6. *Conclusion.* This method of analysis of straight-line nets by the contiguous segments, as herein extended to all the lines in the system, regardless of their relation to a pentagon, hexagon, or other basal polygon, is applicable to any number n of straight lines and is even not restricted to the case that only $m=2$ lines shall pass through a point. The method furnishes a *necessary and sufficient* test for the equivalence or the non-equivalence of two systems of straight lines, and in the case of two equivalent systems this method simplifies the discovery of the substitution which transforms the one system into the other system.

VASSAR COLLEGE

A PRACTICAL METHOD FOR THE MODULAR REPRESENTATION OF FINITE OPERATIONS AND RELATIONS*

BY B. A. BERNSTEIN AND NEMO DEBELY

1. *Introduction.* In previous papers one of the writers developed a general theory for the concrete representation of arbitrary operations and relations in a finite class of elements.† Let p be a prime, and let a mod p denote the least positive integer obtained from integer a by dropping multiples of p. Consider the function $f(x)$ given by

$$f(x) = c_0 + c_1x + \cdots + c_{p-1}x^{p-1}, \qquad \text{mod } p, \tag{1}$$

where x ranges over the complete system of p-residues $0, 1, \cdots, p-1$, and where the coefficients c_i are among the p-residues. The general theory is based on the fact that any unary operation in a class K of p elements, the operation satisfying the condition of closure, can be represented by a polynomial of form (1). But when the number of elements in K is large, the calculation of (1) by the method of the general theory is very laborious, for the work involves, for a class of p elements, the computation modulo p of p determinants each of order $p-1$. For an m-ary operation or an m-adic relation where $m>2$, the calculation of the representation by the method of the general theory is very laborious

* Presented to the Society, April 5, 1930.

† See the Proceedings of the International Mathematical Congress, Toronto, 1924, p. 207, and this Bulletin, vol. 32, p. 533.

even when p is as small as 3. Moreover, the method of the theory is not at all adapted to cases in which p is a letter instead of a given number. The present paper gives a method of obtaining with extreme ease the representations of the theory for operations and relations of any complexity and for p literal or a number of any magnitude.

2. *The Unit-Zero Functions.* The method of the present paper makes fundamental the notion of *unit-zero function.* A function $f(x)$ will be called a *unit-zero function with respect to a* if $f(x)=1$ or 0, according as $x=a$ or $x\neq a$. In general, a function $f(x_1, x_2, \cdots, x_m)$ will be called a *unit-zero function with respect to the sequence* $a_1, a_2, \cdots, a_m$ if $f(x_1, x_2, \cdots, x_m)=1$ or 0, according as the equalities $x_i=a_i$, $(i=1, 2, \cdots, m)$, do or do not all hold. The functions with which our theory is concerned are all *polynomials modulo p*, where p is prime. A unit-zero function with respect to the sequence $a_1, a_2, \cdots, a_m$, if the function be a polynomial modulo p in $x_1, x_2, \cdots, x_m$, will be denoted by $(x_1, x_2, \cdots, x_m; a_1, a_2, \cdots, a_m)_p$.

The unit-zero functions $(x; a)_p$ and $(x_1, x_2, \cdots, x_m; a_1, a_2, \cdots, a_m)_p$ can be readily written down. Indeed, by Fermat's theorem, we have

$$(2) \qquad (x; a)_p = 1 - (x - a)^{p-1}, \bmod p,$$

$$(2') \qquad = 1 + (p - 1)\sum_{k=0}^{p-1} a^k x^{p-1-k}, \bmod p.$$

And, evidently,

$$(3) \quad (x_1, x_2, \cdots, x_m; a_1, a_2, \cdots, a_m)_p = (x_1; a_1)_p (x_2; a_2)_p \cdots (x_m; a_m)_p.$$

From the nature of the unit-zero function we have

$$(4) \quad a(x_1, x_2, \cdots, x_m; a_1, a_2, \cdots, a_m)_p + b(x_1, x_2, \cdots, x_m; b_1, b_2, \cdots, b_m)_p = a, \text{ or } b, \text{ or } 0,$$

according as $x_i=a_i$ all hold, or $x_i=b_i$ all hold, or neither $x_i=a_i$ all hold nor $x_i=b_i$ all hold, $(i=1, 2, \cdots, m)$.

3. *Representations.* The method of representing finite operations and relations by means of unit-zero functions can now be stated. Let K be a finite class of n elements. These elements may be denoted by $0, 1, \cdots, n-1$. The representations of

operations O and relations R in K are given in cases (A)-(E) below.

(A). *O a K-closing m-ary operation, n a prime p.* There is a K-element $e_{a_1a_2\cdots a_m}$ for every sequence of m elements $a_1, a_2, \cdots, a_m$ of K. From (4), the representation of O is the function

$$(5)\quad \sum_{a_1=0}^{p-1} \cdots \sum_{a_{m-1}=0}^{p-1} \sum_{a_m=0}^{p-1} e_{a_1a_2\cdots a_m}(x_1, x_2, \cdots, x_m; a_1, a_2, \cdots, a_m)_p.$$

Thus, the representation of the operation

(i)

	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

is the function $f(x, y)$ given by

$$\text{(ii)}\quad \begin{aligned} f(x, y) &= 2(x, y; 0, 1)_3 + (x, y; 0, 2)_3 + (x, y; 1, 0)_3 \\ &\quad + 2(x, y; 1, 2)_3 + 2(x, y; 2, 0)_3 + (x, y; 2, 1)_3 \\ &= x + 2y, \text{mod } 3. \end{aligned}$$

(B). *O an m-ary operation not K-closing, n a prime p.* There are sequences

$$\alpha_{11}, \alpha_{12}, \cdots, \alpha_{1m}; \alpha_{21}, \alpha_{22}, \cdots, \alpha_{2m}; \cdots; \alpha_{k1}, \alpha_{k2}, \cdots, \alpha_{km}$$

to which no K-elements correspond. Let O' be the operation obtained from O by assigning some K-element, 0 for convenience, to each of these sequences. Let $\phi(x_1, x_2, \cdots, x_m)$ be the function, obtained as in (A), representing O'. The representation of O is the function

$$(6)\quad \phi(x_1, x_2, \cdots, x_m) + \sum_{i=1}^{k} 0/\{1 - (x_1, x_2, \cdots, x_m; \alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{im})_p\}.$$

Thus, consider the operation $f(x)$ defined by

(iii)

x	0	1	2	3	4
$f(x)$	2	—	0	—	1

where $f(1)$ and $f(3)$ do not belong to the class $0, 1, \cdots, 4$. Take the operation $\phi(x)$ defined by

(iv)
$$\begin{array}{c|ccccc} x & 0 & 1 & 2 & 3 & 4 \\ \hline \phi(x) & 2 & 0 & 0 & 0 & 1 \end{array}.$$

The representation of (iv) is given by

(v) $$\phi(x) = 2(x; 0)_5 + (x; 4)_5.$$

Hence, the representation of (iii) is given by

(vi) $$f(x) = \phi(x) + 0/\{1 - (x; 1)_5\} + 0/\{1 - (x; 3)_5\}$$
$$= 3 - 2x^4 - (x-4)^4 + 0/(x-1)^4 + 0/(x-3)^4, \text{ mod } 5.$$

(C). *O an m-ary operation in K, n not prime.* Consider a class K' of p elements $0, 1, \cdots, n-1, \cdots, p-1$, where *$p$ is a prime exceeding n.* Let O' be any operation in K' identical with O for all the sequences of m elements taken from the K-elements $0, 1, \cdots, n-1$. For convenience, we may have O' assign 0 to each of the sequences in K' that are not in K. Let $\phi(x_1, x_2, \cdots, x_m)$ be the representation of O', obtained as in (A) or (B). The representation of O is the function $\phi(x_1, x_2, \cdots, x_m)$ *in which the x_i range over the K-elements* $0, 1, \cdots, n-1$.

Thus, the representation of the operation $f(x)$ defined by

(vii)
$$\begin{array}{c|cccc} x & 0 & 1 & 2 & 3 \\ \hline f(x) & 2 & 1 & 0 & 4 \end{array}$$

is the representation of the operation $\phi(x)$ defined by

(viii)
$$\begin{array}{c|ccccc} x & 0 & 1 & 2 & 3 & 4 \\ \hline \phi(x) & 2 & 1 & 0 & 4 & 0 \end{array},$$

with x ranging over the elements 0, 1, 2, 3.

(D). *R an m-adic relation in K, n a prime p.* Let the sequences which satisfy R be

$$\alpha_{11}, \alpha_{12}, \cdots, \alpha_{1m}; \alpha_{21}, \alpha_{22}, \cdots, \alpha_{2m}; \cdots; \alpha_{k1}, \alpha_{k2}, \cdots, \alpha_{km}.$$

The representation of R is the equation modulo p

(7) $$\sum_{i=1}^{k}(x_1, x_2, \cdots, x_m; \alpha_{i1}, \alpha_{i2}, \cdots, \alpha_{im})_p = 1.$$

Thus, the representation of the dyadic relation defined by

(ix)

	0	1	2
0	−	+	+
1	−	−	+
2	−	−	−

is the modular equation

(x) $$(x, y; 0, 1)_3 + (x, y; 0, 2)_3 + (x, y; 1, 2)_3 = 1.$$

(E). *R an m-adic relation in K, n not prime.* Consider a class K' of p elements $0, 1, \cdots, n-1, \cdots, p-1$, where p is a prime exceeding n. Let R' be any m-adic relation in K' identical with R for all the sequences of m elements taken from the K-elements $0, 1, \cdots, n-1$. For convenience we may have R' contradicted for all the sequences in K' that are not in K. Let the representation of R', obtained as in (D), be the equation modulo p

(8) $$\phi(x_1, x_2, \cdots, x_m) = 1.$$

The representation of R is equation (8), with the x_i *ranging over the K-elements* $0, 1, \cdots, n-1$.

Thus, the representation of the relation R defined by

(xi)

	0	1	2	3
0	−	+	+	+
1	−	−	+	+
2	−	−	−	+
3	−	−	−	−

is the representation of the relation R defined by

(xii)

	0	1	2	3	4
0	−	+	+	+	−
1	−	−	+	+	−
2	−	−	−	+	−
3	−	−	−	−	−
4	−	−	−	−	−,

with x, y ranging over the elements 0, 1, 2, 3.

THE UNIVERSITY OF CALIFORNIA