CLASSES OF POSITIVE DEFINITE UNIMODULAR CIRCULANTS

MORRIS NEWMAN AND OLGA TAUSSKY

All matrices considered here have rational integral elements. In particular some circulants of this nature are investigated. An $n \times n$ circulant is of the form

$$C = \begin{bmatrix} c_0 & c_1 \dots c_{n-1} \\ c_{n-1} & c_0 \dots c_{n-2} \\ & \dots \\ c_1 & c_2 \dots c_0 \end{bmatrix}$$

The following result concerning positive definite unimodular circulants was obtained recently **(3; 4)**:

Let C be a unimodular $n \times n$ circulant and assume that $C = AA'$, where A is an $n \times n$ matrix and A' its transpose. Then it follows that $C = C_1C_1'$ where C_1 is again a circulant.

For general unimodular matrices the assumption $C = AA'$ is stronger than symmetry and positive definiteness if and only if $n \geqslant 8$, as was shown by Minkowski **(1)**. The question therefore arises whether symmetry and positive definiteness suffice even for $n \geqslant 8$ in the theorem above; or in other words, whether a unimodular symmetric positive definite circulant is necessarily of the form AA'. (In this connection it was shown by I. Schoenberg (in a written communication) that a hermitian positive definite circulant with arbitrary complex elements is always of the form $A\bar{A}'$ where A is again a circulant).

It will be shown that the circulant M whose first row is

$$(2, 1, 0, -1, -1, -1, 0, 1)$$

is positive definite, unimodular, but not of the form AA'.

Mordell **(2)** showed that every symmetric positive definite unimodular 8×8 matrix which is not of the form AA' is congruent to the matrix K which corresponds to the quadratic form

$$\sum_{i=1}^{8} x_i^2 + \left(\sum_{i=1}^{8} x_i\right)^2 - 2x_1x_2 - 2x_2x_8.$$

The circulant M therefore is congruent to K.

Received April 12, 1956. The preparation of this paper was sponsored (in part) by the Office of Naval Research.

THEOREM 1. *The circulant M is not of the form AA'.*

Proof. Any matrix of the form AA' corresponds to a quadratic form which represents all integers if $n \geqslant 4$, but certainly represents both odd and even integers for any n. The quadratic form corresponding to M, however, represents only even integers. This proves the theorem.

That M is positive definite can be verified directly. It is no more difficult to characterize all positive definite symmetric unimodular 8×8 circulants. This is done in the following lemma.

LEMMA 1. *Any circulant C whose first row is $(a_0, a_1, \ldots, a_7)$ is unimodular, symmetric, and positive definite if and only if*

$$a_0 = \tfrac{1}{2}(1 + x), \quad a_1 = a_7 = \tfrac{1}{2}y, \quad a_2 = a_6 = 0,$$
$$a_3 = a_5 = -\tfrac{1}{2}y, \quad a_4 = \tfrac{1}{2}(1 - x),$$

where $x > 0$ and $x^2 - 2y^2 = 1$. (The circulant M arises from $x = 3$, $y = 2$.)

Proof. Any circulant C with first row $(a_0, a_1, \ldots, a_7)$ has the eight characteristic roots

$$\alpha_i = \sum_{i=0}^{7} a_i \zeta^i$$

where ζ runs through the eight roots of $x^8 - 1 = 0$. The circulant C is unimodular and positive definite if the algebraic integers α_i are real positive units. From this it follows that C is unimodular, symmetric, and positive definite if and only if

$$(1) \qquad a_0 + 2a_1 + 2a_2 + 2a_3 + a_4 = 1 \qquad (\zeta = 1),$$
$$(2) \qquad a_0 - 2a_1 + 2a_2 - 2a_3 + a_4 = 1 \qquad (\zeta = -1),$$
$$(3) \qquad a_0 - 2a_2 + a_4 = 1 \qquad (\zeta^2 = -1),$$
$$(4) \qquad a_0 - a_4 + (a_1 - a_3)(\zeta - \zeta^3) = \epsilon_1 \qquad (\zeta^4 = -1),$$
$$(5) \qquad a_0 - a_4 - (a_1 - a_3)(\zeta - \zeta^3) = \epsilon_2 \qquad (\zeta^4 = -1),$$

where ϵ_1, ϵ_2 are real and positive units.

The equations (1), (2), (3) imply that $a_2 = 0$, $a_0 + a_4 = 1$, $a_1 + a_3 = 0$. Introducing these relations and $\zeta - \zeta^3 = \pm\sqrt{2}$ for $\zeta^4 = -1$ into (4) and (5) we obtain

$$2a_0 - 1 + 2a_1\sqrt{2} = \epsilon_1,$$
$$2a_0 - 1 - 2a_1\sqrt{2} = \epsilon_2.$$

Hence

$$(6) \qquad (2a_0 - 1)^2 - 8a_1^2 = \epsilon_1\epsilon_2.$$

Since the left side of (6) is rational it follows that $\epsilon_1\epsilon_2 = 1$. Putting $2a_0 - 1 = x$ and $2a_1 = y$ the assertion follows. Since the general solution of $x^2 - 2y^2 = 1$

is given by

$$x - \sqrt{2}\, y = (3 - 2\sqrt{2})^p = (1 - \sqrt{2})^{2p},$$

we find that

$$x - \sqrt{2}y \equiv 3^p - 2p \,.\, 3^{p-1}\sqrt{2}$$
$$\equiv (-1)^p - 2p(-1)^{p-1}\sqrt{2} \qquad (\text{mod } 4).$$

Thus y is always even, and

$$\frac{1+x}{2} \equiv \frac{1+(-1)^p}{2} \qquad (\text{mod } 2),$$

i.e., a_0 is even when p is odd and odd when p is even. Thus the circulants derived from a solution with an even p are congruent to the identity, while those derived from a solution with an odd p are congruent to K.

As the referee pointed out, the two classes of circulants can also be obtained from the fact that every positive definite unimodular 8×8 circulant C is a power of M. For, every power M^n is certainly such a circulant. Conversely, the proof of Lemma 1 shows that there is exactly one such circulant whose characteristic roots are given powers of the characteristic roots of M.

If then n is even, we have $M^n = M^{\frac{1}{2}n}.M^{\frac{1}{2}n} \sim I$ and for n odd we have $M^n = M^{\frac{1}{2}(n-1)}\, M M^{\frac{1}{2}(n-1)} \sim M$.

References

1. H. Minkowski, *Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten*, Gesammelte Abhandlungen *1* (1911), 3–144.
2. L. J. Mordell, *The definite quadratic forms in* 8 *variables with determinant unity*, J. de Math. pures et appliquées, *17* (1938), 41–46.
3. M. Newman and O. Taussky, *On a generalization of the normal basis in abelian algebrain number fields*, Comm. on Pure and Applied Math. *9* (1956), 85–91.
4. O. Taussky, *Unimodular integral circulants*, Math. Zeitschr. *63* (1955), 286–289.

National Bureau of Standards,
Washington 25, *D.C.*