GENERATING FUNCTIONS OF LINEAR DIVISIBILITY SEQUENCES

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

1. INTRODUCTION

A kth-order divisibility sequence is introduced in Hall [3] as a sequence of rational integers $u_0, u_1, u_2, \ldots, u_n, \ldots$ satisfying a linear recurrence relation

$$u_{n+k} = a_1 u_{n+k-1} + \cdots + a_k u_n, \tag{1}$$

where the a's are rational integers, and u_m divides u_n whenever m divides n, for all positive integers m and n.

Some examples follow: 0, 1, 2, 4, 8, ... is a first-order divisibility sequence, while 0, 1, 2, 3, 4, ... is a second-order divisibility sequence. Another second-order divisibility sequence is the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, \ldots,$$

whole recurrence relation is

$$u_{n+2} = u_{n+1} + u_n.$$

If this recurrence relation is generalized to

$$u_{n+2} = xu_{n+1} + yu_n,$$

where x and y are indeterminates, the sequence resulting from the initial terms $u_0 = 0$ and $u_1 = 1$ is the sequence of Fibonacci polynomials. Like the numerical Fibonacci sequence, these polynomials satisfy the divisibility property $u_m | u_n$ (in the ring $I[x, y]$ of polynomials in x and y with integer coefficients) whenever $m | n$. Unlike the Fibonacci numbers, however, the polynomial is irreducible (in $I[x, y]$) whenever the index m is irreducible in I. Thus, the divisibility properties of the more general sequence differ from those of the numerical sequence.

This example and others lead us to extend the coverage of the term kth-order divisibility sequence to include sequences for which any number of the a's in (1) and any number of the initial terms $u_0, u_1, \ldots, u_{k-1}$ are indeterminates. The resulting sequence may then be a sequence of integers, but it may, instead, be a sequence of polynomials in one or more indeterminates $x_1, \ldots, x_p$. In this case, our discussion of divisibility properties refers to arithmetic in the ring $I[x_1, \ldots, x_p]$.

When a divisibility sequence is to be discussed without reference to its recurrence order, we call it a linear divisibility sequence. Thus, a distinction is made between the sequences at hand and nonlinear divisibility sequences, such as the elliptic divisibility sequences studied by Ward [7], [8].

The only known linear divisibility sequences are resultant sequences and their divisors, as defined below. Our purpose in this paper is to discuss generating functions of such sequences. Suppose

$$X(t) = \prod_{i=1}^{p} (t - x_i) \quad \text{and} \quad Y(t) = \prod_{j=1}^{q} (t - y_j)$$

are polynomials with integer coefficients; here, any number of the roots x_i and y_j may be indeterminates. A resultant sequence $\{u_n\}$, $n = 0, 1, \ldots$, is

a sequence of the form

$$u_n = \prod_{j=1}^{q} \prod_{i=1}^{p} \frac{x_i^n - y_j^n}{x_i - y_j}. \tag{2}$$

Thus, $u_n = R_n/R_1$, where $R_n = R_n(X, Y)$ is the resultant of the polynomials

$$\prod_{i=1}^{p} (t - x_i^n) \quad \text{and} \quad \prod_{j=1}^{q} (t - y_j^n).$$

A divisor of a resultant sequence $\{u_n\}$ is a linear divisibility sequence $\{v_n\}$, $n = 0, 1, \ldots$, such that $v_n | u_n$ for $n = 1, 2, \ldots$.

Ward proved in [5] that every resultant sequence is a linear divisibility sequence, and conjectured repeatedly that every linear divisibility sequence is a divisor of a resultant sequence. No proof of this conjecture seems to be known or imminent, even in the case that all the roots are indeterminates!

Before continuing directly toward an investigation of generating functions, we pose another problem, closely related to Ward's conjecture. For (not necessarily distinct) algebraic integers ξ and ζ, let F be the smallest normal field containing both ξ and ζ. Define

$$v_n = \prod_{S} \frac{\xi^n - \zeta^n}{\xi - \zeta}, \quad n = 0, 1, \ldots, \tag{3}$$

the product being taken over all automotphisms S of F. Then the terms v_n are rational integers and the sequence $\{v_n\}$ a linear divisibility sequence. We call this the linear divisibility sequence belonging to ξ, ζ. Suppose now that $\{u_n\}$ is a numerical resultant sequence and that $\{v_n\}$ is a divisor of $\{u_n\}$. Suppose, further, that $u_n = v_n = 1$ and $\{v_n\}$ has no divisors of its own except $(0, 1, 1, \ldots)$ and $\{v_n\}$. Must $\{v_n\}$ be a linear divisibility sequence belonging to some pair of algebraic integers appearing in (2)?

2. RECIPROCAL POLYNOMIALS

Suppose $A \neq 0$. A polynomial

$$H(t) = h_0 + h_1 t + \cdots + h_{2k} t^{2k}$$

of even degree $2k$ is an A-reciprocal polynomial of the first kind if

$$h_{2k-q} = A^{k-q} h_q \quad \text{for } q = 0, 1, \ldots, k,$$

and an A-reciprocal polynomial of the second kind if

$$h_{2k-q} = -A^{k-q} h_q \quad \text{for } q = 0, 1, \ldots, k.$$

In both cases, the roots of $H(t)$ occur in pairs whose product is A; conversely, any polynomial with this property is an A-reciprocal polynomial. A discussion may be found in Burnside and Panton [2, pp. 63-64].

Suppose

$$f = f(t) = \sum_{i=0}^{2k} f_i t^i \quad \text{and} \quad g = g(t) = \sum_{j=0}^{2k} g_j t^j,$$

and write

$$[\alpha, \beta] = \begin{cases} g_\alpha f_\beta - f_\alpha g_\beta & \text{for } \max\{\alpha, \beta\} \leq 2k \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $[\beta, \alpha] = -[\alpha, \beta]$.

Lemma 1a: Suppose

$$0 \le \alpha \le 2k \quad \text{and} \quad 0 \le \beta \le 2k.$$

If f and g are A-reciprocal polynomials of the first kind, then

$$[\alpha, \beta] = A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].$$

Proof:

$$\begin{aligned}[\alpha, \beta] &= g_\alpha f_\beta - f_\alpha g_\beta \\ &= g_{k+q} f_{k+q'} - f_{k+q} g_{k+q'} \\ &= A^q g_{k-q} A^{q'} f_{k-q'} - A^q f_{k-q} A^{q'} g_{k-q'} \\ &= A^{q+q'}[k - q, k - q'] \\ &= A^{\alpha+\beta-2k}[2k - \alpha, 2k - \beta].\end{aligned}$$

Theorem 1a: Suppose

$$F(t) = f_0 + f_1 t + \cdots + f_{2k} t^{2k}$$

and

$$G(t) = g_0 + g_1 t + \cdots + g_{2k} t^{2k}$$

are polynomials of degree $2k > 0$. Let

$$H(t) = F(t)G'(t) - G(t)F'(t) = h_0 + h_1 t + \cdots + h_{4k-1} t^{4k-1}.$$

Suppose $F(t)$ and $G(t)$ are A-reciprocal polynomials of the first kind:

$$f_{k+q} = A^q f_{k-q} \quad \text{and} \quad g_{k+q} = A^q g_{k-q} \quad \text{for } q = 0, 1, \ldots, k.$$

Then $h_{2k-1} = h_{4k-1} = 0$, and $H(t)$ is an A-reciprocal polynomial of the second kind:

$$h_{2k-1+q} = -A^q h_{2k-1-q}, \quad q = 0, 1, \ldots, 2k - 1.$$

Proof:

$$\begin{aligned}H(t) &= \left(\sum_{i=0}^{2k} f_i t^i\right)\left(\sum_{i=0}^{2k-1} (i + 1) g_{i+1} t^i\right) - \left(\sum_{i=0}^{2k} g_i t^i\right)\left(\sum_{i=0}^{2k-1} (i + 1) f_{i+1} t^i\right) \\ &= \sum_{j=0}^{4k-1} t^j \sum_{i=0}^{j} (i + 1)[i + 1, j - i].\end{aligned}$$

Thus, for $q = 0, 1, \ldots, 2k - 1$, we find, after some simplification,

$$h_{2k-1-q} = \sum_{i=0}^{s} (2k - q - 2i)[2k - q - i, i].$$

where

$$s = (2k - q - 2)/2 \text{ for even } q \text{ and } (2k - q - 1)/2 \text{ for odd } q.$$

On the other hand,

$$\begin{aligned}h_{2k-1+q} &= \sum_{i=0}^{2k} (q + 2k - i)[q + 2k - i, i] \\ &= \sum_{i=q}^{2k} (q + 2k - i)[q + 2k - i, i]\end{aligned}$$

(continued)

$$= \sum_{i=0}^{2k-q} (2k - i)[2k - i,\ q + i]$$

$$= \sum_{i=0}^{s} (2k - q - 2i)[2k - i,\ q + i]$$

$$= -A^q \sum_{i=0}^{s} (2k - q - 2i)[2k - q - i,\ i],$$

by Lemma 1a, but this equals $-A^q h_{2k-1-q}$, as desired. In particular, for $q = 0$, we find $h_{2k-1} = -h_{2k-1}$, so that $h_{2k-1} = 0$. That $h_{4k-1} = 0$ follows directly from the definition of $H(t)$.

Lemma 1b: Suppose $0 \le \alpha \le 2k$ and $0 \le \beta \le 2k$. Suppose f and g satisfy

$$g_{k+q} = A^q f_{k-q} \quad \text{for } q = -k, \ldots, 0, \ldots, k.$$

Then

$$[\alpha,\ \beta] = -A^{\alpha+\beta-2k}[2k - \alpha,\ 2k - \beta].$$

Proof:

$$\begin{aligned}[\alpha,\ \beta] &= g_\alpha f_\beta - f_\alpha g_\beta \\ &= g_{k+q} f_{k+q'} - f_{k+q} g_{k+q'} \\ &= A^{q+q'}(f_{k-q} g_{k-q'} - g_{k-q} f_{k-q'}) \\ &= -A^{\alpha+\beta-2k}[2k - \alpha,\ 2k - \beta].\end{aligned}$$

Theorem 1b: Suppose $F(t)$, $G(t)$, and $H(t)$ are as in Theorem 1a, but that for some $A \neq 0$,

$$g_{k+q} = A^q f_{k-q} \quad \text{for } q = -k, \ldots, 0, \ldots, k.$$

Then $h_{4k-1} = 0$, and $H(t)$ is an A-reciprocal polynomial of the first kind:

$$h_{2k-1+q} = A^q h_{2k-1-q} \quad \text{for } q = 0, 1, \ldots, 2k - 1.$$

Proof: The proof is so similar to that of Theorem 1a that it is omitted.

3. GENERATING FUNCTIONS

Suppose $m \ge 1$ and $x_1, \ldots, x_m, y_1, \ldots, y_m$ are (not necessarily distinct) indeterminates. Write

$$X(t) = \prod_{i=1}^{m} (t - x_i) = t^m - X_1 t^{m-1} + \cdots + (-1)^m X_m,$$

$$Y(t) = \prod_{i=1}^{m} (t - y_i) = t^m - Y_1 t^{m-1} + \cdots + (-1)^m Y_m,$$

$$\sigma_0 = 1,\ \sigma_1 = \sum \frac{y_i}{x_i},\ \sigma_2 = \sum \frac{y_{i_1} y_{i_2}}{x_{i_1} x_{i_2}},\ \ldots,\ \sigma_m = \frac{y_1 \cdots y_m}{x_1 \cdots x_m}.$$

Then $\prod_{i=1}^{m} (x_i - y_i) = X_m\left(1 - \frac{y_1}{x_1}\right)\left(1 - \frac{y_2}{x_2}\right) \cdots \left(1 - \frac{y_m}{x_m}\right)$

$$= X_m(1 - \sigma_1 + \sigma_2 - \cdots + (-1)^m \sigma_m)$$

(continued)

$$= \begin{cases} X_m + X_m\sigma_2 + \cdots + X_m\sigma_{m-1} - (X_m\sigma_1 + \cdots + X_m\sigma_m), & \text{odd } m \\ X_m + X_m\sigma_2 + \cdots + X_m\sigma_m - (X_m\sigma_1 + \cdots + X_m\sigma_{m-1}), & \text{even } m. \end{cases} \tag{4}$$

The right side of (4) consists of 2^m terms of the form

$$\pm y_{i_1} y_{i_2} \cdots y_{i_k} x_{i_{k+1}} \cdots x_{i_m}.$$

Let P be the set of those terms having positive coefficient (i.e., an even number of y's) and N the set of those having negative coefficient. In the set $P \cup N$, define a mapping

$$\phi(y_{i_1} y_{i_2} \cdots y_{i_k} x_{i_{k+1}} \cdots x_{i_m}) = y_{i_{k+1}} \cdots y_{i_m} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

If m is odd, ϕ is a one-to-one correspondence between P and N; if m is even, ϕ defines a one-to-one correspondence between P and P, and also between N and N. For each element z of $P \cup N$, we have $z\phi(z) = X_m Y_m$.

At this point, we introduce some more notation. Write

$$x = (x_1, \ldots, x_m),\ y = (y_1, \ldots, y_m),\ \mathcal{A} = (X_m\sigma_0, X_m\sigma_1, \ldots, X_m\sigma_m),$$

$$U_n(x, y) = \sum_{i=1}^{m} (x_i^n - y_i^n),\ n = 0, 1, \ldots,$$

$$\mathcal{F}_n(x, y) = \frac{1}{2}[U_n(x, y) + U_n(x, -y)] = \sum_{\gamma \in P} \gamma^n, \tag{5}$$

$$\mathcal{G}_n(x, y) = \frac{1}{2}[U_n(x, y) - U(x, -y)] = \sum_{\gamma \in N} \delta^n. \tag{6}$$

We index the γ's and δ's in any order, as

$$\gamma_1, \gamma_2, \ldots, \gamma_{2k} \quad \text{and} \quad \delta_1, \delta_2, \ldots, \delta_{2k},$$

where $2k = 2^{m-1}$.

Theorem 2: The sequence $\{u_n\}$ defined by

$$u_n = \frac{U_n}{U_1} = \sum_{i=1}^{m} \frac{x_i^n - y_i^n}{x_i - y_i},\ m \geq 1;\ n = 0, 1, \ldots,$$

is a 2^m-order linear divisibility sequence with generating function

$$\frac{t}{U_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)}, \tag{7}$$

where $F(t)G(t)$ is an $X_m Y_m$-reciprocal polynomial of the first kind, lying in $I[\mathcal{A}, t]$ with degree 2^m in t, and $H(t)$ is an $X_m Y_m$-reciprocal polynomial of the first or second kind, depending on whether m is even or odd, lying in $I[\mathcal{A}, t]$ with degree $2^m - 2$ in t.

Proof: Equation (5) shows that the sum

$$s_n = \sum_{\gamma \in P} \gamma^n$$

is a binary symmetric function (as in Bôcher [1, p. 255]) of the pairs

$$(x_1, y_1), \ldots, (x_m, y_m),$$

namely $X_m\sigma_0$, $X_m\sigma_1$, ..., $X_m\sigma_m$. Since these (ordinary) homogeneous power sums s_n of the γ's thus lie in $I[\mathcal{A}]$, the (ordinary) elementary symmetric functions of the γ's also lie in $I[\mathcal{A}]$. The same is true for the elementary symmetric functions of the δ's. Therefore, the polynomials

$$F(t) = \prod_{i=1}^{2k}(1 - \gamma_i t) \quad \text{and} \quad G(t) = \prod_{j=1}^{2k}(1 - \delta_j t) \tag{8}$$

lie in $I[\mathcal{A}, t]$.

Suppose m is even. Then $F(t)$ is an X_mY_m-reciprocal polynomial of the first kind, since each γ_i is accompanied in $F(t)$ by $\phi(\gamma_i) = X_mY_m\gamma_i^{-1}$. The same is true for $G(t)$. On the other hand, if m is odd, then each γ_i in $F(t)$ equals $X_mY_m\phi(\delta_j) = X_mY_m\gamma_i^{-1}$ for some δ_j in $G(t)$, and conversely for each δ_i in $G(t)$. Thus, $F(t)$ and $G(t)$ are related as in Theorem 1b. In both cases, even m and odd m, the product $F(t)G(t)$ is therefore an X_mY_m-reciprocal polynomial of the first kind.

Since $\{\mathcal{F}_n(x, y)\}$ and $\{g_n(x, y)\}$ are sequences of power sums, we have

$$\sum_{n=0}^{\infty}U_n(x, y)t^n = \sum_{n=0}^{\infty}\mathcal{F}_n(x, y)t^n - \sum_{n=0}^{\infty}g_n(x, y)t^n = \frac{-F'(t)}{F(t)} - \frac{-G'(t)}{G(t)},$$

and (7) follows. Theorems 1a and 1b now apply to the polynomial

$$H(t) = \frac{1}{U_1(x, y)}[F(t)G'(t) - G(t)F'(t)],$$

and the proof of Theorem 2 is finished.

In Theorem 2, the coefficients of the polynomials $H(t)$ and $F(t)G(t)$ lie in $I[\mathcal{A}]$; that is, they themselves are polynomials in the indeterminates $X_m\sigma_0$, $X_m\sigma_1$, ..., $X_m\sigma_m = Y_m$. Of special interest is the possibility that these coefficients lie, *a fortiori*, in the ring

$$I^* = I[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$$

[or a suitable modification of this ring, as in Theorem 2a below; just so that the coefficients in question are polynomials in the coefficients of the underlying polynomials $X(t)$ and $Y(t)$]. If repetition of x_i's and y_i's is allowed, then all these coefficients can possibly lie in I^*. We investigate two such cases in the next section: resultant sequences and certain divisors of resultant sequences which we call Vandermonde sequences. Under the additional hypothesis $X_m = Y_m = 1$, we are able to prove another symmetric property of $H(t)$ and $F(t)G(t)$: as functions of $(X_1, \ldots, X_{m-1}, Y_1, \ldots, Y_{m-1})$, each of their coefficients remains unaltered under the substitution

$$X_i \to X_{m-i}, \; Y_i \to Y_{m-i}, \quad i = 1, \ldots, m - 1.$$

4. RESULTANT SEQUENCES AND VANDERMONDE SEQUENCES

Theorem 2a: Suppose $p \geq 1$, $q \geq 1$, and $p + q \geq 3$. Suppose

$$u_n = \prod_{j=1}^{q}\prod_{i=1}^{p}\frac{x_i^n - y_j^n}{x_i - y_j}, \quad n = 0, 1, \ldots, \tag{2}$$

where

$$X(t) = \prod_{i=1}^{p}(t - x_i) = t^p - X_1t^{p-1} + X_2t^{p-2} - \cdots + (-1)^pX_p, \tag{9}$$

$$(10) \qquad Y(t) = \prod_{j=1}^{q} (t - y_j) = t^q - Y_1 t^{q-1} + Y_2 t^{q-2} - \cdots + (-1)^q Y_q,$$

and

$$I^* = I[X_1, \ldots, X_p, Y_1, \ldots, Y_q].$$

Then, $\{u_n\}$ is a 2^{pq}-order linear divisibility sequence with generating function

$$\frac{t}{R_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)},$$

where

$$R_1 = \prod_{j=1}^{q} \prod_{i=1}^{p} (x_i - y_j)$$

is the resultant of $X(t)$ and $Y(t)$, $F(t)G(t)$ is an $X_p^q Y_q^p$-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree 2^{pq} in t, and $H(t)$ is an $X_p^q Y_q^p$-reciprocal polynomial of the first or second kind, depending on whether p is even or odd, lying in $I^*[t]$ with degree $2^{pq} - 2$ in t.

Proof: Put $m = pq$, $\alpha_k = x_i$ for $iq - q + 1 \le k \le iq$; $i = 1, \ldots, p$, and $\beta_k = y_j$ for $k = \ell q + j$; $\ell = 0, 1, \ldots, p - 1$; $j = 1, \ldots, q$. Then, Theorem 2 applies, where the pairs (x_k, y_k) of Theorem 2 are the pairs (α_k, β_k) of the present discussion. All that remains to be seen is that the coefficients of $H(t)$ and $F(t)G(t)$ lie in I^* and that the dependence of $H(t)$ for first or second kind reciprocity rests on the parity of p alone.

For the latter, we refer to the proof of Theorem 2: Equation (5) shows that for even p, each γ_i occurs in $F(t)$ along with $\phi(\gamma_i) = X_p^q Y_q^p \gamma_i^{-1}$. This makes $F(t)$ an $X_p^q Y_q^p$-reciprocal polynomial of the first kind, and similarly for $G(t)$. For odd p, we find $F(t)$ and $G(t)$ related as in Theorem 1b, and the argument is finished as in the proof of Theorem 2.

Equation (5) also shows that the sum

$$s_n = \sum_{\gamma \in P} \gamma^n$$

is symmetric in $x_1, \ldots, x_p$ and symmetric in $y_1, \ldots, y_q$, since $\mathfrak{F}_n(x, y)$, where $(x, y) = (\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m)$, is a sum of two resultants, each symmetric in $x_1, \ldots, x_p$ and symmetric in $y_1, \ldots, y_q$. Thus, s_n is a polynomial in the elementary symmetric functions of $x_1, \ldots, x_p$ and of $y_1, \ldots, y_q$, namely, the coefficients $X_1, \ldots, X_p$ and $Y_1, \ldots, Y_q$. Each s_n therefore lies in I^*, so that the elementary symmetric functions of the γ's also lie in I^*. The same is true for the elementary symmetric functions of the δ's. Therefore, $F(t)$, $G(t)$, and $H(t)$ all lie in $I^*[t]$.

Theorem 3a: Suppose the generating function $\frac{tH(t)}{F(t)G(t)}$ in Theorem 2a is written out as

$$(11) \qquad \frac{t(h_0 + h_1 t + \cdots + h_{4k-2} t^{4k-2})}{w_0 + w_1 t + \cdots + w_{4k} t^{4k}},$$

where $k = 2^{pq-2}$. Then the coefficients h_i and w_i, regarded as functions of $X_0, \ldots, X_p, Y_0, \ldots, Y_q$, where $X_0 = Y_0 = 1$, satisfy

$$h_i(1, X_{p-1}, \ldots, X_1, 1, 1, Y_{q-1}, \ldots, Y_1, 1) = h_i(1, X_1, \ldots, X_{p-1}, 1, 1, Y_1, \ldots, Y_{q-1}, 1), \quad i = 0, 1, \ldots, 4k-2, \tag{12}$$

$$w_i(1, X_{p-1}, \ldots, X_1, 1, 1, Y_{q-1}, \ldots, Y_1, 1) = w_i(1, X_1, \ldots, X_{p-1}, 1, 1, Y_1, \ldots, Y_{q-1}, 1), \quad i = 0, 1, \ldots, 4k. \tag{13}$$

Proof: Write $x = (x_1, \ldots, x_p)$ and $y = (y_1, \ldots, y_p)$, and consider the effect of the operation of reciprocation,

$$x_i \to x_i^{-1},\ i = 1, 2, \ldots, p \quad \text{and} \quad y_j \to y_j^{-1},\ j = 1, 2, \ldots, q,$$

on the sequence $\{u_n(x, y)\}$ and its generating function. The series belonging to this sequence is transformed into

$$X_p^q Y_q^p[0 + t' + u_2(x, y)t'^2 + u_3(x, y)t'^3 + \cdots], \tag{14}$$

where $t' = t/X_p^q Y_q^p$, and we may write its generating function as

$$\frac{t(h_0' + h_1't + \cdots + h_{4k-2}'t^{4k-2})}{w_0' + w_1't + \cdots + w_{4k}'t^{4k}}, \tag{15}$$

where the h_i' and w_i' are functions of $X_0, \ldots, X_p, Y_0, \ldots, Y_q$. To solve for the h_i' and w_i', note that reciprocation transforms the polynomials (9) and (10) into

$$\frac{(-1)^p}{X_p}[X_0 - X_1t + X_2t^2 - \cdots + (-1)^pX_pt^p]$$

and

$$\frac{(-1)^q}{Y_q}[Y_0 - Y_1t + Y_2t^2 - \cdots + (-1)^qY_qt^q].$$

Therefore

$$h_i' = h_i\left(\frac{X_p}{X_p}, \frac{X_{p-1}}{X_p}, \ldots, \frac{X_0}{X_p}, \frac{Y_q}{Y_q}, \ldots, \frac{Y_0}{Y_q}\right),\ i = 0, 1, \ldots, 4k-2 \tag{16}$$

and

$$w_i' = w_i\left(\frac{X_p}{X_p}, \frac{X_{p-1}}{X_p}, \ldots, \frac{X_0}{X_p}, \frac{Y_q}{Y_q}, \ldots, \frac{Y_0}{Y_q}\right),\ i = 0, 1, \ldots, 4k. \tag{17}$$

If we replace t by $t' = t/X_p^qY_q^p$ in (11) and multiply the resulting rational function by $X_p^qY_q^p$, the series expansion is (14). Thus, (11), as modified, equals (15). Since the degrees of the denominators are equal and $w_0' = w_0 = 1$, we equate denominators and we equate numerators. This gives equal coefficients: $h_i' = h_i$ and $w_i' = w_i$. Equations (16) and (17) now complete the proof

of a more general set of equations than we set out to prove. Clearly, for

$$X_p = Y_q = 1,$$

these equations reduce to (12) and (13).

Theorem 2b: For $p \geq 3$, suppose

$$u_n = \prod_{1 \leq i < j \leq p} \frac{x_i^n - x_j^n}{x_i - x_j}, \quad n = 0, 1, \ldots,$$

where

$$\prod_{i=1}^{p} (t - x_i) = t^p - X_1 t^{p-1} + X_2 t^{p-2} - \cdots + (-1)^p X_p, \tag{9}$$

and

$$I^* = I[X_1, \ldots, X_p].$$

Then $\{u_n\}$ is a $p!$-order linear divisibility sequence with generating function

$$\frac{t}{V_1}\left[\frac{G'(t)}{G(t)} - \frac{F'(t)}{F(t)}\right] = \frac{tH(t)}{F(t)G(t)},$$

where

$$V_1 = \prod_{1 \leq i < j \leq p} (x_i - x_j),$$

$F(t)G(t)$ is an X_p^{p-1}-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree $p!$ in t, and $H(t)$ is an X_p^{p-1}-reciprocal polynomial of the first kind, lying in $I^*[t]$ with degree $p! - 2$ in t.

Proof: As is well known, V_1 is the Vandermonde determinant:

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_p \\ x_1^2 & x_2^2 & \cdots & x_p^2 \\ \vdots & & & \vdots \\ x_1^{p-1} & x_2^{p-1} & \cdots & x_p^{p-1} \end{vmatrix} = (-1)^k \sum x_1^{i_1} x_2^{i_2} \cdots x_p^{i_p},$$

where $\{i_1, i_2, \ldots, i_p\} = \{0, 1, \ldots, p-1\} = \vartheta$ and

$$k_\sigma = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation of } \vartheta \\ 1 & \text{if } \sigma \text{ is an odd permutation of } \vartheta. \end{cases}$$

Half of these $p!$ summands have $k_\sigma = 0$ and the other half, $k_\sigma = 1$. If $p > 3$, then $p!/2$ is even, and each summand $z = x_1^{i_1} x_2^{i_2} \cdots x_p^{i_p}$ with $k_\sigma = 0$ is matched with a summand $X_p^{p-1} z^{-1}$, also with $k_\sigma = 0$; if z has $k_\sigma = 1$, so has $X_p^{p-1} z^{-1}$. The situation is much the same as in the proof of Theorem 2, with one essential difference. Here, the functions $X_p\sigma_0$, $X_p\sigma_1$, ..., $X_p\sigma_p$, where for each

i it is understood that y_i is the x_j appearing with x_i in the product

$$\prod_{i<j}(x_i - x_j),$$

are not symmetric in $x_1, \ldots, x_p$. This is a consequence of the fact that V_1 is not symmetric in $x_1, \ldots, x_p$ [unlike the discriminant V_1^2 of $X(t)$]. We may proceed by dealing directly with the symmetric *quotients*

$$u_n(x) = \frac{x_i^n - x_j^n}{x_i - x_j}$$

rather than the asymmetric products $\prod(x_i^n - x_j^n)$: put

$$\mathcal{F}_n(x) = \frac{1}{2}[u_n(x) + u_n(-x)]$$

and

$$g_n(x) = \frac{1}{2}[u_n(x) - u_n(-x)].$$

The proof for $p > 3$ now follows that of Theorems 2 and 2a so closely that we omit further details.

Consider now the case $p = 3$: for z with $k_\sigma = 0$, we have $X_3^2 z^{-1}$ with $k_\sigma = 1$, and conversely. The polynomials

$$F(t) = (1 - x_1^2 x_2 t)(1 - x_1 x_3^2 t)(1 - x_2^2 x_3 t)$$

and

$$G(t) = (1 - x_1^2 x_3 t)(1 - x_1 x_2^2 t)(1 - x_2 x_3^2 t)$$

are not covered by Theorems 1a and b, since they are of odd degree. Although these theorems can easily be extended to odd-degree polynomials, we choose to defer the case $p = 3$ to the third example in Section 5, where the generating function $tH(t)/F(t)G(t)$ is fully displayed.

Theorem 3b: Suppose the generating function $tH(t)/F(t)G(t)$ in Theorem 2b is written out as

$$\frac{t(h_0 + h_1 t + \cdots + h_{k-2}t^{k-2})}{w_0 + w_1 t + \cdots + w_k t^k},$$

where $k = p!$. Then the coefficients h_i and w_i, regarded as functions of $X_0, \ldots, X_p$ (where $X_0 = 1$) satisfy

$$(12') \qquad h_i(1, X_{p-1}, \ldots, X_1, 1) = h_i(1, X_1, \ldots, X_{p-1}, 1), \quad i = 0, 1, \ldots, k-2,$$

and

$$(13') \qquad w_i(1, X_{p-1}, \ldots, X_1, 1) = w_i(1, X_1, \ldots, X_{p-1}, 1), \quad i = 0, 1, \ldots, k.$$

Proof: The proof is so similar to that of Theorem 3a that we omit it here.

4. REDUCTION OF RECURRENCE ORDER

The definition of *kth-order divisibility sequence* in terms of (1) does not preclude a given kth-order sequence from being a jth-order sequence for

some $j < k$. However, a linear recurrence sequence must be of some *least* recurrence order, and so the following questions arise:

1. When are the recurrence orders of the sequences of §3, as reported, already least possible?
2. When the recurrence order is reducible to a least value k, so that the generating function $tH(t)/F(t)G(t)$ is reducible to a quotient $th(t)/f(t)g(t)$ whose denominator is a polynomial of degree k, then what symmetric properties remain with this reduced generating function?

Clearly, the least recurrence order of a sequence is k if and only if the polynomials $h(t)$ and $f(t)g(t)$ have no common linear factor.

First, we consider the possibilities for common linear factors in case all the x_i's and y_j's are, as in §3, indeterminates. We can then use this information in case some or all of the x_i's and y_j's are algebraic integers.

Possibilities for reduction of generating functions in Theorems 2, 2a, and 2b

1. $H(t)$ has no linear factors in common with $F(t)G(t)$.
2. $F(t)$ and $G(t)$ have a common linear factor.
3. $F(t)$ or $G(t)$ has a repeated linear factor.
4. $H(t)$ has a linear factor in common with $F(t)G(t)$ which is neither a common linear factor of $F(t)$ and $G(t)$ nor a repeated linear factor of $F(t)$ or $G(t)$.

For the general sequences of Theorem 2 and the Vandermonde sequences of Theorem 2b, the second and third possibilities clearly do not occur, since we are dealing with distinct inteterminates. We conjecture that the fourth possibility does not occur for these sequences or for the resultant sequences, either.

For the resultant sequences of Theorem 2a, the second possibility still cannot occur, for, appealing to α's and β's as in the proof of Theorem 2a, the linear divisors of $F(t)$ are all of the form $1 - BAt$ where B is a product of an even number of β's, hence has even weight in the y-indeterminates; on the other hand, the linear divisors of $G(t)$ all involve odd weights in the y-indeterminates.

However, for resultant sequences, the third possibility does occur. It would be difficult to obtain a general classification of occurrences of repeated linear factors within $F(t)$ or $G(t)$, but to acquire some knowledge of such occurrence, we put $p = q = 4$ and seek repeated linear factors: as in the proof of Theorem 2a, we have

$$\begin{aligned} x_1 &= \alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 & y_1 &= \beta_1 = \beta_5 = \beta_9 = \beta_{13} \\ x_2 &= \alpha_5 = \alpha_6 = \alpha_7 = \alpha_8 & y_2 &= \beta_2 = \beta_6 = \beta_{10} = \beta_{14} \\ x_3 &= \alpha_9 = \alpha_{10} = \alpha_{11} = \alpha_{12} & y_3 &= \beta_3 = \beta_7 = \beta_{11} = \beta_{15} \\ x_4 &= \alpha_{13} = \alpha_{14} = \alpha_{15} = \alpha_{16} & y_4 &= \beta_4 = \beta_8 = \beta_{12} = \beta_{16} \end{aligned}$$

The linear factor $1 - y_1y_2x_1^3x_2^3x_3^4x_4^4t$ occurs both as

$$1 - \beta_1\beta_6\alpha_2\alpha_3\alpha_4\alpha_5\alpha_7 \ldots \alpha_{16}t$$

and as

$$1 - \beta_2\beta_5\alpha_1\alpha_3\alpha_4\alpha_6 \ldots \alpha_{16}t.$$

To account for such repetitions, consider the 4 x 4 rectangular array:

	y_1	y_2	y_3	y_4
x_1	1	2	3	4
x_2	5	6	7	8
x_3	9	10	11	12
x_4	13	14	15	16

The sub-array involving 1, 2, 5, 6 corresponds in an obvious way to the equations $\beta_1\beta_6 = \beta_2\beta_5$ and $\alpha_1\alpha_6 = \alpha_2\alpha_5$. Any such occurrence of $\beta_i\beta_j = \beta_\ell\beta_k$ and $\alpha_i\alpha_j = \alpha_\ell\alpha_k$, where $i \neq \ell$, corresponds to a repeated linear factor of $F(t)$ with y-weight 2. The array contains 36 rectangular sub-arrays, each corresponding to a repeated linear factor. A moment's reflection now indicates that there are many more than 36 repeated linear factors of $G(t)$ having y-weight 3, and so on. Since $F'(t)$ and $F(t)$ have a common linear factor whenever $F(t)$ has a repeated linear factor [or the same for $G'(t)$ and $G(t)$], and since

$$H(t) = [F(t)G'(t) - G(t)F'(t)]/R_1,$$

we conclude that the order of recurrence 2^{pq} reported in Theorem 2a can be reduced considerably.

Since $H(t)$ and $F(t)G(t)$ are P-reciprocal polynomials for some P, each linear factor $1 - rt$ of $H(t)$ occurs with $1 - Pr^{-1}t$, and the same pairing occurs in $F(t)G(t)$. For the remainder of this section, we restrict our attention to all the sequences considered in §3 *except* the Vandermonde sequence in the special case $p = 3$. Therefore, in the cases under consideration not only the degree of the denominator, but also that of the numerator, of each generating function, before any possible reductions, is an even positive integer. Accordingly, in the case $1 - rt = 1 - Pr^{-1}t$, this factor occurs an *even* number of times. This remains true in the cases under consideration if any number of the symbols $x_1, \ldots, y_1, \ldots$ represent algebraic integers rather than indeterminates. We summarize and extend these considerations in the following two theorems.

Theorem 4a: For the sequences $\{u_n\}$ of Theorem 2, Theorem 2a, and Theorem 2b (except for $p = 3$), wherein any number of the x_i's and y_i's may be algebraic integers, the least recurrence order k is an even positive integer. The generating function $th(t)/f(t)g(t)$, where $H(t)$ and $F(t)G(t)$ are P-reciprocal polynomials, reduces, by cancellation of common linear factors, to a rational function $th(t)/f(t)g(t)$, where $h(t)\,|\,H(t)$, $f(t)\,|\,F(t)$, and $g(t)\,|\,G(t)$. Moreover, $f(t)g(t)$ is a P-reciprocal polynomial with degree k in t, and $h(t)$ is a P-reciprocal polynomial with degree $k - 2$ in t. The coefficients of these two polynomials lie in $I[\mathcal{A}]$ for the general sequences of Theorem 2, and in I^* for the resultant and Vandermonde sequences of Theorems 2a and 2b.

Proof: All these claims follow easily from the cited theorems, together with the fact that each linear factor $1 - rt$ of $H(t)$ cancels along with another factor, $1 - Pr^{-1}t$. After all such pairs cancel, the remaining linear factors of $h(t)$ and of $f(t)g(t)$ still occur in pairs of the form $1 - rt$, $1 - Pr^{-1}t$, so that we still have P-reciprocal polynomials.

Theorem 4b: The symmetry property for coefficients indicated by (12), (13), (12'), and (13') hold for the coefficients of the reduced polynomials $h(t)$ and $f(t)g(t)$ of Theorem 4a.

Proof: The proof is so similar to that of Theorem 3a that we omit it here.

5. EXAMPLES

Example 1: First, we write out the polynomials $F(t)$, $G(t)$, and $H(t)$ which appear in the generating function of the resultant sequence obtained from $X(t) = (t - x_1)(t - x_2)(t - x_3) = t^3 - at^2 + bt - c$ and $Y(t) = t - d$:

$$F(t) = 1 - (c + ad^2)t + d^2(ac + bd^2)t^2 - cd^4(b + d^2)t^3 + c^2d^6t^4,$$

$$G(t) = 1 - d(b + d^2)t + d^2(ac + bd^2)t^2 - cd^4(c + ad^2)t^3 + c^2d^6t^4,$$

$$H(t) = 1 - d^2(ac + 3cd + bd^2)t^2 + 2cd^3(c + bd + ad^2 + d^3)t^3 - cd^5(ac + 3cd + bd^2)t^4 + c^3d^9t^6.$$

In accord with Theorems 2a and 3a, $H(t)$ is a cd^3-reciprocal polynomial of the first kind, and a and b are interchangeable within each of the coefficients in case $c = d = 1$. Similar observations hold for the product $F(t)G(t)$.

If $c = d = 1$ and $a = b$, then the resultant $R = c + ad^2 - (bd + d^3)$ of $X(t)$ and $Y(t)$ vanishes, and $F(t) = G(t)$ has the root 1 in common with $H(t)$. In this case, the expression

$$\frac{(x_1^n - 1^n)(x_2^n - 1^n)(1^n - 1^n)}{(x_1 - 1)(x_2 - 1)(1 - 1)}$$

formally equals

$$n\frac{(x_1^n - 1)(x_2^n - 1)}{(x_1 - 1)(x_2 - 1)}$$

which generates a sequence of recurrence order less than 8. Nevertheless, this sequence is formally generated by $tH(t)/F(t)G(t)$.

Putting $-a = b = c = d = 1$, we obtain an 8th-order divisibility sequence:

$$0, 1, 2, 1, 8, 11, 14, 34, 64, 109, 242, \ldots .$$

Example 2: Here we examine a divisor of a resultant sequence. Suppose

$$F(t) = (t - x_1)(t - x_2) = t^2 - at - b$$

and

$$G(t) = (t - y_1)(t - y_2) = t^2 - ct - d.$$

Let

$$A_n = (-1)^n(b^n + d^n) \quad \text{and} \quad \Delta^2 = (a^2 + 4b)(c^2 + 4d),$$

and let

$$L_n = x_1^n + x_2^n, \quad \overline{L}_n = y_1^n + y_2^n$$

and

$$F_n = \frac{x_1^n - x_2^n}{x_1 - x_2}, \quad \overline{F}_n = \frac{y_1^n - y_2^n}{y_1 - y_2}, \quad n = 0, 1, \ldots .$$

Each of the latter four expressions is a polynomial in a and b or c and d. The polynomials $L_n = L_n(a, b)$ and $\overline{L}_n(c, d)$ are often called Lucas polynomials, and the polynomials $F_n = F_n(a, b)$ and $\overline{F}_n = \overline{F}_n(c, d)$ are the Fibonacci polynomials mentioned in §1.

The resultant $R_n(F, G)$ of the polynomials $F_n(t) = (t - x_1^n)(t - x_2^n)$ and $G_n(t) = (t - y_1^n)(t - y_2^n)$ can be written as

$$R_n(a, b, c, d) = \frac{1}{4}(L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n)(L_n\overline{L}_n - 2A_n - \Delta F_n\overline{F}_n),$$

since

$$L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n = -2(x_1^n - y_2^n)(x_2^n - y_1^n)$$

and

$$L_n\overline{L}_n - 2A_n - \Delta F_n\overline{F}_n = -2(x_1^n - y_1^n)(x_2^n - y_2^n).$$

Thus, if $(a^2 + 4b)(c^2 + 4d)$ is a perfect square, the sequence with nth term

$$v_n = \frac{L_n\overline{L}_n - 2A_n + \Delta F_n\overline{F}_n}{L_1\overline{L}_1 - 2A_1 + \Delta F_1\overline{F}_1}$$

is a divisor of the resultant sequence

$$\{u_n\} = \{R_n/R_1\}.$$

Writing $D = x_1y_1 + x_2y_2$, we find that the quotient

$$(18) \qquad \frac{1 - bdt^2}{1 + (b + d - D)t + (2bd - bD - dD)t^2 + bd(b + d - D)t^3 + b^2d^2t^4}$$

is a generating function for the sequence $\{v_n\}$.

If we put $D = x$, $-b - d = y$, and $-bd = z$, then the sequence $\{v_n\}$ is the same as the sequence $\{\ell_n(x, y, z)\}$ discussed in detail in [4]. This is a 4th-order divisibility sequence (for which 4 is the least possible order), and as a polynomial in x, we find for $n \geq 2$ the following factorization in terms of linear factors:

$$\ell_n(x, 2\alpha, -\alpha^2 - \beta^2) = \prod_{k=0}^{n-1}(x - 2\alpha \cos 2k\pi/n - 2\beta \sin 2k\pi/n).$$

It seems likely that *every* 4th-order divisibility sequence with $u_0 = 0$ and $u_1 = 1$ is generated by (18) for some choice of b, d, and D. We point out that 3rd-order divisibility sequences are characterized in Hall [3].

Example 3: Here we examine a Vandermonde sequence. Let

$$X(t) = (t - \alpha)(t - \beta)(t - \gamma) = t^3 - At^2 + Bt - C.$$

The Vandermonde sequence whose nth term is

$$(19) \qquad \frac{\alpha^n - \beta^n}{\alpha - \beta} \cdot \frac{\alpha^n - \gamma^n}{\alpha - \gamma} \cdot \frac{\beta^n - \gamma^n}{\beta - \gamma}, \quad n = 0, 1, \ldots,$$

has a generating function

$$\frac{t[1 + 2Ct + C(3C - AB)t^2 + 2C^3t^3 + C^4t^4]}{1 + (3C - AB)t + [B^3 + C(A^3 - 5AB + 6C)]t^2 + C[B(2B^2 - A^2B) + C(7C + 2A^3 - 6AB)]t^3 + C^2[B^3 + C(A^3 - 5AB + 6C)]t^4 + C^4(3C - AB)t^5 + C^6t^6}$$

The first six terms are as follows:

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = AB - C, \quad u_3 = A^2B^2 - B^3 - CA^3$$

$$u_4 = C^3 + 2A^3C^2 - 5ABC^2 + 2B^3C + 3A^2B^2C - 2A^4BC + A^3B^3 - 2AB^4$$

$$u_5 = -C^4 + A^3C^3 + 8ABC^3 + B^3C^2 + A^4BC^2 - 15A^2B^2C^2 - 3A^2B^5 - 3A^5B^2C + AB^4C + 8A^3B^3C + A^6C^2 + A^4B^4 + B^6.$$

For $C = 1$, note that *all* the terms of the sequence are symmetric in A and B, in accord with Theorem 3b.

As a special case, put $A^3 = x$, $B = 0$, and $C = C$. The generating function is then

$$\frac{t(C^2t^2 + Ct + 1)^2}{(C^2t^2 + Ct + 1)^3 + Cx(Ct + 1)^2t^2},$$

and it is easily seen that the numerator and denominator have a common root if and only if $x = 0$, in which case the sequence degenerates to a Fibonacci sequence. Thus, except for $x = 0$, this Vandermonde sequence is of recurrence order 6 and not of any lesser order.

For $A^3 = x$, $B = 0$, $C = 1$, the first nine terms are:

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = -1, \quad u_3 = -x, \quad u_4 = 2x + 1, \quad u_5 = x^2 + x - 1,$$
$$u_6 = -3x^2 - 8x, \quad u_7 = -x^3 - x^2 + 9x + 1, \quad u_8 = 4x^3 + 18x^2 + 6x - 1.$$

It is not difficult to prove that the nth term

$$u_n = u_n(x)$$

of this sequence factors as follows:

$$u_n(x) = (-1)^{n+1} \prod_{k=1}^{\left[\frac{n-1}{2}\right]} [-4x \cos^2 k\pi/n - (4 \cos^2 4\pi/n - 1)^3].$$

We conjecture that $u_n(x)$ is irreducible in $I[x]$ if and only if n is a prime positive integer.

Finally, we list some terms of the numerical 6th-order divisibility sequence $\{u_n(-1)\}$ and remark that

$$|u_n(-1)| \leq F_n \quad (= \text{the } n\text{th Fibonacci number}),$$

for $1 \leq n \leq 100$ and perhaps for all positive integers n.

$$0, 1, -1, 1, -1, -1, 5, -8, 7, 1, -19, 43, -55, 27, 64, -211, 343, -307, -85, 911,$$
$$u_{20} = -1919 = -19 \cdot 101, \quad u_{22} = -989 = -43 \cdot 23$$
$$u_{23} = -3151 = -23 \cdot 137, \quad u_{25} = -15049 = -101 \cdot 149$$
$$u_{27} = 5671 = 53 \cdot 107, \quad u_{54} = -989617855 = 174505u_{27}.$$

REFERENCES

1. Maxime Bôcher. *Higher Algebra.* New York: Macmillan, 1931.
2. William S. Burnside & Arthur W. Panton. *The Theory of Equations*, Vol. 1. New York: Dover, 1960 (1912).
3. Marshall Hall. "Divisibility Sequences of Third Order." *Amer. J. Math.* 58 (1936):577-584.
4. Clark Kimberling. "Divisibility Properties of Recurrent Sequences." *The Fibonacci Quarterly* 14, No. 4 (1976):369-376.
5. Morgan Ward. "Linear Divisibility Sequences." *Trans. AMS* 41 (1937): 276-286.
6. Morgan Ward. "Arithmetical Properties of Sequences in Rings." *Annals of Math.* 39 (1938):210-219.

7. Morgan Ward. "The Law of Apparition of Primes in a Lucasian Sequence." *Trans. AMS* 44 (1948):68-86.
8. Morgan Ward. "Memoir on Elliptic Divisibility Sequences." *Amer. J. Math.* 70 (1948):31-74.
9. Morgan Ward. "The Law of Repetition of Primes in an Elliptic Divisibility Sequence." *Duke Math. J.* 15 (1948):941-946.

*****

LOCAL PERMUTATION POLYNOMIALS IN THREE VARIABLES OVER Z_p

GARY L. MULLEN
The Pennsylvania State University, Sharon, PA 16146

1. INTRODUCTION

If p is a prime, let Z_p denote the integers modulo p and Z_p^* the set of nonzero elements of Z_p. It is well known that every function from $Z_p \times Z_p \times Z_p$ into Z_p can be represented as a polynomial of degree $< p$ in each variable. We say that a polynomial $f(x_1, x_2, x_3)$ with coefficients in Z_p is a *local permutation polynomial* in three variables over Z_p if $f(x_1, a, b)$, $f(c, x_2, d)$, and $f(e, f, x_3)$ are permutations in x_1, x_2, and x_3, respectively, for all a, b, c, d, e, $f \in Z_p$. A general theory of local permutation polynomials in n variables will be discussed in a subsequent paper.

In an earlier paper [2], we considered polynomials in two variables over Z_p and found necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in two variables over Z_p. The number of Latin squares of order p was thus equal to the number of sets of coefficients satisfying the conditions given in [2]. In this paper, we consider polynomials in three variables over Z_p and again determine necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in three variables over Z_p.

As in [1], a *Latin cube of order* n is defined as an $n \times n \times n$ cube consisting of n rows, n columns, and n levels in which the numbers 0, 1, ..., $n - 1$ are entered so that each number occurs exactly once in each row, column, and level. Clearly the number of Latin cubes of order p equals the number of local permutation polynomials in three variables over Z_p. We say that a Latin cube is *reduced* if row one, column one, and level one are in the form 0, 1, ..., $n - 1$. The number of reduced Latin cubes of order p will equal the number of sets of coefficients satisfying the set of conditions given in Section 2.

In Section 3, we use our theory to show that there is only one reduced local permutation polynomial in three variables over Z_3 and, thus, there is precisely one reduced Latin cube of order three.

2. A NECESSARY AND SUFFICIENT CONDITION

Clearly, the only local permutation polynomials in three variables over Z_p are $x_1 + x_2 + x_3$ and $x_1 + x_2 + x_3 + 1$, so that we may assume p to be an odd prime. We will make use of the following well-known formula: