COLLOQUIUM MATHEMATICUM

VOL. LVIII 1989 FASC. 1

STRONG RIESZ SETS AND POLYNOMIALS

BY

TODD COCHRANE AND ROBERT E. DRESSLER (MANHATTAN, KANSAS)

Let T denote the circle group and $M(T)$ the set of finite Borel measures on T. For any $\mu \in M(T)$ the Fourier–Stieltjes transform $\hat{\mu}$ is defined by

$$\hat{\mu}(n) = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{-in\theta} d\mu(\theta), \quad n \in \mathbf{Z}.$$

A subset S of $\mathbf{Z}$ is called a *Riesz set* if, for any $\mu \in M(T)$ with $\operatorname{supp} \hat{\mu} \subset S$, μ is absolutely continuous with respect to Lebesgue measure on T. Throughout this paper we shall endow $\mathbf{Z}$ with the topology of its Bohr compactification. The closure of a subset S of $\mathbf{Z}$ will be denoted by $\bar{S}$.

In [5], Meyer defined a set of integers to be a *strong Riesz set* if its closure is a Riesz set and in Theorem 2 of the same paper he showed that the union of a strong Riesz set and a Riesz set is a Riesz set. In Proposition 4 of [5] Meyer proved that the set of squares is a strong Riesz set. In [3], Dressler and Pigno showed that the set of integers representable as a sum of two squares is a strong Riesz set. In this paper we extend these results and give a criterion for determining the closure of the set of values represented by a polynomial in n variables.

To begin, we recall that a basic neighborhood of zero is given by

$$N(\beta_1, \beta_2, \ldots, \beta_k, \varepsilon) = \{x \in \mathbf{Z}: \ \|\beta_i x\| < \varepsilon, \ 1 \leqslant i \leqslant k\},$$

where $\beta_1, \beta_2, \ldots, \beta_k$ are any real numbers, $\varepsilon > 0$, and $\|\cdot\|$ denotes the distance to the nearest integer. In particular, if the β_i are all rational, then the neighborhood is just an arithmetic progression through the origin. Basic neighborhoods of other points are just translates of these neighborhoods.

For any polynomial $f = f(\mathbf{x}) = f(x_1, x_2, \ldots, x_n)$ with integer coefficients we let S_f denote the set of values represented by f as the variables run through the set of integers.

THEOREM 1. *Let $b \in \mathbf{Z}$. Then the following are equivalent:*

(i) $b \in \bar{S}_f$.

(ii) *Every arithmetic progression containing b has a nonempty intersection with S_f.*

(iii) *The congruence $f(\mathbf{x}) \equiv b \pmod m$ is solvable for all positive integers m.*

(iv) *The equation $f(\mathbf{x}) = b$ is solvable over the ring of p-adic integers for every prime p.*

Proof. The equivalence of (ii) and (iii) is easily seen and that of (iii) and (iv) is well known. Also, the fact that (i) implies (ii) is trivial. Thus we need only show that (iii) implies (i). If f is a constant polynomial, this implication is trivial, so we may assume that f is nonconstant. Let b be an integer satisfying (iii) and let

$$N = N(\beta_1, \beta_2, \ldots, \beta_k, \varepsilon) + b$$

be a neighborhood of b. We will show by induction on k that for any modulus $m \neq 0$ there exists an n-tuple of integers $\boldsymbol{a}$ such that

$$f(\boldsymbol{a}) \equiv b \pmod{m} \quad \text{and} \quad f(\boldsymbol{a} + m\boldsymbol{t}) \in N$$

for infinitely many n-tuples $\boldsymbol{t}$.

Suppose that $k = 1$, $N = N(\beta, \varepsilon) + b$, and m is a positive integer. If β is rational, say $\beta = r/s$, we take $\boldsymbol{a}$ to be a solution of the congruence $f(x) \equiv b \pmod{ms}$. Then, for any n-tuple of integers $\boldsymbol{t}$,

$$\|(f(\boldsymbol{a} + ms\boldsymbol{t}) - b)\beta\| = 0, \quad \text{that is,} \quad f(\boldsymbol{a} + ms\boldsymbol{t}) \in N.$$

If β is irrational, then we take $\boldsymbol{a}$ to be any solution of the congruence $f(x) \equiv b \pmod{m}$. Let $\boldsymbol{c}$ be an n-tuple of integers such that $f(\boldsymbol{a} + t m\boldsymbol{c})$ is a nonconstant polynomial in the variable t; for instance, let $\boldsymbol{c}$ be a point where the maximal homogeneous part of f does not vanish. Then $\beta(f(\boldsymbol{a} + tm\boldsymbol{c}) - b)$ is a nonconstant polynomial with an irrational leading coefficient, and so its values are uniformly distributed modulo one (see [2], Theorem VI, p. 71). In particular, it will take on a value less than ε modulo one for infinitely many t.

Suppose now that the claim is true for $k-1$. Let $N = N(\beta_1, \ldots, \beta_k, \varepsilon) + b$ and let m be a positive integer. Suppose first that $\beta_1, \ldots, \beta_k$, 1 are linearly independent over $\boldsymbol{Z}$. Let $\boldsymbol{a}$ be any solution of the congruence $f(x) \equiv b \pmod{m}$ and again let $\boldsymbol{c}$ be an n-tuple such that $f(\boldsymbol{a} + tm\boldsymbol{c})$ is nonconstant. Then for any nonzero n-tuple of integers $\boldsymbol{u}$ the polynomial in t

$$\sum_{i=1}^{k} u_i \beta_i (f(\boldsymbol{a} + mt\boldsymbol{c}) - b)$$

has an irrational leading coefficient, and so its values are uniformly distributed modulo one. Hence by Weyl's Criterion ([2], Theorem III, p. 66) the k-tuples

$$(\beta_1(f(\boldsymbol{a} + mt\boldsymbol{c}) - b), \ldots, \beta_k(f(\boldsymbol{a} + mt\boldsymbol{c}) - b))$$

are uniformly distributed in the unit cube, and so

$$\|\beta_i(f(\boldsymbol{a} + mt\boldsymbol{c}) - b)\| < \varepsilon, \quad 1 \leqslant i \leqslant k,$$

for infinitely many integers t.

Suppose now that $\beta_1, \ldots, \beta_k$, 1 are linearly dependent over $\boldsymbol{Z}$, say, without loss of generality, that

$$\beta_k = \frac{u}{u_k} - \sum_{i=1}^{k-1} \frac{u_i}{u_k} \beta_i \tag{1}$$

for some $u, u_i \in \boldsymbol{Z}$, $1 \leqslant i \leqslant k$, $u_k \neq 0$. Set

$$U = \max\{|u_1|, |u_2|, \ldots, |u_k|\}.$$

We apply the induction hypothesis to the neighborhood

$$N' = N\left(\frac{\beta_1}{u_k}, \ldots, \frac{\beta_{k-1}}{u_k}, \frac{\varepsilon}{kU}\right) + b$$

of b, and to the modulus mu_k. Thus, there exists an $\boldsymbol{a} \in \boldsymbol{Z}^n$ such that

$$f(\boldsymbol{a}) \equiv b \pmod{mu_k},$$

and

$$\left\| \frac{\beta_i}{u_k}(f(\boldsymbol{a} + mu_k\boldsymbol{t}) - b) \right\| < \frac{\varepsilon}{kU}, \quad 1 \leqslant i \leqslant k-1,$$

for infinitely many $\boldsymbol{t} \in \boldsymbol{Z}^n$. For any such $\boldsymbol{t}$ we have

$$\|\beta_i(f(\boldsymbol{a} + mu_k\boldsymbol{t}) - b)\| < \varepsilon, \quad 1 \leqslant i \leqslant k-1,$$

and, by (1) and the triangle inequality for $\|\cdot\|$,

$$\|\beta_k(f(\boldsymbol{a} + mu_k\boldsymbol{t}) - b)\| \leqslant \left\| \frac{u}{u_k}(f(\boldsymbol{a} + mu_k\boldsymbol{t}) - b) \right\| + \sum_{i=1}^{k-1} \left\| \frac{u_i}{u_k}\beta_i(f(\boldsymbol{a} + mu_k\boldsymbol{t}) - b) \right\|$$

$$\leqslant 0 + \sum_{i=1}^{k-1} |u_i| \frac{\varepsilon}{kU} < \varepsilon.$$

Hence $f(\boldsymbol{a} + mu_k\boldsymbol{t}) \in N(\beta_1, \ldots, \beta_k, \varepsilon) + b$.

The next two theorems give examples of strong Riesz sets that generalize the examples referred to at the beginning of this paper.

THEOREM 2. *If $f(x, y)$ is a positive definite quadratic form with integer coefficients, then $\boldsymbol{S}_f$ is a strong Riesz set.*

Proof. (We recall that a form is said to *represent zero over a given field* if it does so in a nontrivial manner.) If $b \in \bar{\boldsymbol{S}}_f$, then by Theorem 1 the form $f(x, y) - bz^2$ represents zero over every p-adic field. Thus, by [1], Lemma 2, p. 67, it represents zero over $\boldsymbol{R}$ as well. Since f is positive definite, b must be positive. Thus, by the F. and M. Riesz Theorem, $\bar{\boldsymbol{S}}_f$ is a Riesz set.

Theorem 2 does not generalize to positive definite forms in three variables. For example, if $f = x^2 + 7y^2 + z^2$, then it follows readily from Theorem 1 that $\bar{\boldsymbol{S}}_f = \boldsymbol{Z}$. Let $b \in \boldsymbol{Z}$. If p is an odd prime, then the congruence $f \equiv b \pmod{p}$ has a nonsingular solution which can be lifted to a solution $(\mathrm{mod}\, p^e)$ for any $e \geqslant 1$. If $p = 2$, then the congruence $f \equiv b \pmod 8$ has a solution with either x or y odd. This solution can be lifted to a solution $(\mathrm{mod}\, 2^e)$ for any $e \geqslant 3$ (see [1], Theorem 3, p. 42).

THEOREM 3. *Let $f(x)$ be a quadratic or quartic polynomial in one variable with integer coefficients. Then S_f is a strong Riesz set.*

We need the following lemmas:

LEMMA 1 ([4], p. 139, ex. 5). *Let $f(x)$ be a polynomial with integer coefficients irreducible over $\mathbf{Q}$ and of degree $\geqslant 2$. Then there exist infinitely many primes p such that the congruence $f(x) \equiv 0 \pmod{p}$ has no solution.*

LEMMA 2([1]). *For any two nonsquare integers d_1, d_2 there exist infinitely many primes p such that d_1 and d_2 are quadratic nonresidues* (mod p).

Proof. We may assume that d_1, d_2 are square free. Say

$$d_i = (-1)^{\alpha_i} 2^{\beta_i} d e_i, \quad \text{where } \alpha_i, \beta_i = 0 \text{ or } 1,$$

d is the greatest common divisor of the odd parts of d_1, d_2, and e_1, e_2 are odd. In particular, we note that d, e_1 and e_2 are pairwise relatively prime.

Case i. Suppose $d \neq 1$. We choose p such that

$$p \equiv 1 \pmod{8}, \quad \left(\frac{d}{p}\right) = -1, \quad \left(\frac{e_1}{p}\right) = \left(\frac{e_2}{p}\right) = 1.$$

These four conditions depend only on the residue class of p (mod $8de_1e_2$), and so, by Dirichlet's Theorem on primes in arithmetic progressions, infinitely many such p exist.

Case ii. $d = 1$, $e_1 \neq 1$, $e_2 \neq 1$. In this case choose p such that

$$p \equiv 1 \pmod{8}, \quad \left(\frac{e_1}{p}\right) = \left(\frac{e_2}{p}\right) = -1.$$

Case iii. $d = 1$, $e_1 = 1$, $e_2 \neq 1$. If $d_1 = \pm 2$, we choose p so that

$$p \equiv 5 \pmod{8} \quad \text{and} \quad \left(\frac{e_2}{p}\right) = -\left(\frac{2^{\beta_2}}{p}\right).$$

If $d_1 = -1$, we choose p so that

$$p \equiv 3 \pmod{8} \quad \text{and} \quad \left(\frac{e_2}{p}\right) = -\left(\frac{(-1)^{\alpha_2} 2^{\beta_2}}{p}\right).$$

Case iv. $d = 1$, $e_1 \neq 1$, $e_2 = 1$ (same as case iii).

Case v. $d = e_1 = e_2 = 1$. If d_1, $d_2 = \pm 2$, we choose p so that

$$p \equiv 5 \pmod{8}.$$

If $d_1 = -1$, $d_2 = 2$ or $d_1 = 2$, $d_2 = -1$, we take

$$p \equiv 3 \pmod{8}.$$

([1]) The referee points out that this lemma is essentially contained in the work of Dirichlet.

Finally, if $d_1 = -1$, $d_2 = -2$ or $d_1 = -2$, $d_2 = -1$, we take

$$p \equiv 7 \pmod 8.$$

Proof of Theorem 3. First suppose that $f(x)$ is a quadratic polynomial, and without loss of generality assume that the leading coefficient is positive. Let m be the minimum value attained by f over $\boldsymbol{R}$ and let b be any integer less than m. Then $f(x)-b$ is irreducible over $\boldsymbol{R}$, and so by Lemma 1 there exists a prime p such that the congruence

$$f(x) \equiv b \pmod p$$

has no solution. Hence, by Theorem 1, $b \notin \bar{S}_f$. Thus $\bar{S}_f$ is bounded from below, and therefore is a Riesz set.

Suppose now that f is a fourth degree polynomial and again assume that the leading coefficient is positive and that m is the minimum value attained by f over $\boldsymbol{R}$. Let b be an integer less than m. Set $g(x) = f(x)-b$. Then $g(x)$ is either irreducible over $\boldsymbol{Q}$ or factors into a product of two irreducible quadratic polynomials with integer coefficients. If $g(x)$ is irreducible, we can proceed as above. Suppose $g(x) = h(x)k(x)$, where h and k are irreducible quadratic polynomials over $\boldsymbol{Z}$. Let d, e be the discriminants of h, k, respectively. By Lemma 2 there exists a prime p such that

$$\left(\frac{d}{p}\right) = \left(\frac{e}{p}\right) = -1.$$

For this prime the congruence $g(x) \equiv 0 \pmod p$ has no solution. Therefore $b \notin \bar{S}_f$, and so $\bar{S}_f$ is bounded from below.

We do not know whether S_f is a strong Riesz set in the cases where f is a cubic polynomial or a polynomial of degree $\geqslant 5$ in one variable, or whether there exist any indefinite binary quadratic forms f for which S_f is a strong Riesz set **(P 1373)**. We can prove the following however. If $f(x)$ is a monic cubic polynomial or a monomial of the form x^d for a fixed $d \geqslant 2$, then S_f is a closed set, and hence is a strong Riesz set if and only if it is a Riesz set.

REFERENCES

[1] Z. J. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York 1966.
[2] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Hafner Pub., New York 1972.
[3] R. E. Dressler and L. Pigno, *On strong Riesz sets*, Colloq. Math. 29 (1974), pp. 157–158.
[4] G. J. Janusz, *Algebraic Number Fields*, Academic Press, New York 1973.
[5] Y. Meyer, *Spectres des mesures et mesures absolument continues*, Studia Math. 30 (1968), pp. 87–99.

DEPARTMENT OF MATHEMATICS
KANSAS STATE UNIVERSITY
CARDWELL HALL
MANHATTAN, KANSAS 66506, U.S.A.

Reçu par la Rédaction le 14.9.1988