^{(k_0)}(0) = c_0 \lambda^{k_0} f_+^{(k_0)}(0)$. But $f_+^{(k_0)}(0) \neq 0$, so $c_0 = \lambda^{-k_0}$. By (13), we conclude that $f(x) = \lambda^{-k_0} f(\lambda x)$ on $[0, \varepsilon]$. A simple

calculation shows that

$$f_+^{(k)}(0) = \lambda^{k-k_0} f_+^{(k)}(0) \text{ for any } k \in \mathbf{Z}_+.$$

Clearly, $\lambda \neq 1$ yields that $f_+^{(k)}(0) = 0$ for $k \neq k_0$. Note that $f_-^{(k)}(0) = 0$ for any nonnegative integer k . Accordingly, $\lim_{x \rightarrow 0} f^{(k)}(x)$ exists for $k \neq k_0$. By Lemma 4.1, $\lim_{x \rightarrow a_j} f^{(k)}(x)$ exists for all a_j if $k \neq k_0$. Put $g(a_j) = \lim_{x \rightarrow a_j} f^{(k_0+1)}(x)$ and $g(x) = f^{(k_0+1)}(x)$ for $x \neq a_j$. We will show that $g(x)$ satisfies the following refinement equation

$$g(x) = \lambda^{k_0+1} \sum_{j=0}^N c_j g(\lambda x - d_j).$$

Fix $x_0 \in \mathbf{R}$. If $\{x_0, \lambda x_0 - d_j, j = 1, \dots, N\} \cap \{a_j, j = 1, \dots, M+1\} = \emptyset$, by taking the $(k_0 + 1)$ -th derivative at x_0 on both sides of

$$f(x) = \sum_{j=0}^N c_j f(\lambda x - d_j),$$

we obtain

$$g(x_0) = \lambda^{k_0+1} \sum_{j=0}^N c_j g(\lambda x_0 - d_j). \quad (14)$$

Let us consider the remaining case when the intersection of two sets is non-empty. Without loss of generality, we may suppose that

$$\{x_0, \lambda x_0 - d_j, j = 1, \dots, N\} \cap \{a_j, j = 1, \dots, M+1\} = \{x_0, \lambda x_0 - d_j, j = 1, \dots, N_0\}$$

with an integer N_0 . Select an $\varepsilon > 0$ such that

$$(x_0 - \varepsilon, x_0) \cap \{a_j, j = 1, \dots, M+1\} = \emptyset$$

and $(\lambda x_0 - d_k - \lambda \varepsilon, \lambda x_0 - d_k) \cap \{a_j, j = 1, \dots, M+1\} = \emptyset$, for $k = 1, \dots, N$.

Hence $f(x), f(\lambda x - d_j) \in \mathbf{C}^\infty(x_0 - \varepsilon, x_0)$, where $j = 1, \dots, N$. Then, for $x \in (x_0 - \varepsilon, x_0)$, we have

$$g(x) - \lambda^{k_0+1} \sum_{j=0}^{N_0} c_j g(\lambda x - d_j) = \lambda^{k_0+1} \sum_{j=N_0+1}^N c_j g(\lambda x - d_j). \quad (15)$$

By taking the limits on both sides of (15), and noting that

$$\lim_{x \rightarrow x_0 -} \lambda^{k_0+1} \sum_{j=N_0+1}^N c_j g(\lambda x - d_j) = \lambda^{k_0+1} \sum_{j=N_0+1}^N c_j g(\lambda x_0 - d_j)$$

and

$$\lim_{x \rightarrow x_0 -} (g(x) - \lambda^{k_0+1} \sum_{j=0}^{N_0} c_j g(\lambda x - d_j)) = g(x_0) - \lambda^{k_0+1} \sum_{j=0}^{N_0} c_j g(\lambda x_0 - d_j),$$

we conclude that

$$g(x_0) = \lambda^{k_0+1} \sum_{j=0}^N c_j g(\lambda x_0 - d_j).$$

Combining the results above, we arrive to the equality

$$g(x) = \lambda^{k_0+1} \sum_{j=0}^N c_j g(\lambda x - d_j), \text{ for all } x \in \mathbf{R}.$$

Next, by Theorem 1.1, we obtain that $g(x) \equiv 0$, since the function $g \in \mathbf{C}^\infty$ is compactly supported. Using $f^{(k_0+1)}|_{(a_j, a_{j+1})}(x) = g|_{(a_j, a_{j+1})}(x) \equiv 0$, we conclude that $f(x)$ is a spline function. \square

Now, we begin the proof of Proposition 2.5. For this, we shall give some definitions (see also [3]) and a lemma. The functions of the form $G(w) = \sum_{j=0}^N a_j e^{-2\pi i b_j w}$ are referred to as *quasi-trigonometric polynomials*, where $a_j \in \mathbf{C}$, $a_j \neq 0$ and $b_j \in \mathbf{R}$ such that $b_0 < b_1 < \dots < b_N$. In case $b_j \in \mathbf{Z}$, such polynomials are simply trigonometric polynomials. If $b_0 = 0$, $G(w)$ is called a *normalized quasi-trigonometric polynomial*. For the quasi-trigonometric polynomial $G(w)$, one can write

$$G(w) = e^{-2\pi i r_1 w} G_1(w) + e^{-2\pi i r_2 w} G_2(w) + \dots + e^{-2\pi i r_l w} G_l(w), \quad (16)$$

where each G_j is a trigonometric polynomial and $0 \leq r_1 < \dots < r_l < 1$ are distinct. It is easy to see that up to a permutation of terms this decomposition is unique and we shall call (16) the *standard decomposition* of $G(w)$. Moreover, as in [3], we write $\mathbf{A}_G(w) := \sum_{j=0}^H c_j e^{-2\pi i k_j w}$ for the greatest common divisor

of the trigonometric polynomials $\{G_j\}$ normalized so that $k_0 = 0, c_0 = 1$ and $k_j \geq 0$ are distinct. It is easy to see that $\mathbf{A}_G(w) = \alpha e^{-2\pi i j w} G(w)$ for some constant α and an integer j , if and only if, $G(w)$ is a trigonometric polynomial. Then we have

Lemma 4.2. *Suppose that two normalized quasi-trigonometric polynomials G_1 and G_2 satisfy the equality $G_1(w)G_2(w) = R(w)(1 - e^{-2\pi i w})$, where $R(w) = 1 + \sum_{j=1}^N a_j e^{-2\pi i b_j w}$ and $0 < b_1 < b_2 < \dots < b_n$ are irrational numbers. Then there exists a positive integer P and a set $S_0 \subset S_1 := \{0, 1, \dots, P-1\}$ such that $G_1(w) = \alpha(w) \prod_{j \in S_0} (e^{-2\pi i j/P} - e^{-2\pi i w/P})$ and $G_2(w) = \beta(w) \prod_{j \in S_1 \setminus S_0} (e^{-2\pi i j/P} - e^{-2\pi i w/P})$, where α, β are some quasi-trigonometric polynomials.*

Proof. Set $G_P(w) := R(Pw)(1 - e^{-2\pi i Pw})$, $G_{1P}(w) := G_1(Pw)$ and $G_{2P}(w) := G_2(Pw)$ for any integer P . Note that $\mathbf{A}_{G_P}(w) = 1 - e^{-2\pi i Pw}$. We claim that the conclusion holds if there exists a positive integer P such that

$$\mathbf{A}_{G_{1P}}(w)\mathbf{A}_{G_{2P}}(w) = 1 - e^{-2\pi i Pw}. \quad (17)$$

Indeed, on both sides of (17) we have trigonometric polynomials. Setting $z = e^{-2\pi i w}$, we see that $1 - z^P$ is a product of two polynomials in z . So there exists a set $S_0 \subset \{0, 1, \dots, P-1\}$ such that $\mathbf{A}_{G_{1P}}(w) = \prod_{j \in S_0} (e^{-2\pi i j} - e^{-2\pi i w})$, which implies $G_1(w) = \prod_{j \in S_0} (e^{-2\pi i j/P} - e^{-2\pi i w/P})\alpha(w)$, where $\alpha(w)$ is a quasi-trigonometric polynomial. Similarly, we have $G_2(w) = \prod_{j \in S_1 \setminus S_0} (e^{-2\pi i j/P} - e^{-2\pi i w/P})\beta(w)$, where $\beta(w)$ is a quasi-trigonometric polynomial. The claim follows immediately. Hence, in order to complete the proof, it suffices to show that there exists a positive integer P such that $\mathbf{A}_{G_{1P}}(w)\mathbf{A}_{G_{2P}}(w) = 1 - e^{-2\pi i Pw}$.

Write $G_1(w) = \sum_{j=0}^{N_1} a_{1j} e^{-2\pi i b_{1j} w}$ and $G_2(w) = \sum_{j=0}^{N_2} a_{2j} e^{-2\pi i b_{2j} w}$. Then there exists a positive integer, say, P such that each element in the set

$$\{Pb_{1j}, Pb_{2k}, P(b_{1j} - b_{1j'}), P(b_{2k} - b_{2k'}) \mid 0 \leq j, j' \leq N_1, 0 \leq k, k' \leq N_2\}$$

is either integer or irrational. Write

$$R(w)(1 - e^{-2\pi i P w}) = G_{1P}(w)G_{2P}(w). \quad (18)$$

We claim that for each w_0 satisfying $1 - e^{-2\pi i P w_0} = 0$, one has

$$\mathbf{A}_{G_{1P}}(w_0)\mathbf{A}_{G_{2P}}(w_0) = 0.$$

Suppose that there is an element $w_0 \in \{w | 1 - e^{-2\pi i P w} = 0\}$ such that neither $\mathbf{A}_{G_{1P}}(w_0)$ nor $\mathbf{A}_{G_{2P}}(w_0)$ is zero. Write w_0 in the form $j_0/P + I_0$, where $0 \leq j_0 < P$, $j_0, I_0 \in \mathbf{Z}$. Then $\mathbf{A}_{G_{1P}}(j_0/P + I) \neq 0$ and $\mathbf{A}_{G_{2P}}(j_0/P + I) \neq 0$ for every $I \in \mathbf{Z}$.

On the other hand, for each $I \in \mathbf{Z}$, one has $G_{1P}(j_0/P + I)G_{2P}(j_0/P + I) = 0$ (see (18)). It follows that there exists an infinite set $\mathbf{Z}_0 \subset \mathbf{Z}$, such that $G_{1P}(j_0/P + I) = 0$ for each $I \in \mathbf{Z}_0$ (otherwise, one can replace G_{1P} by G_{2P}). According to the choice of P , we have the following decomposition

$$G_{1P}(w) = G_1(Pw) = e^{-2\pi i r_1 w} Q_1(w) + e^{-2\pi i r_2 w} Q_2(w) + \cdots + e^{-2\pi i r_l w} Q_l(w),$$

where $0 \leq r_1 < \cdots < r_l$ are all irrational numbers (except perhaps for $r_1 = 0$) and $Q_j(w)$ are trigonometric polynomials. Moreover, by the choice of P all the differences $r_i - r_j$ are also irrational. Substituting $j_0/P + I$ with $I \in \mathbf{Z}_0$ into $G_{1P}(w)$ we have

$$G_{1P}(j_0/P + I) = \sum_{k=1}^l e^{-2\pi i r_k I} e^{-2\pi i r_k j_0/P} Q_k(j_0/P) = \sum_{k=1}^l e^{-2\pi i r_k I} V_k = 0, \quad (19)$$

where $V_k = e^{-2\pi i r_k j_0/P} Q_k(j_0/P)$ are all independent of I . Suppose that I_1, \dots, I_l are l distinct elements of \mathbf{Z}_0 . (As \mathbf{Z}_0 is infinite, one can find in it l distinct elements.) Let M be the $l \times l$ generalized Vandermonde matrix

$$M = (e^{-2\pi i r_k I_j})_{1 \leq k, j \leq l}.$$

Note that all the r_k , where $k \geq 2$, are irrational and all the differences $r_k - r_j$ are irrational, so the matrix M is non-singular. Taking $I = I_1, \dots, I_l$ in (19),

we obtain $M\mathbf{V} = 0$, where $\mathbf{V} := (V_1, \dots, V_l)^T$. It follows that all $V_j = 0$ and thus $Q_k(j_0/P) = 0$ for every k . Hence $\mathbf{A}_{G_{1P}}(j_0/P + I) = 0$ for each $I \in \mathbf{Z}$, which contradicts to $\mathbf{A}_{G_{1P}}(w_0)\mathbf{A}_{G_{2P}}(w_0) \neq 0$ and proves the claim.

Moreover, for each w_0 such that $\mathbf{A}_{G_{1P}}(w_0)\mathbf{A}_{G_{2P}}(w_0) = 0$, one has $1 - e^{-2\pi i P w_0} = 0$. Indeed, if $1 - e^{-2\pi i P w_0} \neq 0$, then $1 - e^{-2\pi i P(w_0 + I)} \neq 0$ for any $I \in \mathbf{Z}$. So, $R(w_0 + I) = 0$ for each $I \in \mathbf{Z}$. By a similar method, we can show that $R(w) \equiv 0$, which contradicts to the definition of $R(w)$. Similarly, one can show that the roots of $\mathbf{A}_{G_{1P}}(w)\mathbf{A}_{G_{2P}}(w) = 0$ are of multiplicity 1. Hence we have $\mathbf{A}_{G_{1P}}(w)\mathbf{A}_{G_{2P}}(w) = 1 - e^{-2\pi i P w}$. The lemma follows. \square

Proof of Proposition 2.5. Suppose $B(x|(1, \sqrt{5/2})) = f_1(x) * f_2(x)$, where $f_1(x)$ and $f_2(x)$ are splines. By the Fourier transform, we have

$$\widehat{f}_1(w)\widehat{f}_2(w) = \frac{1 - e^{-2\pi i w}}{2\pi i w} \frac{1 - e^{-2\pi i \sqrt{5/2} w}}{2\pi i \sqrt{5/2} w}. \quad (20)$$

By Corollary 2.2 of [3], $\widehat{f}_j(w)$ has the form of $p_j(w)/w$, where $p_j(w)$ is a quasi-trigonometric polynomial with $p_j(0) = 0$ for $j = 1, 2$. Then we have

$$p_1(w)p_2(w) = R(w)(1 - e^{-2\pi i w}),$$

where $R(w) := \frac{1 - e^{-2\pi i \sqrt{5/2} w}}{-4\pi^2 \sqrt{5/2}}$. Lemma 4.2 with S_0 (or $S_1 \setminus S_0$) containing 0 implies that there exists an integer P_1 such that either $p_1(w)$ (or $p_2(w)$) is of the form of $(1 - e^{-2\pi i w/P_1})q_1(w)$, where $q_1(w)$ is a quasi-trigonometrical polynomial. Without loss of generality we may assume that $p_1(w) = (1 - e^{-2\pi i w/P_1})q_1(w)$. Note that $w = 0$ is a root of $p_1(w)$ and $p_2(w)$ of multiplicity 1. Hence, by a similar method as above applied to $w' = \sqrt{5/2}w$, we obtain that $p_2(w)$ is of the form $p_2(w) = (1 - e^{-2\pi i \sqrt{5/2} w/P_2})q_2(w)$, where P_2 is a positive integer and q_2 is a quasi-trigonometrical polynomial.

Set $Z(f) := \{w \mid f(w) = 0, w \in \mathbf{C}\}$ and $Z'(f) := \{w \mid f(\sqrt{10}w) = 0, w \in \mathbf{C}\}$. We claim $Z(p_1) \setminus Z'(p_1) \neq \emptyset$, i.e., there exists $w_0 \in \mathbf{C}$ such that $p_1(w_0) = 0$ but

$p_1(\sqrt{10}w_0) \neq 0$. To prove this, note that

$$Z(p_1/q_1) = \{I_1 P_1 \mid I_1 \in \mathbf{Z}\}$$

and

$$Z'(p_1 q_2) = \{I_2/\sqrt{10}, I_3 P_2/5 + k/5 \mid I_2, I_3 \in \mathbf{Z}, 1 \leq k \leq P_2 - 1\}.$$

We can see that $Z(p_1/q_1) \setminus Z'(p_1 q_2) \neq \emptyset$. Since $Z(p_1/q_1) \subset Z(p_1)$ and $Z'(p_1) \subset Z'(p_1 q_2)$, we derive that $Z(p_1) \setminus Z'(p_1) \neq \emptyset$, where $(Z(p_1/q_1) \setminus Z'(p_1 q_2)) \subset (Z(p_1) \setminus Z'(p_1))$.

Hence there exists a w_0 such that $p_1(w_0) = 0$ while $p_1(\sqrt{10}w_0) \neq 0$. As a result, we see that $p_1(\sqrt{10}w)/p_1(w)$ cannot be a mask polynomial. Thus, f_1 is not $\sqrt{10}$ -refinable. The proposition follows. \square

5 Proofs of Theorem 2.6 and Theorem 2.7

Proof of Theorem 2.6. Let us begin with part (B). Write $A = (m_1, \dots, m_n)$, where $m_j \in \mathbf{R} \setminus 0$. We shall prove that, for each element of A , for instance, m_1 there exists an element $m \in A$ and an integer p such that $m = pm_1/\lambda$.

Consider the Fourier transform

$$\widehat{B}(w|A) = \prod_{j=1}^n \frac{1 - e^{-2\pi i w m_j}}{2\pi i w m_j}.$$

Since $B(x|A)$ satisfies the refinement equation, we have

$$\widehat{B}(\lambda w|A) = p(w)\widehat{B}(w|A), \tag{21}$$

where $p(w)$ is the mask polynomial. Note that

$$p(w) = \frac{\widehat{B}(\lambda w|A)}{\widehat{B}(w|A)} = \lambda^{-n} \prod_{j=1}^n \frac{Q(\lambda m_j w)}{Q(m_j w)},$$

where $Q(w) = 1 - e^{-2\pi i w}$. Put

$$Z_j := \{w \mid Q(m_j w) = 0, w \neq 0\} \text{ and } Z'_j := \{w \mid Q(\lambda m_j w) = 0, w \neq 0\}.$$

Since $p(w)$ is an entire function, one has

$$\bigcup_{j=1}^n Z_j \subset \bigcup_{j=1}^n Z'_j. \quad (22)$$

A simple calculation shows that

$$Z_j := \{I_j/m_j \mid I_j \in \mathbf{Z} \setminus 0\} \text{ and } Z'_j := \{k_j/(m_j\lambda) \mid k_j \in \mathbf{Z} \setminus 0\}.$$

Let us consider Z_1 . Put $J_1 := \{j \mid Z_1 \cap Z'_j \neq \emptyset\}$. By (22), we see that $Z_1 \subset \bigcup_{j \in J_1} Z'_j$. Select an entry in J_1 , say, u . Since $Z_1 \cap Z'_u \neq \emptyset$, there exist $I_1 \in \mathbf{Z} \setminus 0$ and $k_u \in \mathbf{Z} \setminus 0$ such that $I_1/m_1 = k_u/(m_u\lambda)$. Hence, we can find two coprime integers P_{1u}, Q_{1u} such that $m_u = P_{1u}m_1/(Q_{1u}\lambda)$. Similarly, for any index $u \in J_1$, we can find two coprime integers P_{1u}, Q_{1u} such that

$$m_u = P_{1u}m_1/(Q_{1u}\lambda). \quad (23)$$

Note that for each fixed $I_1 \in \mathbf{Z} \setminus 0$ there exist $u \in J_1, k_u \in \mathbf{Z} \setminus 0$ such that

$$\frac{I_1}{m_1} = \frac{k_u}{m_u\lambda} = \frac{k_u Q_{1u}}{m_1 P_{1u}},$$

since $Z_1 \subset \bigcup_{j \in J_1} Z'_j$. Hence, for any $I_1 \in \mathbf{Z} \setminus 0$, there exist $u \in J_1$ and $k_u \in \mathbf{Z} \setminus 0$ such that $k_u/I_1 = P_{1u}/Q_{1u}$, i.e., $k_u = I_1 P_{1u}/Q_{1u}$. So, there exists $u \in J_1$ such that $Q_{1u} \mid I_1$ for any $I_1 \in \mathbf{Z} \setminus 0$.

We claim that one can find a $u_1 \in J_1$ such that $Q_{1u_1} = 1$. Indeed, suppose $Q_{1u} \neq 1$ for each $u \in J_1$. Take $I_1 = \prod_{u \in J_1} |Q_{1u}| + 1$. But then I_1 is not divisible by Q_{1u} for each $u \in J_1$, a contradiction.

Next, by (23), there exists an index u_1 such that

$$m_{u_1} = \frac{P_{1u_1}m_1}{\lambda}.$$

Setting $m := m_{u_1}$ and $p := P_{1u_1}$ we complete the proof of (B).

Consider parts (A) and (C). Using (B), one obtains an infinite sequence u_1, u_2, \dots , such that $m_{u_k} = P_{u_k u_{k-1}} m_{u_{k-1}}/\lambda$, for some $P_{u_k u_{k-1}} \in \mathbf{Z}$, where

$k \geq 2$. Since each index in this sequence is at most n , the sequence contains two equal indices. Without loss of generality, we may suppose that $u_{l+1} = u_1$, where l is a positive integer. Then

$$\begin{aligned}
m_{u_2} &= \frac{1}{\lambda} P_{u_1 u_2} m_{u_1}, \\
m_{u_3} &= \frac{1}{\lambda} P_{u_2 u_3} m_{u_2}, \\
m_{u_4} &= \frac{1}{\lambda} P_{u_3 u_4} m_{u_3}, \\
&\vdots \\
m_{u_l} &= \frac{1}{\lambda} P_{u_{l-1} u_l} m_{u_{l-1}}.
\end{aligned} \tag{24}$$

This yields $\lambda^l = P_{u_1 u_2} \cdots P_{u_{l-1} u_l} \in \mathbf{Z}$, proving part (A). Moreover, by using (24), one can see that $m_{u_2} = m_{u_1} p_1 / \lambda$, $m_{u_3} = m_{u_1} p_2 / \lambda^2, \dots, m_{u_l} = p_{l-1} m_{u_1} / \lambda^{l-1}$, where $p_1 := P_{u_1 u_2}$, $p_2 := p_1 P_{u_2 u_3}, \dots, p_{l-1} := p_{l-2} P_{u_{l-1} u_l}$. Hence $p_j | p_{j+1}$ for $j = 1, 2, \dots, l-2$, and $p_{l-1} | \lambda^l$. Thus the sub-vector $(m_{u_1}, \dots, m_{u_l})$ has the form of $(v, v p_1 \lambda^{-1}, \dots, v p_{l-1} \lambda^{-l+1})$, where $v := m_{u_1}$, proving (C).

It remains to prove (D). Consider the Fourier transform of $B(x|A)$

$$\widehat{B}(w|A) = \prod_{j=1}^n \frac{1 - e^{-2\pi i m_j w}}{2\pi i m_j w}. \tag{25}$$

Since $B(x|A)$ is a λ -refinable spline with integer translations, by Theorem 2.2 and Theorem 2.3, we can write $\widehat{B}(w|A)$ in the form

$$\widehat{B}(w|A) = e^{-2\pi i z_0 w} \prod_{j=0}^{k-1} p(e^{2\pi i \lambda^j w}) \left(\frac{1 - e^{-2\pi i \lambda^j w}}{2\pi i \lambda^j w} \right)^h, \tag{26}$$

where $z_0 := d_0(1 + \lambda + \dots + \lambda^{k-1})/(\lambda^k - 1)$, h is an integer and $p(z)$ is a polynomial.

Set

$$G_1(w) := \prod_{j=0}^{k-1} p(e^{2\pi i \lambda^j w}) (1 - e^{-2\pi i \lambda^j w})^h$$

and

$$G_2(w) := \prod_{j=1}^n (1 - e^{-2\pi i m_j w}).$$

Comparing (25) and (26), one gets $G_2(w) = e^{2\pi i \alpha w} G_1(w)$, where α is a constant. Expanding $\prod_{j=0}^{k-1} p(e^{2\pi i \lambda^j w})(1 - e^{-2\pi i \lambda^j w})^h$, we see that each term has the form $e^{2\pi i w \sum_{j=0}^{k-1} b_j \lambda^j}$ with $b_j \in \mathbf{Z}$. Since $\lambda^k > 1$ is an integer, by the theorem of Capelli (see [20] or p. 92 in [24]), λ is an algebraic integer of degree k . Thus the difference between two distinct numbers in the form of $\sum_{j=0}^{k-1} b_j \lambda^j$ is non-integer. We conclude that $\mathbf{A}_{G_1}(w) = p(e^{2\pi i w})(1 - e^{-2\pi i w})^h$. A simple observation also shows that $\mathbf{A}_{G_2}(w) = \prod_{m_j \in \mathbf{Z}} (1 - e^{-2\pi i m_j w})$. Since $\mathbf{A}_{G_1}(w) = \mathbf{A}_{G_2}(w)$, there are h integer entries in the vector A . Without loss of generality, suppose that $m_1, \dots, m_h \in \mathbf{Z}$. Note that

$$G_1(w) = \prod_{j=0}^{k-1} \mathbf{A}_{G_1}(\lambda^j w) = \prod_{j=0}^{k-1} \prod_{r=1}^h (1 - e^{-2\pi i m_r \lambda^j w}).$$

Then $G_2(w) = e^{2\pi i \alpha w} \prod_{j=0}^{k-1} \prod_{r=1}^h (1 - e^{-2\pi i m_r \lambda^j w})$. It follows that $\alpha = 0$, so the vector A can be written as a union of $(m_r, \lambda m_r, \dots, \lambda^{k-1} m_r), r = 1, \dots, h$, proving part (D). \square

Proof of Theorem 2.7. We begin with (A). Assume that

$$M = (m_1, \dots, m_n) \in \mathbf{R}^{s \times n}.$$

It is well-known that the Fourier transform of $B(x|M)$ is

$$\widehat{B}(w|M) = \prod_{j=1}^n \frac{1 - e^{-2\pi i w^T m_j}}{2\pi i w^T m_j}.$$

Since $B(x|M)$ is λ -refinable, the mask polynomial H is given by the formulae $H(w) = \widehat{B}(\lambda w|M)/\widehat{B}(w|M)$.

Put $W := \{w | w^T m_j \neq 0, \text{ for all } j\}$. Select a $w_0 \in W$ and consider

$$\widehat{f}(z|w_0) := \widehat{B}(zw_0|M) = \prod_{j=1}^n \frac{1 - e^{-2\pi i zw_0^T m_j}}{2\pi i zw_0^T m_j}, \quad (27)$$

where $z \in \mathbf{R}$. Observe that $\widehat{f}(z|w_0)$ can be considered as the Fourier transform of the univariate box spline $B(x|(w_0^T m_1, \dots, w_0^T m_n))$, which is λ -refinable for

each fixed $w_0 \in W$ with the function $\widehat{f}(\lambda z|w_0)/\widehat{f}(z|w_0) = H(zw_0)$ being a quasi-trigonometric polynomial. Then, by Theorem 2.6, there exists a positive integer l such that $\lambda^l \in \mathbf{Z}$, proving part (A).

Select an entry in the vector $(w_0^T m_1, \dots, w_0^T m_n)$, for instance, $w_0^T m_0$. Since $B(x|(w_0^T m_1, \dots, w_0^T m_n))$ is λ -refinable, one can find an integer p_{w_0} and an index j_{w_0} satisfying $2 \leq j_{w_0} \leq n$ such that $w_0^T m_{j_{w_0}} = p_{w_0} w_0^T m_0 / \lambda$ for any $w_0 \in W$ (see part (B) in Theorem 2.6). Each w_0 corresponds to an index j_{w_0} . For an index j , set $W(j) = \{w_0 \in W | j_{w_0} = j\}$. Then $\cup_{j=2}^n W(j) = W$. Since the s dimensional Lebesgue outer measure of W is infinite, there exists a subset of W , say, W_0 such that, for any $w_0 \in W_0$, the index j_{w_0} is a constant and the s dimensional Lebesgue outer measure of W_0 is positive. We suppose the constant index j_{w_0} is u_1 . Then

$$p_{w_0} \frac{w_0^T m_0}{\lambda} = w_0^T m_{u_1} \quad (28)$$

for any $w_0 \in W_0$. We now consider all integers p_{w_0} . For each $q \in \mathbf{Z}$, set

$$W_0(q) := \{w_0 | p_{w_0} = q, \quad w_0 \in W_0\}.$$

Then

$$\bigcup_{q \in \mathbf{Z}} W_0(q) = W_0.$$

We claim that there exists a positive integer q_1 such that the s dimensional Lebesgue outer measure of $W_0(q_1)$ is positive. Indeed, the s dimensional Lebesgue outer measure of W_0 is positive and the set \mathbf{Z} is countable. Hence there exist s linearly independent elements of $W_0(q_1)$. Let us denote them by w_1, \dots, w_s .

We have

$$q_1 \frac{w_j^T m_0}{\lambda} = w_j^T m_{u_1},$$

for each $1 \leq j \leq s$, by (28). It follows that

$$w_j^T \mathbf{V} = 0, \quad (29)$$

for each $1 \leq j \leq s$ where $\mathbf{V} := (q_1 \frac{m_0}{\lambda} - m_{u_1})$. Let A be the $s \times s$ matrix

$$A = (w_j^T)_{1 \leq j \leq s}.$$

Then A is non-singular, because w_j are linearly independent. The equality (29) can be written as $A\mathbf{V} = 0$. It follows that $\mathbf{V} = 0$, because A is non-singular. Hence $m_{u_1} = q_1 m_0 / \lambda$. Putting $m := m_{u_1}, p := q_1$, we complete the proof of (B).

Part (C) can be proved by the same method as in the proof of the part (C) of Theorem 2.6. We omit the details.

It remains to prove (D). Set $W' := W \cap \mathbf{Z}^s$. By the definition of W , one can see that $W' = \mathbf{Z}^s \setminus (\cup_{j=1}^n H_j)$, where $H_j := \{w \in \mathbf{Z}^s | w^T m_j = 0\}$. Then $B(x | (w_0^T m_1, \dots, w_0^T m_n))$ is λ -refinable with integer translations for every $w_0 \in W'$. By Theorem 2.6, the vector $(w_0^T m_1, \dots, w_0^T m_n)$ can be written as

$$(w_0^T m_{u_{11}}, \dots, w_0^T m_{u_{1k}}, w_0^T m_{u_{21}}, \dots, w_0^T m_{u_{2k}}, \dots, w_0^T m_{u_{t1}}, \dots, w_0^T m_{u_{tk}}).$$

Here, for each fixed $r = 1, \dots, t$, one has $w_0^T m_{u_{r,h+1}} = \lambda w_0^T m_{u_{r,h}}$, where $h = 1, \dots, k-1$ and $t := n/k$ is an integer. Hence, each $w_0 \in W'$ corresponds to the index vector $P(w_0) := (u_{11}, \dots, u_{1k}, \dots, u_{t1}, \dots, u_{tk})$, which is a permutation of $(1, \dots, n)$.

Let us denote the set consisting of all permutations of $(1, \dots, n)$ by \mathbf{P} . For each $p \in \mathbf{P}$ put

$$W'(p) := \{w_0 \in W' | P(w_0) = p\}.$$

We claim that there exists a $p_0 \in \mathbf{P}$ such that $\text{span}(W'(p_0)) = \mathbf{R}^s$, i.e., that there are s linearly independent vectors in $W'(p_0)$. For a contradiction, assume that $\text{span}(W'(p_0))$ is contained in a $(s-1)$ -hyperplane for every $p_0 \in \mathbf{P}$. Note that

$$\cup_{p \in \mathbf{P}} W'(p) = W' = \mathbf{Z}^s \setminus (\cup_{j=1}^n H_j).$$

Then

$$\mathbf{Z}^s = (\cup_{p \in \mathbf{P}} W'(p)) \cup (\cup_{j=1}^n H_j). \quad (30)$$

Since $\#\mathbf{P}$ is finite, the equation (30) shows that \mathbf{Z}^s can be written as a finite union of hyperplanes, yielding a contradiction.

Without loss of generality, we may suppose that $\text{span}(W'(p_0)) = \mathbf{R}^s$ for $p_0 = (u_{11}, \dots, u_{1k}, \dots, u_{t1}, \dots, u_{tk})$. Then, one can select s linearly independent vectors in $W'(p_0)$, say w_1, \dots, w_s , such that for each fixed $1 \leq r \leq t$ and $1 \leq j \leq s$, one has $w_j^T m_{u_{r,h+1}} = \lambda w_j^T m_{u_{r,h}}$, where $1 \leq h \leq k-1$. Hence, for fixed r and h , we obtain the following linear equations

$$w_j^T m_{u_{r,h+1}} = w_j^T \lambda m_{u_{r,h}},$$

where $j = 1, \dots, s$. Solving these linear equations, we get $m_{u_{r,h+1}} = \lambda m_{u_{r,h}}$, where $r = 1, \dots, t$ and $h = 1, \dots, k-1$.

Hence the matrices $(m_{u_{r1}}, \dots, m_{u_{rk}})$, $1 \leq r \leq t$, are of the form $(m_0, \lambda m_0, \dots, \lambda^{k-1} m_0)$ with $m_0 := m_{u_{r1}}$. Consequently, the matrix M can be written as a union of t matrices of the same form. \square

Acknowledgements. We thank both referees whose remarks improved the readability of the paper. The research of the first named author was supported by the Lithuanian Foundation of Studies and Science. The second named author was supported by the National Natural Science Foundation of China (10401021).

References

- [1] P. Auscher, Wavelet bases for $L^2(R)$ with rational dilation factor, in: Wavelets and Their Applications, edited by M. B. Ruskai et al. (Jones and Bartlett, 1992), pp. 439-452.
- [2] A. Cavaretta, W. Dahmen and C. A. Micchelli, Stationary subdivision, *Mem. Amer. Math. Soc.*, **93** (1991), 1-186.

- [3] X.-R. Dai, D.-J. Feng and Y. Wang, Classification of refinable splines, *Constructive Approx.*, **24** (2006), 187-200.
- [4] X.-R. Dai, D.-J. Feng and Y. Wang, Refinable functions with non-integer dilations, *J. Func. Anal.*, **250** (2007), 1-20.
- [5] X.-R. Dai, D.-J. Feng and Y. Wang, Structure of refinable splines, *Appl. Comput. Harmonic Anal.*, **22** (2007), 374-381.
- [6] I. Daubechies and J. C. Lagarias, Two-scale difference equations I. Existence and global regularity of solutions, *SIAM J. Math. Anal.*, **22** (1991), 1388-1410.
- [7] I. Daubechies, Ten lectures on wavelets, CBMS-NSF Regional Conference Series in Applied Mathematics, 61, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.
- [8] B. de Mathan, Numbers contravening a condition in density modulo 1, *Acta Math. Acad. Sci. Hung.*, **36** (1980), 237-241.
- [9] C. de Boor, K. Höllig and S. Riemenschneider, *Box Splines*, Springer-Verlag, New York, 1993.
- [10] R. DeVore and A. Ron, Developing a computation-friendly mathematical foundation for spline functions, *SIAM News*, May (2005) p.5.
- [11] A. Dubickas, On the fractional parts of lacunary sequences, *Math. Scand.*, **99** (2006), 136-146.
- [12] P. Erdős, On a family of symmetric Bernoulli convolutions, *Amer. J. Math.*, **61** (1939), 974-976.
- [13] P. Erdős, Problems and results on Diophantine approximations. II, *Repartition modulo 1, Actes Colloq. Marseille-Luminy 1974, Lecture Notes in Math.*, **475** (1975), 89-99.

- [14] D. J. Feng and Y. Wang, Bernoulli convolutions associate with certain non-Pisot numbers, *Adv. Math.*, **187** (2004), 173-194.
- [15] T. N. T. Goodman, Refinable spline functions, in: C.C. Chui, L.L. Schumaker (Eds.), *Approximation Theory IX*, Vanderbilt University Press, Nashville. TN. 1998, pp. 1-25.
- [16] Y. Guan, S. Lu and Y. Tang, Characterization of compactly supported refinable splines whose shifts form a Riesz basis, *J. Appr. Th.*, 133 (2005), 245-250.
- [17] R. Q. Jia and C. A. Micchelli, Using the refinement equations for the construction of pre-wavelets. II. Powers of two, *Curves and Surfaces*, 209-246, Academic Press, Boston, MA, 1991.
- [18] R. Q. Jia and N. Sivakumar, On the linear independence of integer translates of box splines with rational direction, *Linear Algebra and Appl.*, **135** (1990), 19-31.
- [19] A. Khintchine, Über eine Klasse linearer diophantischer Approximationen, *Rend. Circ. Mat. Palermo*, **50** (1926), 170-195.
- [20] S. Lang, *Algebra*, 3rd ed., Graduate texts in mathematics **211**, Springer-Verlag, New York, Berlin, 2002.
- [21] W. Lawton, S. L. Lee and Z. Shen, Characterization of compactly supported refinable splines, *Adv. Comp. Math.*, **3** (1995), 137-145.
- [22] Y. Peres and W. Schlag, Smoothness of projections, Bernoulli convolutions, and the dimension of exceptions, *Duke Math. J.*, **102** (2000), 193-251.
- [23] A. D. Pollington, On the density of the sequence $\{n_k\xi\}$, *Illinois J. Math.*, **23** (1979), 511-515.

- [24] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of mathematics and its applications **77**, CUP, Cambridge, 2000.
- [25] B. Solomyak, On the random series $\sum \pm \lambda^n$ (an Erdős problem), *Ann. Math.*, **142** (1995), 611-625.
- [26] Q. Sun, Refinable functions with compact support, *J. Appr. Th.*, **86** (1996), 240-252.
- [27] D. X. Zhou, Some characterizations for box spline wavelets and linear Diophantine equations, *Rocky Mountain J. Math.*, **28** (1998), 1539-1560.