CIRCULANTS AND HORADAM'S SEQUENCES

JEROME MINKUS
Berkeley, California

In a certain problem in knot theory it became necessary to evaluate the following $n \times n$ determinant:

$$(1)\qquad C_n(k,-(2k+1),k) = \begin{vmatrix} k & -(2k+1) & k & 0 & 0 & \cdots & & 0 \\ 0 & k & -(2k+1) & k & 0 & \cdots & & 0 \\ 0 & 0 & k & -(2k+1) & k & \cdots & & 0 \\ & \cdots & & & \cdots & & & \\ 0 & & \cdots & & & k & -(2k+1) & k \\ k & 0 & 0 & & \cdots & 0 & k & -(2k+1) \\ -(2k+1) & k & 0 & & \cdots & 0 & 0 & k \end{vmatrix}$$

where k is an integer. The purpose of this note is to express this determinant (and other determinants of the same form) in terms of Horadam's generalized sequences (see [5]).

$C_n(k,-(2k+1),k)$ belongs to the class of determinants known as "circulants." A determinant is a circulant if each row is a cyclic permutation of the preceding row. If the first row of an $n \times n$ circulant is $(a_0, a_1, \ldots, a_{n-1})$ then the second row will be $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$, the third $(a_{n-2}, a_{n-1}, a_0, \ldots, a_{n-3})$ and so on. If we let $C(a_0, a_1, \ldots, a_{n-1})$ denote the value of the $n \times n$ circulant with first row $(a_0, a_1, \ldots, a_{n-1})$ then the following pretty result holds (see Aitken [1, p. 123] or Muir [8, p. 445]):

Theorem 1: Let $\omega = \exp(2\pi i/n)$. Then

$$(2)\qquad C(a_0, a_1, \ldots, a_{n-1}) = \prod_{j=0}^{n-1} (a_0 + a_1\omega^j + a_2\omega^{2j} + \cdots + a_{n-1}\omega^{(n-1)j}).$$

For the particular case in which we are interested, all but 3 consecutive terms in each row of the determinant vanish. In agreement with (1), we will let $C_n(a_0, a_1, a_2)$ denote the value of the $n \times n$ circulant whose first row is $(a_0, a_1, a_2, 0, \ldots, 0)$. Equation (2) then reduces to

$$(3)\qquad C_n(a_0, a_1, a_2) = \prod_{j=0}^{n-1} (a_0 + a_1\omega^j + a_2\omega^{2j}).$$

Here a_0, a_1, and a_2 may be any real or complex numbers. We will assume throughout that $a_0 \neq 0$. It is also reasonable to assume that $n \geq 3$. It is clear that (up to sign) $C_n(a_0, a_1, a_2)$ is equal to $C(0, \ldots, 0, a_0, a_1, a_2, 0, \ldots, 0)$; i.e., it doesn't really matter where the 3 consecutive terms appear in the first row of the circulant.

As a consequence of Theorem 1 we get:

Corollary 2: Let x_1, x_2 be the roots of the quadratic equation

$$(4)\qquad a_0x^2 + a_1x + a_2 = 0 \quad (a_0 \neq 0).$$

Then

$$(5)\qquad C_n(a_0, a_1, a_2) = a_0^n(x_1^n - 1)(x_2^n - 1).$$

Proof: From (4) it follows that

$$(6)\qquad x_1 + x_2 = -a_1/a_0 \quad \text{and} \quad x_1x_2 = a_2/a_0.$$

Again let $\omega = \exp(2\pi i/n)$. Then

$$a_0^n(x_1^n - 1)(x_2^n - 1) = a_0^n\prod_{j=0}^{n-1}(x_1 - \omega^j)(x_2 - \omega^j) = a_0^n\prod_{j=0}^{n-1}(x_1x_2 - (x_1 + x_2)\omega^j + \omega^{2j})$$

$$= a_0^n\prod_{j=0}^{n-1}(a_2/a_0 + (a_1/a_0)\omega^j + \omega^{2j}) = \prod_{j=0}^{n-1}(a_2 + a_1\omega^j + a_0\omega^{2j}) = \prod_{j=0}^{n-1}(a_0 + a_1\omega^j + a_2\omega^{2j})$$

and the desired result then follows from (3).

Corollary 2 will suffice for our purposes. However, it should be noted that for an arbitrary circulant with first row $(a_0, a_1, \ldots, a_{n-1})$ an analogous result holds relating $C(a_0, \ldots, a_{n-1})$ and $\Pi(x_i^n - 1)$ where $x_1, x_2, \ldots, x_{n-1}$ are the roots of $a_0x^{n-1} + a_1x^{n-2} + \ldots + a_{n-1} = 0$ (compare Muir [8, p. 471]).

Following Horadam [5] for any integers p,q we define the sequences $u_n \equiv u_n(p,q)$ and $v_n \equiv v_n(p,q)$ (for $n \geq 0$) recursively by

(7) $$u_0 = 1, \quad u_1 = p, \quad u_n = pu_{n-1} - qu_{n-2} \quad (n \geq 2)$$

and

(8) $$v_0 = 2, \quad v_1 = p, \quad v_n = pv_{n-1} - qv_{n-2} \quad (n \geq 2)$$

In particular

(9) $$u_{n-1}(1,-1) = F_n \quad (\text{for } n \geq 1)$$

and

(10) $$v_n(1,-1) = L_n \quad (n \geq 2)$$

where $\{F_n\}$ is the ordinary Fibonacci sequence starting with $F_1 = F_2 = 1$ and

(11) $$L_n = F_{n+1} + F_{n-1} \quad (n \geq 2)$$

is the associated Lucas sequence.

The following can be verfied easily (see Horadam [5] and Bachmann [6, Chap. 2, pp. 73-78]):

Lemma 3: Let α,β be the roots of

(12) $$x^2 - px + q = 0$$

and let $d = +\sqrt{p^2 - 4q}$. Then for all $n \geq 0$

(13) $$\alpha^{n+1} - \beta^{n+1} = du_n(p,q)$$

and

(14) $$\alpha^n + \beta^n = v_n(p,q).$$

Equations (13) and (14) remain true even in the "degenerate" case $d = 0$ (i.e., $p^2 = 4q$ and $\alpha = \beta$), but then (13) is no longer useful for determining $u_n(p,q)$. Note further that although p,q are assumed to be rational integers, the recursion formulas (7) and (8) make equally good sense if we allow p and q to take real or complex values. Equations (13) and (14) (and most of the results stated below) remain valid in this more general setting. However, in this note we will restrict ourselves to integer Horadam sequences (and to circulants with integer entries).

Combining Corollary 2 and Lemma 3 gives:

Theorem 4: For any integers a, b, and c ($a \neq 0$),

(15) $$C_n(a,b,c) = a^n + c^n - v_n(-b,ac) \quad (n \geq 3).$$

Proof: From equation (5), we get

(16) $$C_n(a,b,c) = a^n(x_1^n - 1)(x_2^n - 1)$$

where x_1,x_2 are the roots of

(17) $$ax^2 + bx + c = 0.$$

Multiplying (17) by a and letting $z = ax$, we get

(18) $$z^2 + bz + ac = 0.$$

The roots of (18) are $z_1 = ax_1$ and $z_2 = ax_2$. Therefore,

(19) $$z_1 + z_2 = -b \quad \text{and} \quad z_1z_2 = ac.$$

If we let $p = -b$ and $q = ac$ in Lemma 3, then equation (14) becomes

(14′) $$z_1^n + z_2^n = v_n(-b,ac).$$

Now plug $x_i = z_i/a$ ($i = 1,2$) into (16) and use (14′) and (19) to get

$$\begin{aligned} C_n(a,b,c) &= a^n\big((z_1/a)^n - 1\big)\big((z_2/a)^n - 1\big) \\ &= a^n\left(\frac{(z_1z_2)^n}{a^{2n}} + 1 - \frac{(z_1^n + z_2^n)}{a^n}\right) \\ &= c^n + a^n - v_n(-b,ac), \text{ which is equation (15) above.} \end{aligned}$$

Thus we can use properties of $C_n(a,b,c)$ to give us information about $v_n(-b,ac)$ and vice versa. For example:

Corollary 5: For any integers r, a, b, and c ($a \neq 0$,

(20) $$v_n(-rb,r^2ac) = r^n v_n(-b,ac).$$

Proof: Equation (15) implies that

(21) $$C_n(ra,rb,rc) = r^n(a^n + c^n) - v_n(-rb,r^2ac).$$

But $C_n(ra,rb,rc)$ is an $n \times n$ determinant. Therefore,

(22) $$C_n(ra,rb,rc) = r^n C_n(a,b,c) = r^n(a^n + c^n - v_n(-b,ac))$$

and (20) follows.

Equation (20) can also be proved directly [i.e., without introducing $C_n(ra,rb,rc)$] by comparing $(\alpha^n + \beta^n)$ with $(\alpha_0^n + \beta_0^n)$ where α,β (resp. α_0,β_0) are the roots of

$$x^2 + rbx + r^2ac = 0 \quad (\text{resp. } x^2 + bx + ac = 0).$$

When $c = a$ [as is the case in (1) above], then we can express $C_n(c,b,c)$ in terms of Horadam sequences which are different from the sequence $\{v_n(-b,c^2)\}$ given by Theorem 4.

Theorem 6: Let b,c be integers $c \neq 0$. Let $r = -(b + 2c)$ and suppose $r \neq 0$. Let $u_n \equiv u_n(r,-rc)$ and $v_n \equiv v_n(r,-rc)$. Then for each $m \geq 2$,

(23) $$C_{2m-1}(c,b,c) = -(v_{2m-1})^2/r^{2m-1}$$

and

(24) $$C_{2m}(c,b,c) = -(b^2 - 4c^2)(u_{2m-1})^2/r^{2m}.$$

The proof of Theorem 6 depends on:

Lemma 7: Let $r = -(b + 2c)$. Then,

(25) $$(v_{2m-1}(r,-rc))^2 = v_{2m-1}(-rb,(rc)^2) - 2(rc)^{2m-1}$$

and

(26) $$(b^2 - 4c^2)(u_{2m-1}(r,-rc))^2 = v_{2m}(-rb,(rc)^2) - 2(rc)^{2m}.$$

Proof of Lemma 7: We will prove (26) by using (13) and (14). The proof of (25) is almost exactly the same and will be left as an exercise.

Let α,β be the roots of $x^2 - rx - rc = 0$. Then,

(27) $$\alpha\beta = -rc.$$

Choose $\alpha = \dfrac{r + \sqrt{r^2 + 4rc}}{2}$ and $\beta = \dfrac{r - \sqrt{r^2 + 4rc}}{2}$. Note that $d^2 = r^2 + 4rc = b^2 - 4c^2$, since $r = -(b + 2c)$. Using this fact, it is easily verified that

(28) $$\alpha^2 = r\alpha_0 \quad \text{and} \quad \beta^2 = r\beta_0,$$

where $\alpha_0 = \dfrac{-b + \sqrt{b^2 - 4c^2}}{2}$ and $\beta_0 = \dfrac{-b - \sqrt{b^2 - 4c^2}}{2}$ are the roots of $x^2 + bx + c^2 = 0$.

Now applying Lemma 3 (first with respect to α,β and then with respect to α_0,β_0), we get

$$\begin{aligned}(b^2 - 4c^2)(u_{2m-1}(r,-rc))^2 &= (r^2 + 4rc)(u_{2m-1}(r,-rc))^2 \\ &= (du_{2m-1}(r,-rc))^2 = (\alpha^{2m} - \beta^{2m})^2 \\ &= (\alpha^2)^{2m} + (\beta^2)^{2m} - 2(\alpha\beta)^{2m} \\ &= r^{2m}(\alpha_0^{2m} + \beta_0^{2m}) - 2(-rc)^{2m} \quad [\text{using (27) and (28)}] \\ &= r^{2m}v_{2m}(-b,c^2) - 2(rc)^{2m} \\ &= v_{2m}(-rb,(rc)^2) - 2(rc)^{2m} \quad [\text{using (20)}].\end{aligned}$$

Proof of Theorem 6:

$$\begin{aligned}r^{2m-1}C_{2m-1}(c,b,c) &= C_{2m-1}(rc,rb,rc) \\ &= 2(rc)^{2m-1} - v_{2m-1}(-rb,(rc)^2) \quad [\text{using (15)}] \\ &= -(v_{2m-1}(r,-rc))^2 \quad [\text{using (25)}].\end{aligned}$$

This proves (23). Equation (24) follows in the same way from (26).

When $|r| = s^2$, equations (23) and (24) can be rewritten in the following simpler form:

Corollary 8: If $(b + 2c) = \pm s^2$, then for all $m \geq 2$,

(29) $$C_{2m-1}(c,b,c) = \pm(v_{2m-1}(s,\pm c))^2$$

and

(30) $$C_{2m}(c,b,c) = \mp(b - 2c)(u_{2m-1}(s,\pm c))^2.$$

Proof: The proof of (30) depends on the fact that for any integers r, p, and q

(31) $$u_n(rp,r^2q) = r^n u_n(p,q).$$

This is analogous to (20) and is easily seen by comparing $(\alpha^{n+1} - \beta^{n+1})/d$ and $(\alpha_0^{n+1} - \beta_0^{n+1})/d_0$ where α,β (resp. α_0,β_0) are the roots and d (resp. $d_0 = d/r$) is the discriminant of $x^2 - rpx + r^2q = 0$ (resp. $x^2 - px + q = 0$).

Now if $r = -(b + 2c) = \mp s^2$, then it follows from (24) and (31) that

$$C_{2m}(c,b,c) = -(b^2 - 4c^2)(u_{2m-1}(\mp s^2,\pm s^2c))^2/(\mp s^2)^{2m}$$

(32) $$= \frac{-(b^2 - 4c^2)}{s^2}(u_{2m-1}(\mp s,\pm c))^2 = \mp(b - 2c)(u_{2m-1}(\mp s,\pm c))^2,$$

since $-(b^2 - 4c^2) = r(b - 2c) = \mp s^2(b - 2c)$. It also follows from (31) that for any p,q

$$u_n(-p,q) = u_n((-1)p,(-1)^2q) = (-1)^n u_n(p,q).$$

Therefore,

$$(u_{2m-1}(-s,\pm c))^2 = (u_{2m-1}(+s,\pm c))^2$$

and it doesn't matter which sign we choose for s on the right side of (32). This proves (30). The proof of (29) is essentially the same.

Note that if we allow p and q to take on real or complex values in the recursion formulas (7) and (8) defining $u_n(p,q)$ and $v_n(p,q)$ then the above argument shows that (23) and (24) can always be simplified to

(29′) $$C_{2m-1}(c,b,c) = -(v_{2m-1}(\sqrt{r},-c))^2$$

(30′) $$C_{2m}(c,b,c) = (b - 2c)(u_{2m-1}(\sqrt{r},-c))^2$$

where $r = -(b + 2c)$.

If in Corollary 8 we let $b + 2c = p^2$ and $c = q$, then (29) and (30) can be rewritten as

(33) $$C_{2m-1}(q,p^2 - 2q,q) = (v_{2m-1}(p,q))^2$$

and

(34) $$C_{2m}(q,p^2 - 2q,q) = -(p^2 - 4q)(u_{2m-1}(p,q))^2.$$

The cases $b + 2c = \pm 1$ are of particular interest.

If $b + 2c = +1$ and we let $c = k + 1$, then (29) and (30) become

(35) $$C_{2m-1}(k+1,-(2k+1),k+1) = (v_{2m-1}(1,k+1))^2$$

and

(36) $$C_{2m}(k+1,-(2k+1),k+1) = (4k+3)(u_{2m-1}(1,k+1))^2.$$

If $b + 2c = -1$ and $c = k$, then we get

(37) $$C_{2m-1}(k,-(2k+1),k) = -(v_{2m-1}(1,-k))^2$$

and

(38) $$C_{2m}(k,-(2k+1),k) = -(4k+1)(u_{2m-1}(1,-k))^2.$$

For $k = 1$, equations (37) and (38) reduce to

(37′) $$C_{2m-1}(1,-3,1) = -L_{2m-1}^2$$

and

(38′) $$C_{2m}(1,-3,1) = -5F_{2m}^2.$$

(Compare Fielder [2, p. 356].) The determinant dealt with in Fielder's paper is an example of a "continuant"—another important class of determinants (see Muir [8, Chap. XIII]).

The circulants $C_n(k,-(2k+1),k)$ and $C_n(k+1,-(2k+1),k+1)$ arose in the following topological problem: To each pair of odd integers a,b satisfying $a \geq 3$, $|b| < a$, $(a,b) = 1$, there can be associated a "knot with two bridges" (see Schubert [10]). Let $M(n,a,b)$ denote the n sheeted branched cyclic covering the two-bridge knot associated with the pair $\{a, b\}$. Then it can be shown (Minkus [7]) that the one-dimensional integral homology group of

$M(n, 4k + 1, 4k - 1)$ is an abelian group on n generators $A_1, A_2, \ldots, A_n$ subject to the n defining relations $kA_i - (2k + 1)A_{i+1} + kA_{i+2} = 0$ ($i = 1, 2, \ldots, n$), subscripts reduced mod n when necessary. Similarly, the homology group of $M(n, 4k + 3, 4k + 1)$ has defining relations $(k + 1)A_i - (2k + 1)A_{i+1} + (k + 1)A_{i+2} = 0$ ($i = 1, 2, \ldots, n$). Thus, $C_n(k, -(2k + 1), k)$ and $C_n(k + 1, -(2k + 1), k + 1)$ are the determinants of the "relation matrices" of these groups. When these circulants are nonzero, they are (in absolute value) equal to the orders of these groups (compare Fox [3, p. 149]). Note that $C_n(k + 1, -(2k + 1), k + 1)$ and $-C_n(k, -(2k + 1), k)$ are perfect squares for odd values of n, in agreement with the theorem of Plans [9]. In the case $k = 1$ [equations (37′) and (38′) above], the two-bridge knot of type $\{5, 3\}$ is just the figure-eight knot. The homology groups of the branched cyclic coverings of this knot have been determined by Fox and agree with (37′) and (38′) (see [4, p. 193]).

REFERENCES

1. A. C. Aitkin. *Determinants and Matrices*. New York: Interscience Publishers, 1951.
2. D. C. Fielder. "Fibonacci Numbers in Tree Counts for Sector and Related Graphs." *The Fibonacci Quarterly* 12, No. 4 (1974):355-359.
3. R. H. Fox. "A Quick Trip through Knot Theory." In *Topology of 3-Manifolds and Related Topics* (Proc. Univ. of Georgia Inst., 1961), ed. M. K. Fort. Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1962, pp. 120-167.
4. R. H. Fox. "The Homology Characters of the Cyclic Coverings of Knots of Genus One." *Annals of Mathematics* 71, No. 1 (1960):187-196.
5. H. F. Horadam. "Basic Properties of a Certain Generalized Sequence of Numbers." *The Fibonacci Quarterly* 3, No. 3 (1965):161-176.
6. P. Bachmann. *Niedere Zahlentheorie*. Vol. 2. Leipzig: Teubner, 1910.
7. J. B. Minkus. "On the Branched Cyclic Coverings of Knots with Two Bridges." Unpublished material.
8. T. Muir. *A Treatise on the Theory of Determinants*. New York: Dover, 1960.
9. C. McA. Gordon. "A Short Proof of a Theorem of Plans on the Homology of the Branched Cyclic Coverings of a Knot." *Bull. Amer. Math. Soc.* 77, No. 1 (1971).
10. H. Schubert. "Knoten mit zwei Brucken." *Mathematische Zeitschrift* 65 (1956):133-170.

*****

AN EXPANSION OF GOLUBEV'S 11 × 11 MAGIC SQUARE OF PRIMES TO ITS MAXIMUM, 21 × 21

LOREN L. DICKERSON
Huntsville, Alabama

Edgar Karst, in the December 1972 issue of *The Fibonacci Quarterly* presented Golubev's magic square of order 11 consisting of prime numbers of the form $30x + 17$ and asked whether someone is able to attach a frame of order 13. The characteristics in Golubev's square are additionally "magic" in several ways which are repeated from the article cited. The stated requirements imposed were that:

1. All n rows, n columns, and 2 major diagonals have the same sum equal to n x the central number (n x 63317 in Golubev's square).
2. All included numbers be prime numbers equal to 17 plus an integral multiple of 30, with the multiple not divisible integrally by 17.
3. The sums of each pair of opposite (top and bottom or left and right) borders, excepting corner numbers, equal 2 x (the order less 2) x the central number [here 2 x 7 x 63317 or 2 x (n - 2) x 63317].
4. The sums of opposite outer elements in any row or column equal 2 x the central number, for any order.
5. The opposite corner primes in the squares of each order have the sum 2 x the central prime (2 x 63317).

The addition of frames of the order 13 through 21 was as far as I could go with positive primes of form $30x + 17$ centered about 63317, following the rules imposed above. There were about 46 unused primes left over in the series. This is of course not enough for another (23rd-order) frame, but the availability of more primes in the progression suggests the possibility of rearrangements of complementary pairs and that an additional degree of magicality might be accomplished in the 21 x 21 square.