THE EXTENSION PROBLEM FOR POSITIVE-DEFINITE FUNCTIONS[1]

BY
Walter Rudin

Introduction

Although we shall be primarily concerned with positive-definite functions on euclidean spaces and on groups of lattice points, we begin by stating the extension problem in a more general context.

If S is a subset of a locally compact abelian group G, we define $\mathrm{PD}(S)$ to be the class of all continuous complex-valued functions φ on $S - S$ (the set of all points $x - y \in G$, with $x \in S$, $y \in S$) which satisfy the inequality

$$\sum_{i,j=1}^{N} c_i \bar{c}_j \varphi(x_i - x_j) \geqq 0 \tag{1}$$

for every positive integer N, for every choice of complex numbers $c_1, \cdots, c_N$, and for every choice of points $x_1, \cdots, x_N$ in S. If S is a finite set, the above requirement may also be written in the form

$$\sum_{x,y \in S} c(x)\overline{c(y)}\varphi(x - y) \geqq 0 \tag{2}$$

for every complex function c on S.

We emphasize that the members of $\mathrm{PD}(S)$ are functions defined on $S - S$, not on S (unless S is a subgroup of G). Also, $\mathrm{PD}(G)$ is precisely the class of all continuous positive-definite functions on G, in the usual terminology.

If a function $\varphi \in \mathrm{PD}(G)$ is restricted to $S - S$, we clearly obtain a member of $\mathrm{PD}(S)$. We are concerned with the following question: Under what circumstances do these restrictions cover $\mathrm{PD}(S)$? In other words, *under what circumstances is it true that every* $\varphi \in \mathrm{PD}(S)$ *has an extension which lies in* $\mathrm{PD}(G)$?

In this direction, M. G. Krein [7] proved that *if I is an interval on the real line R, then every $\varphi \in \mathrm{PD}(I)$ has an extension which lies in* $\mathrm{PD}(R)$.

The main contribution of the present paper is a proof that the analogue of Krein's theorem fails to hold in euclidean spaces of higher dimensions:

Theorem. *If $n > 1$, and if I^n is an n-dimensional cube in R^n, there exists a function $\varphi \in \mathrm{PD}(I^n)$ which cannot be extended to a member of* $\mathrm{PD}(R^n)$.

For recent literature on Krein's theorem, in particular on the question of the uniqueness of the extension, we refer to Akutowicz [1], [2] and Devinatz [4]. Applications to information theory have been discussed by Chover [3]. Higher-dimensional situations are also discussed in [4].

Our method of attack is quite different from the ones used by the above-

Received May 4, 1962.

[1] Sponsored by the Mathematics Research Center, U. S. Army, Madison, Wisconsin and by the National Science Foundation.

named authors. In Section 1 we consider a finite set S in a discrete group G, and we show that the extension problem can be rephrased as the problem of representing certain positive trigonometric polynomials on the dual group of G as sums of squares. In Section 2 these considerations are used to prove that our extension problem always has a solution if $G = Z$, the additive group of all integers, and if S is a finite arithmetic progression in Z. This in turn leads to an easy proof of Krein's theorem. In Section 3 we use a theorem of Hilbert [6], which states that there exist positive polynomials of 2 real variables which are not sums of squares of polynomials, to derive an analogous result for trigonometric polynomials on the 2-dimensional torus T^2, and hence prove that our extension problem may fail to have a solution if $G = Z^2$, the group of all lattice points in the plane, and if S is a square of lattice points (with at least 16 points). An interpolation theorem transfers this negative result from Z^2 to R^2, and hence to R^n, for any $n \geqq 2$.

After completion of the present paper the author learned that one of its main results (Theorem 3.3, the possible nonexistence of a positive-definite extension in Z^2) was proved earlier by Calderón and Pepinsky [8], in a publication devoted primarily to crystallography, and that the two methods of proof are the same. As far as new results are concerned, the main contributions of the present paper are therefore contained in Theorems 3.4 and 3.5. Theorem 1.4 is new in the generality in which it is stated here, but the same idea is used in [8].

1. Connections with sums of squares

In this section, G is a discrete abelian group, S is a finite subset of G, $\Delta = S - S$, Γ is the (compact) dual group of G, and the symbol (x, γ) denotes the value of the character $\gamma \in \Gamma$ at the point $x \in G$. Functions of the form

$$f(\gamma) = \textstyle\sum_{x \in S} c(x)(x, \gamma) \qquad (\gamma \in \Gamma) \tag{3}$$

will be called *S-polynomials*; Δ-polynomials are defined similarly. If (3) holds, we have

$$c(x) = \hat{f}(x) = \int_\Gamma f(\gamma)(-x, \gamma)\, d\gamma, \tag{4}$$

where $d\gamma$ denotes the Haar measure of Γ; $\hat{f}$ is the *Fourier transform* of f.

We let X_S be the real vector space consisting of all real Δ-polynomials, we let P_S be the set of all nonnegative members of X_S, and we let Q_S be the set of all finite sums f of the form

$$f = \textstyle\sum_j |g_j|^2, \tag{5}$$

where each g_j is an S-polynomial.

It is clear that X_S is finite-dimensional (dim X_S = cardinality of Δ) that P_S and Q_S are convex cones in X_S, and that P_S contains Q_S.

If φ is a function on Δ such that $\varphi(-x) = \overline{\varphi(x)}$, the equation

$$L_\varphi(f) = \sum_{x \in \Delta} \varphi(x)\hat{f}(x) \tag{6}$$

defines a real linear functional on X_S. Conversely, every real linear functional on X_S is L_φ for some such φ.

1.1 LEMMA. *A function φ on $S - S$ belongs to* PD(S) *if and only if $L_\varphi(f) \geqq 0$ for every $f \in Q_S$.*

Proof. If $g(\gamma) = \sum c(x)(x, \gamma)$ is an S-polynomial, then

$$| g(\gamma) |^2 = \sum_{x,y \in S} c(x)\overline{c(y)}(x - y, \gamma), \tag{7}$$

so that

$$L_\varphi(| g |^2) = \sum_{x,y \in S} c(x)\overline{c(y)}\varphi(x - y). \tag{8}$$

The lemma follows from (2), (5), and (8).

1.2 LEMMA. *A function φ defined on $S - S$ can be extended to a member of* PD(G) *if and only if $L_\varphi(f) \geqq 0$ for every $f \in P_S$.*

Proof. If $\varphi \in$ PD(G), Bochner's theorem shows that there is a nonnegative measure μ on Γ such that

$$\varphi(x) = \int_\Gamma (-x, \gamma)\, d\mu(\gamma) \qquad (x \in G). \tag{9}$$

For $f \in X_S$, we then have

$$L_\varphi(f) = \sum \hat{f}(x)\varphi(x) = \sum \hat{f}(x) \int_\Gamma (-x, \gamma)\, d\mu(\gamma) = \int_\Gamma f\, d\mu, \tag{10}$$

so that $L_\varphi(f) \geqq 0$ if $f \in P_S$.

Conversely, suppose $L_\varphi(f) \geqq 0$ for all $f \in P_S$. If $f \in X$ and $-1 \leqq f \leqq 1$, the relation $L_\varphi(1) = \varphi(0)$ shows that $| L_\varphi(f) | \leqq \varphi(0)$. If $\varphi(0) = 0$, it follows that $L_\varphi = 0$ on X_S, and hence that $\varphi = 0$ on Δ. Otherwise, we may assume without loss of generality that $\varphi(0) = 1$. Then L_φ is a linear functional of norm 1 on X_S (relative to the supremum norm). By the Hahn-Banach theorem, L_φ extends to a linear functional of norm 1 on the space of all real continuous functions on Γ, and by the Riesz representation theorem there is a measure μ on Γ, of total variation $|| \mu || = 1$, such that

$$L_\varphi(f) = \int_\Gamma f(-\gamma)\, d\mu(\gamma) \qquad (f \in X_S). \tag{11}$$

Since $1 = L_\varphi(1) = \mu(\Gamma) \leqq || \mu || = 1$, we have $\mu \geqq 0$. Applying (11) to $f(x) = (x, \gamma) + (-x, \gamma)$ and to $f(x) = i[(x, \gamma) - (-x, \gamma)]$, with $x \in S$, we conclude that

$$\varphi(x) = \int_\Gamma (-x, \gamma)\, d\mu(\gamma) \qquad (x \in \Delta). \tag{12}$$

The right side of (12) defines a member of PD(G), since $\mu \geqq 0$, and hence furnishes the desired extension of φ.

1.3 LEMMA. *The cone Q_S is closed in X_S.*

Proof. Let d be the number of points in Δ. Then $\dim X_S = d$. Suppose $r > d$ and

$$f = \sum_1^r |g_j|^2, \tag{13}$$

each g_j being an S-polynomial. Each $|g_j|^2$ is in X_S, and since $r > d$, there is a nontrivial relation

$$\sum_1^r \lambda_j |g_j|^2 = 0 \tag{14}$$

with real coefficients λ_j. Renumbering the g_j, if necessary, we may assume that $\lambda_r \geqq \lambda_j$ for $j < r$. We solve (14) for $|g_r|^2$ and substitute into (13) obtaining

$$f = \sum_1^{r-1} (1 - \lambda_j/\lambda_r) |g_j|^2.$$

Since $\lambda_j/\lambda_r \leqq 1$, we have shown that every sum of r squares $|g_j|^2$ is also a sum of $r - 1$ such squares. *Hence every $f \in Q_S$ is a sum of d squares $|g_j|^2$.*

If now $f_n \in Q_S$ ($n = 1, 2, 3, \cdots$) and $f_n \to f$ uniformly on Γ, there are S-polynomials $g_{j,n}$ such that

$$f_n = \sum_{j=1}^d |g_{j,n}|^2 \qquad (n = 1, 2, 3, \cdots). \tag{15}$$

The f_n are uniformly bounded on Γ; hence so are the $g_{j,n}$, by (15). It follows that there is a sequence $\{n_i\}$, $n_i \to \infty$, such that

$$\lim_{i\to\infty} \hat{g}_{j,n_i}(x) = c_j(x) \tag{16}$$

exists for $1 \leqq j \leqq d$ and for all $x \in S$. Putting

$$g_j(\gamma) = \sum_{x \in S} c_j(x)(x, \gamma) \qquad (1 \leqq j \leqq d, \quad \gamma \in \Gamma) \tag{17}$$

we see that $f = \sum |g_j|^2$. Thus $f \in Q_S$, and this proves that Q_S is closed.

1.4 THEOREM. *The following two conditions on a finite set S in a discrete abelian group G are equivalent:*

(A) $P_S = Q_S$.

(B) *Every $\varphi \in$ PD(S) can be extended to a function in* PD(G).

Proof. If $\varphi \in$ PD(S), Lemma 1.1 shows that $L_\varphi(f) \geqq 0$ for all $f \in Q_S$. If (A) holds, it follows that $L_\varphi(f) \geqq 0$ for all $f \in P_S$, and then Lemma 1.2 shows that (B) holds.

Conversely, if (A) is false, there exists $f_0 \in P_S$ such that $f_0 \notin Q_S$. Since Q_S is a closed convex cone in X_S (Lemma 1.3), there is a hyperplane Π through the origin of X_S such that f_0 is on one side of Π and Q_S is on the other. In other words, there is a real linear functional L on X_S such that $L(f_0) < 0$ but $L(f) \geqq 0$ for all $f \in Q_S$. Then $L = L_\varphi$ for some function φ on Δ. Lemma 1.1

shows that $\varphi \in \mathrm{PD}(S)$, and Lemma 1.2 shows that φ cannot be extended to a function in $\mathrm{PD}(G)$. Thus (B) fails if (A) fails.

2. A proof of Krein's theorem

2.1 THEOREM. *If $S = \{m, m+1, \cdots, m+N\} \subset Z$, the group of integers, then every $\varphi \in \mathrm{PD}(S)$ has an extension to a function in* $\mathrm{PD}(Z)$.

Proof. If $f(e^{i\theta}) = \sum_{-N}^{N} a_n e^{in\theta}$ and $f(e^{i\theta}) \geqq 0$ for all real θ, then $f = |g|^2$ for some g of the form $g(e^{i\theta}) = \sum_{n \in S} b_n e^{in\theta}$ (Fejér-Riesz [5]). Thus $P_S = Q_S$, in the terminology of Section 1, and Theorem 1.4 completes the proof.

2.2 LEMMA. *If $\varphi \in \mathrm{PD}(Z)$, and if*

$$\Phi(t) = (n+1-t)\varphi(n) + (t-n)\varphi(n+1) \quad (n \in Z, n \leqq t \leqq n+1), \tag{18}$$

then $\Phi \in \mathrm{PD}(R)$, and $\Phi(n) = \varphi(n)$ for $n \in Z$.

Proof. It is evident that Φ coincides with φ on Z. If we set

$$K(t) = \max(1 - |t|, 0) \qquad (t \in R), \tag{19}$$

(18) is equivalent to

$$\Phi(t) = \sum_{n \in Z} \varphi(n) K(t-n) \qquad (t \in R). \tag{20}$$

For $0 < r < 1$, define

$$\Phi_r(t) = \sum_{n \in Z} \varphi(n) r^{|n|} K(t-n) \qquad (t \in R), \tag{21}$$

and note that

$$\sum_{n \in Z} \varphi(n) r^{|n|} e^{inx} \geqq 0 \qquad (x \in R) \tag{22}$$

since $\varphi \in \mathrm{PD}(Z)$. Since the Fourier transform $\hat{K}$ of K is nonnegative, and since

$$\Phi_r(t) = \int_{-\infty}^{\infty} \hat{K}(x) \{ \sum_{n \in Z} \varphi(n) r^{|n|} e^{inx} \} e^{-itx}\, dx, \tag{23}$$

we see that Φ_r is the Fourier transform of a nonnegative function. Hence $\Phi_r \in \mathrm{PD}(R)$, for $0 < r < 1$, and the same is true of $\Phi = \lim_{r \to 1} \Phi_r$.

2.3 THEOREM (Krein). *If S is an open segment in R, every $\varphi \in \mathrm{PD}(S)$ can be extended to a function in* $\mathrm{PD}(R)$.

Proof. For $k = 1, 2, 3, \cdots$, let G_k be the subgroup of R which is generated by the number $1/k$, and put $S_k = S \cap G_k$. If $\varphi \in \mathrm{PD}(S)$, its restriction φ_k to $S_k - S_k$ belongs to $\mathrm{PD}(S_k)$, and since G_k is isomorphic to Z, Theorem 2.1 shows that φ_k can be extended to a function in $\mathrm{PD}(G_k)$. By linear interpolation (Lemma 2.2) we obtain functions $\Phi_k \in \mathrm{PD}(R)$ which coincide with φ on $S_k - S_k$. If J is a closed subinterval of $S - S$, the continuity of φ

shows that $\{\Phi_k\}$ tends to φ on $S - S$, uniformly on J, and that $\{\Phi_k\}$ is an equicontinuous sequence on J.

Each Φ_k is the Fourier-Stieltjes transform of a nonnegative measure μ_k on R. Hence

$$(24) \qquad | \Phi_k(x) - \Phi_k(y) | \leqq \int_{-\infty}^{\infty} | e^{ixt} - e^{iyt} | \, d\mu_k(t),$$

and the Schwarz inequality yields

$$(25) \qquad | \Phi_k(x) - \Phi_k(y) |^2 \leqq 2\,\Phi_k(0) \, | \Phi_k(0) - \Phi_k(x - y) |$$

for any $x, y \in R$.

Since $\{\Phi_k\}$ is equicontinuous on J, (25) shows that $\{\Phi_k\}$ is equicontinuous on all of R, and therefore a subsequence $\{\Phi_{k_i}\}$ will converge to a function $\Phi \in \mathrm{PD}\,(R)$ which coincides with φ on $S - S$. This completes the proof.

3. The extension problem in R^p, for $p > 1$

We begin with a statement of the theorem of Hilbert which was alluded to in the Introduction.

3.1 THEOREM. *If $N \geqq 3$, there are polynomials $F(s, t)$ of degree $2N$ which are positive for all real (s, t) and which are not sums of squares of polynomials.*

Hilbert worked with homogeneous polynomials; hence the number of variables in his statement is 3. He also obtained analogous results for polynomials in more variables, for $N \geqq 2$. For simplicity in writing the proof of Theorem 3.2 we restrict ourselves to 2 variables.

We let Z^2 be the group of all lattice points in the plane, i.e., the set of all points in R^2 with integer coordinates. For $N = 1, 2, 3, \cdots$, we let S_N be the set of all $n = (i, j) \in Z^2$ whose coordinates satisfy $0 \leqq i \leqq N$, $0 \leqq j \leqq N$.

3.2 THEOREM. *Fix $N \geqq 3$. If $S = S_N$ and $G = Z^2$, then (in the terminology of Section 1) $Q_S \neq P_S$.*

Proof. Let X_S be as in Section 1, let Y be the space of all polynomials

$$(26) \qquad F(s, t) = \sum_{p,q=0}^{2N} a_{pq}\, s^p t^q \qquad (a_{pq} \text{ real}),$$

and let Ψ be the linear map of X_S into Y given by

$$(27) \qquad (\Psi f)(s, t) = (1 + s^2)^N (1 + t^2)^N f\left(\frac{s + i}{s - i}, \frac{t + i}{t - i}\right).$$

(This change of variables was suggested by A. P. Calderón.) Since $\dim X = (2N + 1)^2 = \dim Y$, and since Ψ evidently preserves linear independence, it follows that Ψ is a 1-1 map of X onto Y.

Suppose now that $f \in Q_S$. Then $f = \sum | g_j |^2$, each g_j being an S-polynomial. Setting

(28) $$G_j(s, t) = (s - i)^N(t - i)^N g_j\left(\frac{s + i}{s - i}, \frac{t + i}{t - i}\right),$$

we see that G_j is a (complex) polynomial of degree at most N in each of the variables s, t, and that

(29) $$(\Psi f)(s, t) = \sum_j | G_j(s, t) |^2.$$

Setting $F = \Psi f$ and $G_j = u_j + iv_j$ (u_j, v_j real for real arguments), we have $F \in Y$, u_j and v_j are polynomials, and $F = \sum (u_j^2 + v_j^2)$.

Hence, if P_S and Q_S were equal, every positive F of the form (26) would be a sum of squares of polynomials, in contradiction to Hilbert's theorem.

3.3 Theorem. *For* $N \geqq 3$, *there exists* $\varphi \in \mathrm{PD}(S_N)$ *which cannot be extended to a member of* $\mathrm{PD}(Z^2)$.

Proof. This follows immediately from Theorems 1.4 and 3.2.

3.4 Theorem. *Let* $S = S_N$, $\Delta = S - S$, *both in* Z^2. *Let* S^* *be the convex hull of* S *in* R^2. *To each* $\varphi \in \mathrm{PD}(S)$ *there corresponds a* $\Phi \in \mathrm{PD}(S^*)$ *such that* $\Phi(n) = \varphi(n)$ *for all* $n \in \Delta$.

Proof. The proof is suggested by the construction in Lemma 2.2.

Let U be the open square with vertices at $(\pm\frac{1}{2}, \pm\frac{1}{2})$, let λ be a measurable function which vanishes outside U, such that $\int | \lambda |^2 = 1$, and put

(30) $$K(x) = \int \lambda(x + y)\overline{\lambda(y)}\, dy \qquad (x \in R^2),$$

(31) $$\Phi(x) = \sum_{n \in \Delta} \varphi(n)K(x - n) \qquad (x \in R^2).$$

(It is understood that integrals without subscripts are extended over R^2, with respect to Lebesgue measure.)

If $m \in Z^2$ and $m \neq 0$, then $K(m) = 0$, and $K(0) = 1$. Hence $\Phi(n) = \varphi(n)$ for $n \in \Delta$. Also, Φ is clearly continuous. To show that $\Phi \in \mathrm{PD}(S^*)$ we have to prove that

(32) $$\sum_{i,j} c_i \bar{c}_j \Phi(x_i - x_j) \geqq 0$$

for every choice of finitely many complex numbers c_i and points $x_i \in S^*$.

If we set $\varphi(n) = 0$ outside Δ and

(33) $$\Lambda(y) = \sum_i c_i \lambda(y - x_i) \qquad (y \in R^2),$$

substitution of (30) into (31) shows that the left side of (32) is equal to

(34) $$\sum_{n \in Z^2} \varphi(n) \int \Lambda(y + n)\overline{\Lambda(y)}\, dy.$$

The integrals in (34) are equal to

(35) $$\sum_{m \in Z^2} \int_U \Lambda(y + n + m)\overline{\Lambda(y + m)}\, dy;$$

since $\Lambda = 0$ outside $S^* + U$, only finitely many terms of the sum in (35) are different from zero. It follows that (34) is equal to

$$\int_U dy \sum_{m,r \in Z^2} \Lambda(y + r)\overline{\Lambda(y + m)}\varphi(r - m). \tag{36}$$

If $y \in U$ and $y + r \in S^* + U$, then $r \in S^* + U - U$; since

$$Z^2 \cap (S^* + U - U) = S,$$

(36) is not changed if we restrict m and r to lie in S. But $\varphi \in \text{PD}(S)$, and hence (see (2)) the integrand in (36) is nonnegative for every $y \in U$. This establishes (32) and completes the proof.

3.5 THEOREM. *Let S^* be a closed square in R^2. There exists $\Phi \in \text{PD}(S^*)$ which cannot be extended to a function in* PD (R^2).

Proof. Assume, without loss of generality, that S^* is the convex hull of S_3, in the notation of Theorem 3.2. By Theorem 3.3 there exists $\varphi \in \text{PD}(S_3)$ which cannot be extended to a function in PD (Z^2). By Theorem 3.4, there exists $\Phi \in \text{PD}(S^*)$ such that $\Phi = \varphi$ on $S_3 - S_3$. If Φ could be extended to a function $\Phi^* \in \text{PD}(R^2)$, the restriction of Φ^* to Z^2 would be an extension of φ and would be in PD (Z^2), which is a contradiction. The theorem follows.

3.6 *Remarks*. (a) In Theorem 3.4 we could have replaced the square S_N by a rectangle of lattice points in the plane or in R^p for any $p \geqq 2$, without any change in the proof.

(b) The fact that the extension problem may fail to have a solution in R^2 (Theorem 3.5) implies immediately that the same is true in R^p for any $p \geqq 2$.

REFERENCES

1. E. J. AKUTOWICZ, *On extrapolating a positive definite function from a finite interval*, Math. Scand., vol. 7 (1959), pp. 157–169.
2. ———, *Sur l'approximation par certaines fonctions entières*, Ann. Sci. École Norm. Sup. (3), vol. 77 (1960), pp. 281–301.
3. J. CHOVER, *On normalized entropy and the extensions of a positive-definite function*, J. Math. Mech., vol. 10 (1961), pp. 927–945.
4. A. DEVINATZ, *On the extensions of positive definite functions*, Acta Math., vol. 102 (1959), pp. 109–134.
5. L. FEJÉR, *Über trigonometrische Polynome*, J. Reine Angew. Math., vol. 146 (1916), pp. 53–82.
6. D. HILBERT, *Ueber die Darstellung definiter Formen als Summe von Formenquadraten*, Math. Ann., vol. 32 (1888), pp. 342–350.
7. M. G. KREIN, *Sur le problème du prolongement des fonctions hermitiennes positives et continues*, C. R. (Doklady) Acad. Sci. URSS (N. S.), vol. 26 (1940), pp. 17–22.
8. A. CALDERÓN AND RAY PEPINSKY, *On the phases of Fourier coefficients for positive real periodic functions*, Computing Methods and the Phase Problem in X-Ray Crystal Analysis, published by The X-Ray Crystal Analysis Laboratory, Department of Physics, The Pennsylvania State College, 1952, pp. 339–348.

UNIVERSITY OF WISCONSIN
MADISON, WISCONSIN