JOURNAL OF COMBINATORIAL THEORY 11, 93–100 (1971)

Generating Operations of Point Algebras

MARSHALL SAADE

Department of Mathematics, University of Georgia, Athens, Georgia 30601

Communicated by Marshall Hall, Jr

Received July 24, 1969

In this paper we define a class C of groupoids on $S^n(=S \times S \times \cdots \times S)$ for arbitrary sets S and integers $n \geqslant 2$. For n a prime we give necessary and sufficient conditions in order for the binary operation $(\cdot)$ of $(S^n, \cdot)$ in C to generate each of the binary operations $(*)$ for all $(S^n, *)$ in C.

1. INTRODUCTION

Let S be a non-empty set, n an integer $\geqslant 2$, and $j(1), j(2),..., j(n)$ a sequence of (not-necessarily distinct) integers such that $1 \leqslant j(i) \leqslant n$, $i = 1,..., n$. A *shuffling operation* (s-operation), $(\cdot)$, on $S^n(=S \times S \times \cdots \times S)$ is defined as follows:

$$(a_1 ,..., a_n) \cdot (b_1 ,..., b_n) = (1_{j(1)} ,..., n_{j(n)}) \tag{1.1}$$

for all $(a_1 ,..., a_n)$, $(b_1 ,..., b_n)$ in S^n, where each $i_{j(i)}$ is a fixed element either equal to $a_{j(i)}$ or $b_{j(i)}$. The elements of S^n are called *points* and the groupoid $(S^n, \cdot)$ is called a *point algebra*.

There are $(2n)^n$ s-operations on S^n if $|S| > 1$. An s-operation $(\cdot)$ is called a *generating operation* if for each other s-operation $(*)$ on S^n there is a polynomial θ in $(\cdot)$, $(a_1 ,..., a_n)$, $(b_1 ,..., b_n)$ such that

$$(a_1 ,..., a_n) * (b_1 ,..., b_n) = \theta(\cdot, (a_1 ,..., a_n), (b_1 ,..., b_n)).$$

In this case we say $(\cdot)$ *generates* $(*)$ (or that $(*)$ is generated by $(\cdot)$).

In his studies of some properties of point algebras for $n = 2$ in [1], Evans comments on generating operations [1, p. 364]. The main result of this paper is thus to give, for n a prime, necessary and sufficient conditions for an s-operation to be a generating operation. The conditions provide a practical test for determining whether or not an s-operation is a generating operation for a given prime n.

The results of this paper are contained in the author's doctoral dissertation which was prepared at Emory University under the direction of Professor Trevor Evans. The author acknowledges the assistance and invaluable criticisms of Professor Evans.

2. Main Result

Before stating the main result we describe two sequences induced by an s-operation. Any operation as described in (1.1) induces a (finite) sequence of positive integers for each k, $1 \leqslant k \leqslant n$, defined as follows. The positive integer $j(k)$ is the subscript in the k-th place of $(1_{j(1)}, \ldots, n_{j(n)})$, $j(j(k))$ is the subscript in the $j(k)$-th place and generally $j(j(\cdots(j(j(k)))\cdots))$ $(i + 1 j\text{'s})$ is the subscript in the $j(j(\cdots(j(j(k)))\cdots))$-th place $(i\ j\text{'s})$, for $0 \leqslant i \leqslant n-1$. If we denote $j(j(\cdots(j(k))\cdots))$ $(t\ j\text{'s})$ by $j^t(k)$ the sequence induced is

$$j(k), j^2(k), \ldots, j^n(k). \tag{2.1}$$

We note that $1 \leqslant j^i(k) \leqslant n$ and that the sequence in (2.1) may or may not be a permutation of $1, 2, \ldots, n$.

Another sequence induced by the point $(1_{j(1)}, \ldots, n_{j(n)})$ is

$$j(1), j(2), \ldots, j(n). \tag{2.2}$$

The main result may now be stated.

Theorem 2.1. *Let n be a prime and let $(\cdot)$ be an s-operation defined as in* (1.1), *where $|S| > 1$. Then the following three conditions are necessary and sufficient for $(\cdot)$ to be a generating operation*:

(i) *For some $j(i)$ and some $j(k)$, $i_{j(i)} = a_{j(i)}$ and $k_{j(k)} = b_{j(k)}$ in the point $(1_{j(1)}, \ldots, n_{j(n)})$.*

(ii) *For some k, $1 \leqslant k \leqslant n$, the sequence in* (2.1) *is a permutation of* $1, \ldots, n$.

(iii) *The sequence in* (2.2) *is a permutation of* $1, \ldots, n$.

We prove in the next three lemmas, for any $n \geqslant 2$, that an operation $(\cdot)$ fails to be a generating operation if any one of the conditions (i), (ii), (iii) of Theorem 2.1 fails to hold. In each proof we produce an s-operation which cannot be generated by $(\cdot)$.

Lemma 2.1. *If condition* (i) *does not hold then $(\cdot)$ is not a generating operation.*

Proof. Suppose in the point $(1_{j(1)}, ..., n_{j(n)})$ all the $i_{j(i)}$ belong to exactly one of the sets $A = \{a_1, ..., a_n\}$ or $B = \{b_1, ..., b_n\}$. Then any product of $(a_1, ..., a_n)$'s or $(b_1, ..., b_n)$'s will be a point containing all coordinates from exactly one of the sets A or B. Thus no s-operation whose product involves coordinates from both A and B can be generated by $(\cdot)$.

Before stating the next lemma we introduce some notations. The symbol $P[(i_1, k_1), ..., (i_r, k_r)]$, will denote any point containing the element i_j in the k_j-th place, $j = 1, ..., r$, where the other coordinates, if any, are not stipulated. The k_j are not ordered in any particular way. Also, in the sequel we will use capital letters, with or without subscripts, to denote points.

LEMMA 2.2. *If condition* (ii) *does not hold then* $(\cdot)$ *is not a generating operation.*

Proof. Suppose for no k, $1 \leqslant k \leqslant n$, is the sequence in (2.1), $j(k), ..., j^n(k)$, a permutation of $1, ..., n$. Since, in particular, $j(1), ..., j^n(1)$ is not a permutation of $1, ..., n$, some one of $1, ..., n$ is not a term of this sequence. Let t be such an integer and consider any s-operation $(*)$ on S^n defined by:

$$(a_1, ..., a_n) * (b_1, ..., b_n) = P[(a_t, j(1))].$$

We show $(*)$ cannot be generated by $(\cdot)$. Since $j(1), ..., j^n(1)$ has n terms each of which is a member of the set $\{1, ..., n\} - \{t\}$ then for some s, $m > 0$, $j^{s+m}(1) = j^s(1)$ where $s + m \leqslant n$. However, noting that

$$\begin{aligned}
P[(a_t, j(1))] &= A_1 \cdot B_1, \quad \text{where} \quad A_1 \text{ or } B_1 \text{ is a } P[(a_t, j^2(1))],\\
P[(a_t, j^2(1))] &= A_2 \cdot B_2, \quad \text{where} \quad A_2 \text{ or } B_2 \text{ is a } P[(a_t, j^3(1))],\\
&\vdots\\
P[(a_t, j^s(1))] &= A_s \cdot B_s, \quad \text{where} \quad A_s \text{ or } B_s \text{ is a } P[(a_t, j^{s+1}(1))],\\
&\vdots\\
P[(a_t, j^{s+m-1}(1))] &= A_{s+m-1} \cdot B_{s+m-1},\\
&\qquad \text{where} \quad A_{s+m-1} \text{ or } B_{s+m-1} \text{ is a } P[(a_t, j^s(1))],\\
P[(a_t, j^s(1))] &= A_{s+m} \cdot B_{s+m},\\
&\qquad \text{where } A_{s+m} \text{ or } B_{s+m} \text{ is a } P[(a_t, j^{s+1}(1))], \text{ etc.,}
\end{aligned}$$

and that $t \neq j^q(1)$ for all q, the conclusion follows.

LEMMA 2.3. *If condition* (iii) *does not hold then* $(\cdot)$ *is not a generating operation.*

Proof. Suppose the sequence in (2.2) is not a permutation of $1, ..., n$.

Then let k be an integer, $1 \leqslant k \leqslant n$, not included in the sequence in (2.2) Then, for example, the s-operation $(*)$ defined by

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_k, \ldots, a_k)$$

cannot be generated by $(\cdot)$ since any product of $(a_1, \ldots, a_n)$'s or $(b_1, \ldots, b_n)$'s under $(\cdot)$ omits a_k.

Thus we have proved the necessity of the three conditions of Theorem 2.1. We note that the necessity proof did not require that n be prime. In order to prove sufficiency of the three conditions we first prove Lemmas 2.4 through 2.9. For these lemmas we assume that the three conditions of the theorem hold for the s-operation $(\cdot)$, where n is a prime and $|S| > 1$, even though we restate that n is prime in lemmas where this fact is used.

LEMMA 2.4. *Let $j(k), \ldots, j^n(k)$ be a permutation of $1, \ldots, n$. Then $j^n(k) = k$.*

Proof. Suppose $j^n(k) \neq k$. Then $j^s(k) = k$ for some $s < n$ since k is one of $1, \ldots, n$. Hence $j^{s+1}(k) = j(k)$ where $s + 1 \leqslant n$. This is false since the $j^i(k)$, $i = 1, \ldots, n$ are distinct.

LEMMA 2.5. *Let $j(k), \ldots, j^n(k)$ be a permutation of $1, \ldots, n$. Then $j(i), \ldots, j^n(i)$ is a cyclic permutation of $j(k), \ldots, j^n(k)$ for each $i = 1, \ldots, n$.*

Proof. Since $j(k), \ldots, j^n(k)$ is a permutation of $1, \ldots, n$, $j(i) = j^s(k)$ for some positive integer s. Hence $j^2(i) = j^{s+1}(k)$, etc. Generally, $j^{n-s}(i) = j^{n-1}(k), j^{n-s+1}(i) = j^n(k)(=k), j^{n-s+2}(i) = j(k), \ldots, j^n(i) = j^{s-1}(k)$.

LEMMA 2.6. *Let n be a prime and let $1 < k \leqslant n$. Then the terms of the following sequence are distinct:*

$$k \bmod n, (2k - 1) \bmod n, \ldots, (ik - (i - 1)) \bmod n, \ldots, (nk - (n - 1)) \bmod n$$

Proof. Suppose $mk - (m - 1) \equiv rk - (r - 1) \bmod n$, where $0 < m, r \leqslant n$. Then $(m - r)(k - 1) \equiv 0 \bmod n$. Thus $n \mid (m - r)(k - 1)$. Since $0 < k - 1 < n$ and n is prime then $n \mid m - r$. However, $|m - r| < n$. Thus $|m - r| = 0$ and $m = r$.

LEMMA 2.7. *Let n be a prime and let $1 \leqslant i \leqslant n$ and $1 < k \leqslant n$. Then the terms of the following sequence are distinct:*

$$j^{k \bmod n}(i), j^{(2k-1) \bmod n}(i), \ldots, j^{(tk-(t-1)) \bmod n}(i), \ldots, j^{(nk-(n-1)) \bmod n}(i). \qquad (2.3)$$

Proof. From Lemma 2.6 the superscripts of the terms of the sequence in (2.3) are distinct and if $a \neq b$, $0 \leqslant a, b \leqslant n-1$ then $j^a(i) \neq j^b(i)$, from condition (ii) and Lemma 2.5. We note that in the sequence in (2.3) one of the superscripts is 0. In this case and in the sequel, $j^0(k) = k(=j^n(k))$.

If a point $P[(x, i), (y, j)]$ of S^n is such that there is a polynomial Ψ in $\cdot$, $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ where

$$P[(x, i), (y, j)] = \Psi(\cdot, (a_1, \dots, a_n), (b_1, \dots, b_n))$$

and such that the x and y of the i-th and j-th places of $P[(x, i), (y, j)]$, respectively, originate from a pair of different points on the right side of the above equation, then we say x and y *split*.

LEMMA 2.8. *Let n be a prime and let $P[(x, i), (y, j)]$ be a point of S^n. Then x and y split.*

Proof. Assume x and y do not split. Then for $i \neq k$,

$$\begin{aligned} &P[(x, i), (y, k)] \text{ is } P[(x, j(i)), (y, j(k))] \cdot V_1 \text{ or } W_1 \cdot P[(x, j(i)), (y, j(k))],\\ &P[(x, j(i)), (y, j(k))] \text{ is } P[(x, j^2(i)), (y, j^2(k))] \cdot V_2 \text{ or } W_2 \cdot P[(x, j^2(i)), (y, j^2(k))]\\ &\quad\vdots\\ &P[(x, j^{n-1}(i)), (y, j^{n-1}(k))] \text{ is } P[(x, j^n(i)), (y, j^n(k))] \cdot V_n\\ &\qquad\qquad\text{ or } W_n \cdot P[(x, j^n(i)), (y, j^n(k))], \end{aligned}$$

that is,

$$P[(x, j^{n-1}(i)), (y, j^{n-1}(k))] \text{ is } P[(x, i), (y, k)] \cdot V_n \text{ or } W_n \cdot P[(x, i), (y, k)].$$

Referring to the definition of $(\cdot)$,

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (1_{j(1)}, \dots, n_{j(n)}),$$

and to the sets $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$, we note (using in the remainder of the proof of this lemma the symbol $c\{j^t(k)\}$ to denote $c_{j^t(k)}$, for $t = 1, \dots, n$ and similarly for $c_{j^t(i)}$):

$$\begin{aligned} &c\{j(k)\} \text{ and } c\{j(i)\} \text{ are both in } A \text{ or both in } B,\\ &c\{j^2(k)\} \text{ and } c\{j^2(i)\} \text{ are both in } A \text{ or both in } B, \qquad (2.4)\\ &\quad\vdots\\ &c\{j^n(k)\} \text{ and } c\{j^n(i)\} \text{ are both in } A \text{ or both in } B, \end{aligned}$$

where, from Lemma 2.5, $j(i), \dots, j^n(i)$ is a cyclic permutation of $j(k), \dots, j^n(k)$. Thus (since $i \neq k$) there is an s, $1 < s \leqslant n$, such that

$$j(i) = j^s(k), \dots, j^{n-s+1}(i) = j^n(k)(=k), \dots, j^n(i) = j^{s-1}(k). \qquad (2.5)$$

We note in (2.5) that for each r, $1 \leqslant r \leqslant n$, $j^r(i) = j^{[s+(r-1)] \bmod n}(k)$. From Lemma 2.7 the terms of the sequence

$$j(k), j^{s \bmod n}(k), j^{(2s-1) \bmod n}(k), \ldots, j^{[(n-1)s-(n-2)] \bmod n}(k) \qquad (2.6)$$

are distinct, noting that $j(k) = j^{(ns-(n-1)) \bmod n}(k)$ in the sequence (2.3). Using (2.5) and (2.6) we may restate (2.4) (with the n statements in a possibly different order) as:

$$\begin{gathered} c\{j(k)\} \text{ and } c\{j^{s \bmod n}(k)\} \text{ are both in } A \text{ or both in } B, \\ c\{j^{s \bmod n}(k)\} \text{ and } c\{j^{(2s-1) \bmod n}(k)\} \text{ are both in } A \text{ or both in } B, \\ \vdots \\ c\{j^{[(n-1)s-(n-2)] \bmod n}(k)\} \text{ and } c\{j(k)\} \text{ are both in } A \text{ or both in } B. \end{gathered} \qquad (2.7)$$

Thus from (2.7) we deduce that

$$c\{j(k)\},\ c\{j^{s \bmod n}(k)\},\ c\{j^{(2s-1) \bmod n}(k)\}, \ldots,\ c\{j^{[(n-1)s-(n-2)] \bmod n}(k)\}$$

are all in A or all in B, that is, $c\{j(k)\}, \ldots, c\{j^n(k)\}$ are all in A or all in B. Since $\{j(k), \ldots, j^n(k)\} = \{j(1), \ldots, j(n)\}$ this means $c\{j(1)\}, \ldots, c\{j(n)\}$ are all in A or all in B. This contradicts condition (i) of Theorem 2.1. Hence x and y split.

LEMMA 2.9. *Let n be a prime and let i, k, be integers such that $1 \leqslant i$, $k \leqslant n$. Then if $x = (a_1, \ldots, a_n)$ there is a polynomial $\theta(\cdot, x)$ such that*

$$\theta(\cdot, x) = P[(a_i, k)] \quad \text{for some} \quad P[(a_i, k)].$$

Proof. Since $j(k), \ldots, j^n(k)(= k)$ is a permutation of $1, \ldots, n$ there is an integer s, $1 \leqslant s \leqslant n$ such that $i = j^s(k)$. Let x be denoted by $P[(a_i, i)] = P[(a_i, j^s(k))]$. Then

$$\begin{gathered} x^2 = P[(a_i, j^{s-1}(k))] = A_1 \text{ for some } P[(a_i, j^{s-1}(k))], \text{ either } x \cdot A_1 \text{ or } A_1 \cdot x \\ \text{is } P[(a_i, j^{s-2}(k))] = A_2 \text{ for some } P[(a_i, j^{s-2}(k))], \\ \vdots \\ \text{either } x \cdot A_{s-1} \text{ or } A_{s-1} \cdot x \text{ is } P[(a_i, k)] = A_s \text{ for some } P[(a_i, k)]. \end{gathered}$$

Thus A_s is a product of x's. Let $\theta(\cdot, x) = A_s$. Hence

$$\theta(\cdot, x) = P[(a_i, k)] \quad \text{for some} \quad P[(a_i, k)].$$

Proof of Theorem 2.1 (sufficiency). Let $(*)$ be an s-operation defined by

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (d_1, \ldots, d_n) = D$$

for all $(a_1, ..., a_n)$, $(b_1, ..., b_n)$ in S^n. In particular each d_i is in $\{a_1, ..., a_n\}$ or $\{b_1, ..., b_n\}$. By a simple induction argument, applying Lemma 2.8, we see D can be written as a product (under $(\cdot)$) of points $P_1[(d_1, k_1)], ..., P_n[(d_n, k_n)]$, $P_{n+1}, ..., P_t$ with the following properties: for $i = 1, ..., n$, $P_i[(d_i, k_i)]$ is a point containing d_i in its k_i-th place and such that, after carrying out the multiplication of these points, the d_i in the i-th place of D originated from the k_i-th place of P_i. (The other places of $P_i[(d_i, k_i)]$ are of course arbitrary.) If there are any other points $P_{n+1}, ..., P_t$ in this product they are arbitrary and hence we let each of these be $(a_1, ..., a_n)$. Since in each $P_i[(d_i, k_i)]$, $i = 1, ..., n$, the other $n - 1$ places are arbitrary, we see from Lemma 2.9 there are polynomials $\theta_i(\cdot, x)$ (where x is $(a_1, ..., a_n)$ or $(b_1, ..., b_n)$) such that

$$\theta_i(\cdot, x) = P[(d_i, k_i)] \quad \text{for some} \quad P[(d_i, k_i)].$$

Thus we conclude there is a polynomial $\theta(\cdot, (a_1, ..., a_n), (b_1, ..., b_n))$ such that

$$(d_1, ..., d_n) = \theta(\cdot, (a_1, ..., a_n), (b_1, ..., b_n)).$$

This concludes the proof of Theorem 2.1.

3. A Related Result

Theorem 3.1. *Let $n > 1$ and not a prime. There is an s-operation, $(\cdot)$, satisfying conditions* (i), (ii), *and* (iii) *of Theorem* 2.1 *and such that $(\cdot)$ is not a generating operation.*

Proof. Let $n = xy$, x, y integers and $x \geqslant 2$ and $y \geqslant 2$. Let $k = x + 1$. Consider the n-termed sequence

$$\begin{aligned}&(k+1) \bmod n,\ 2k \bmod n, ..., (qk - (q-2)) \bmod n, ...,\\ &(nk - (n-2)) \bmod n\ (= 2).\end{aligned} \tag{3.1}$$

The terms of the sequence in (3.1) are not distinct. In particular,

$$((y+1)k - (y-1)) \equiv (k+1) \bmod n,$$

where clearly $y + 1 < n$. We construct an s-operation, $(\cdot)$, as follows:

$$(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (c_2, c_3, ..., c_n, c_1),$$

where $c_i = a_i$ for each i in the sequence of (3.1) and $c_j = b_j$ for each j not a member of the sequence. Clearly $(c_2, c_3, ..., c_n, c_1)$ contains both a_i

and b_j terms. It is easily seen that the s-operation, $(\cdot)$, satisfies conditions (i), (ii), and (iii) of Theorem 2.1. We now show that no point, $P[(a_1, 2), (b_1, k+1)]$, will split under $(\cdot)$. This is seen easily since by construction of $(\cdot)$, if i and j occur in the same column of the array

$$\begin{array}{cccccc} 2 & 3,\ldots, & i,\ldots, n-k+1, & n-k+2,\ldots, & 1 \\ k+1 & k+2,\ldots, & k+(i-1),\ldots, n, & 1,\ldots, & k, \end{array}$$

then either $c_i = a_i$ and $c_j = a_j$ or $c_i = b_i$ and $c_j = b_j$. That is, the following situation occurs (where $k+i$ below means $(k+i) \bmod n$):

$$\begin{aligned} P[(a_1, 2), (b_1, k+1)] &\text{ is } V_1 \cdot P[(a_1, 3), (b_1, k+2)] \text{ or} \\ &\qquad P[(a_1, 3), (b_1, k+2)] \cdot V_1, \\ P[(a_1, 3), (b_1, k+2)] &\text{ is } V_2 \cdot P[(a_1, 4), (b_1, k+3)] \text{ or} \\ &\qquad P[(a_1, 4), (b_1, k+3)] \cdot V_2, \\ &\vdots \\ P[(a_1, 1), (b_1, k)] &\text{ is } V_n \cdot P[(a_1, 2), (b_1, k+1)] \text{ or} \\ &\qquad P[(a_1, 2), (b_1, k+1)] \cdot V_n. \end{aligned}$$

Hence it follows that $(\cdot)$ is not a generating operation since, in particular, no operation $(*)$ defined by

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = P[(a_1, 2), (b_1, k+1)]$$

can be generated by $(\cdot)$.

Reference

1. T. Evans, Product of points—some simple algebras and their identities, *Amer. Math. Monthly* **74** (1967), 362–372.