ON GENERATING THE SIMPLE GROUP $LF(2, 2^N)$ BY TWO OPERATORS OF PERIODS TWO AND THREE*

ABRAHAM SINKOV

The purpose of this paper is to consider the question of the number of abstractly distinct ways in which it is possible for two operators of periods two and three to generate the simple group $LF(2, 2^N)$. The general procedure to be followed in studying such a problem has been outlined by Professor Brahana† and has already been applied to $LF(2, 2^3)$ by the author.‡ Those previous results suggested the present generalization.

Since the $2^{2N}-1$ substitutions of period two in $LF(2, 2^N)$ are all conjugate,§ it is sufficient in seeking possible generating operators to consider only one of them, say

$$T \equiv \left(\frac{1, 1}{0, 1}\right).$$

In the representation of G on 2^N+1 letters, T leaves fixed the single element ∞. The largest subgroup within which T is invariant is $G^{(\infty)}$, composed of all the substitutions

$$T_\mu \equiv \left(\frac{1, \mu}{0, 1}\right), \qquad \mu \text{ in the } GF[2^N],$$

which keep the single element ∞ unchanged. The group $G(^\infty)$ is abelian, of order 2^N and of type $(1, 1, 1, \cdots)$.

If the operators of period three are divided up into sets of complete conjugates under $G^{(\infty)}$, then the various members of each set satisfy with T the same abstract relations, and it is sufficient to select from each such set only one operator to serve as a possible second generator with T. The number of these sets to be considered depends

* Presented to the Society, February 20, 1937.

† H. R. Brahana, *Pairs of generators for the known simple groups whose orders are less than one million*, Annals of Mathematics, vol. 31 (1930), pp. 542, 543.

‡ *Necessary and sufficient conditions for generating certain simple groups by two operators of periods two and three*, American Journal of Mathematics, vol. 49 (1937), pp. 69–72, hereafter referred to as *Necessary and sufficient conditions*.

§ The various properties of $LF(2, 2^N)$ of which use is made in this paper are given in Dickson's *Linear Groups with an Exposition of the Galois Field Theory*, 1901, chap. 12.

on the form of 2^N+1. For, when 2^N+1 is a multiple of three, G contains $2^N(2^N-1)$ operators of period three, whereas when 2^N+1 is not a multiple of three, there are $2^N(2^N+1)$ such operators.

In the former case, there are 2^N-1 sets of 2^N operators each, and we may choose as a representative from each set the operator

$$S_\alpha \equiv \left(\begin{array}{cc} 0, & x^{2\alpha} \\ \hline 1, & x^\alpha \end{array}\right), \qquad \alpha = 0, 1, 2, \cdots, 2^N-2,$$

where x is a primitive root of the $GF[2^N]$. In the latter case, there are 2^N+1 sets of 2^N operators each. We may again choose the 2^N-1 operators S_α together with the two additional operators

$$S_{2^N} \equiv \left(\begin{array}{cc} x^{(2^N-1)/3}, & 0 \\ \hline 0, & 1 \end{array}\right)$$

and $S_{2^N+1}=(S_{2^N})^2$. Since

$$S_{2^N}T = \left(\begin{array}{cc} x^{(2^N-1)/3}, & x^{(2^N-1)/3} \\ \hline 0, & 1 \end{array}\right)$$

is of period three, S_{2^N} and T generate a tetrahedral group of order 12. The same is true of S_{2^N+1} and T, so that neither of these pairs can be used to generate the entire group. Moreover, S_0T is of period two, so that $\{S_0, T\}$ is of order six. In every case then, it is sufficient to consider only the 2^N-2 operators S_α, $(\alpha\neq 0)$.

Now it may happen, for a particular subscript k, that T and S_k generate a proper subgroup H of G instead of the entire group. We note however that

$$S_\alpha T = \left(\begin{array}{cc} 0, & x^{2\alpha} \\ \hline 1, & 1+x^\alpha \end{array}\right)$$

may not be of period 2, 3, or 4 for any α whatever. Hence, on referring to the list of possible subgroups of $LF(2, 2^N)$, one sees that H is either a linear fractional group $LF(2, 2^{N/r})$ or else is of order 2^sd. But the latter case may be ruled out. For, if a subgroup H of order 2^sd existed, the commutative subgroup within it of order 2^s would include the commutator subgroup of H. Hence d, and therefore the period of $S_\alpha T$, is at most three,* which is not possible.

H is therefore a linear fractional group, and the number x^k must be an element in the $GF[2^{N/r}]$. If we set $N/r=t$, then $(x^k)^{2^t-1}=1$, from which $k(2^t-1)\equiv 0$ modulo (2^N-1). The number k is thus re-

* H. R. Brahana, *Certain perfect groups generated by two operators of periods two and three*, American Journal of Mathematics, vol. 50 (1928), p. 348.

quired to be a multiple of $(2^N-1)/(2^t-1)$. This condition is also sufficient, since every subscript which has, with 2^N-1, a greatest common divisor of the form $(2^N-1)/(2^t-1)$, t being a divisor of N, corresponds to an operator S which generates with T a subgroup of $LF(2, 2^t)$ and hence a proper subgroup of $LF(2, 2^N)$.

We may therefore eliminate from the set of operators S_α all those whose subscripts satisfy the above requirement. There will then remain, in place of the original 2^N-2, exactly

$$A \equiv 2^N - \sum 2^{N/p_1} + \sum 2^{N/p_1p_2} - \cdots + (-1)^r \sum 2^{N/p_1p_2\cdots p_r},$$

where the p_i are the distinct prime divisors of N and the jth summation is taken with respect to all the possible combinations of these p_i, j at a time. This number A is a simplification of the expression

$$(2^N - 2) - \sum (2^{N/p_1} - 2) + \sum (2^{N/p_1p_2} - 2) - \cdots \\ + (-1)^r \sum (2^{N/p_1p_2\cdots p_r} - 2),$$

and its correctness is established as follows: Let k be of the required form. Then if t involves b distinct primes, S_k will appear $C_{b,j}$ times in the jth summation. The number of times that it will appear in the entire expression is

$$1 - b + C_{b,2} - \cdots + (-1)^b = (1-1)^b \equiv 0.$$

Any subscript not of the form required by the preceding paragraph will appear only once in the first term.

The operators S which now remain will all generate with T the entire group G. But the pairs are not necessarily abstractly distinct, for in reducing their number to A we have taken account of only the inner automorphisms of G. It still remains necessary to consider the possible outer automorphisms. The group of automorphisms of the linear fractional group has been studied by O. Schreier and B. L. van der Waerden.* It follows from their results that the only possible outer automorphisms of $LF(2, 2^N)$ are to be found among the automorphisms of the $GF[2^N]$. From this result, it can be seen that the group of outer automorphisms of $LF(2, 2^N)$ is the cyclic group generated by the substitution $z'=z^2$, of period N.

This substitution is commutative with T and transforms S_l into S_{2l}, provided we consider the subscript $2l$ reduced modulo (2^N-1). As a result, the relations satisfied by T and S_l are abstractly identical with those satisfied by T and S_{2^il}, where i may take on any value

* Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, vol. 6 (1928), pp. 303–322.

whatever. Hence the A operators S may be divided up into sets, in such a way that the subscripts of all the operators in any set are obtainable from some one of them by continued multiplications by two and reduction modulo (2^N-1). The number of operators in any particular set is exactly N, except in those cases when the number 2^N-1 and the subscripts of the set have a greatest common divisor of the form $(2^N-1)/(2^r-1)$. But these have already been eliminated. The number of sets obtained, and therefore the number of distinct definitions of the group, is consequently A/N.

As a corollary, we have the number theoretic result that A/N is always an integer. When N is prime, the corollary reduces to a special case of Fermat's theorem. It was pointed out to me by Professor Gill that the number A/N is identically Dickson's $N_{N,2}$,* or the number of irreducible polynomials of degree N in a $GF[2]$. This coincidence can be used to advantage in the following way:

Consider two distinct irreducible polynomials in the $GF[2]$ of degree N in the variables x and X, respectively. Let S_1 and σ_1 designate the substitutions

$$\left(\frac{0,\ x^2}{1,\ x}\right) \quad \text{and} \quad \left(\frac{0,\ X^2}{1,\ X}\right),$$

respectively, and suppose that the pairs of generators T, S_1 and T, σ_1 are abstractly identical. Then we get an automorphism of G by making T correspond to itself and S_1 correspond to σ_1. As a result, every combination of S_1 and T will have the same period as the corresponding combination of σ_1 and T. Consider in particular all the combinations of the generators which will reduce to the identity. The formal procedure of calculating them is identical for the two separate cases if we hold all processes of modular reduction by means of the polynomial modulus until the very last step. We see then that we can thus obtain a considerable number of pairs of identical expressions in x and X such that both members of each pair will reduce to the same value. But such a result will necessarily imply that the two polynomial moduli are identical, which is a contradiction. Hence a given S_α will yield with T all the possible definitions of $LF(2,\ 2^N)$ if we take advantage of all the distinct methods of generating the $GF[2^N]$.

We shall bring this paper to a close by demonstrating an interesting general property of every pair of generators S and T of an $LF(2,\ 2^N)$.

In the study of groups generated by two operators of periods two

* *Linear Groups*, p. 18.

and three respectively, the following substitution has been found very useful:

$$P = (ST)^{-1}, \qquad S = P^2Q,$$
$$Q = (ST)^2S, \qquad T = P^3Q.$$

It replaces the relations $S^3 = T^2 = (ST)^n = (S^{-1}T^{-1}ST)^p = 1$ by $P^n = Q^p = (QP^3)^2 = (QP^2)^3 = 1$. We shall designate either of these sets of relations by the abbreviated notation $(2, 3, n; p)$.

From the substitution of the equivalents for S and T in the definitions of P and Q, it results that

$$P = \left(\frac{x^\alpha + x^{2\alpha},\ x^{3\alpha}}{x^\alpha,\quad 0}\right) = \left(\frac{1 + x^\alpha,\ x^{2\alpha}}{1,\quad 0}\right),$$
$$Q = \left(\frac{x^{2\alpha} + x^{3\alpha},\qquad x^{3\alpha}}{1,\qquad x^\alpha + x^{2\alpha} + x^{3\alpha}}\right).$$

By induction

$$Q^{2N} = \left(\frac{A_N,\quad x^{3\alpha}}{1,\ x^\alpha + A_N}\right),$$

where $A_N = \sum_{i=0}^{N+1} x^{(2^i+1)\alpha}$. Now the period of Q is the same as that of the commutator of S and T. Since

$$K \equiv TST^{-1}S^{-1} = \left(\frac{1 + x^{2\alpha},\ x^{2\alpha}}{1,\quad x^{2\alpha}}\right)$$

and

$$K^{2N} = \left(\frac{B_N,\quad x^{2\alpha}}{1,\ 1 + B_N}\right),$$

where $B_N = 1 + \sum_{i=1}^{N+1} x^{2^i\alpha}$, it follows that

$$K^{2N+1} = \left(\frac{B_N + x^{2\alpha}B_N + x^{2\alpha},\ x^{2\alpha}B_N + x^{4\alpha}}{x^{2\alpha} + B_N,\qquad x^{2\alpha}B_N}\right)$$

and

$$K^{2N-1} = \left(\frac{x^{2\alpha}(1 + B_N)\ ,\ x^{2\alpha}(1 + x^{2\alpha} + B_N)}{1 + x^{2\alpha} + B_N,\ 1 + B_N(1 + x^{2\alpha})}\right).$$

If the period p of K divides 2^N+1, $B_N = x^{2\alpha}$; if it divides $2^N - 1$, $B_N = 1 + x^{2\alpha}$.

Suppose that p divides 2^N+1. Then, since $B_{N-1}^2 = B_N + x^{2\alpha}$, we have $B_{N-1}=0$, and

$$\begin{aligned}
A_{N-1} &= x^{\alpha}(B_{N-1}+1) + x^{2\alpha} = x^{\alpha} + x^{2\alpha},\\
Q^{2^{N-1}} &= \left(\frac{x^{\alpha}+x^{2\alpha},\ \ x^{3\alpha}}{1,\ \ x^{2\alpha}}\right),\\
Q^{2^{N-1}+1} &= \left(\frac{x^{5\alpha},\ \ x^{6\alpha}}{x^{3\alpha},\ \ x^{4\alpha}+x^{5\alpha}}\right)\left(\frac{x^{2\alpha},\ \ x^{3\alpha}}{1,\ \ x^{\alpha}+x^{2\alpha}}\right),\\
Q^{2^{N-1}+1}P &= \left(\frac{x^{3\alpha},\ \ x^{5\alpha}}{x^{\alpha}+x^{3\alpha},\ \ x^{3\alpha}}\right) = \left(\frac{x^{2\alpha},\ \ x^{4\alpha}}{1+x^{2\alpha},\ \ x^{2\alpha}}\right),\\
(Q^{2^{N-1}+1}P)^2 &= 1,\\
(Q^{(p+1)/2}P)^2 &= 1.
\end{aligned}$$

In the same way, if p divides 2^N-1,

$$Q^{2^{N-1}} = \left(\frac{x^{2\alpha},\ \ x^{3\alpha}}{1,\ \ x^{\alpha}+x^{2\alpha}}\right),$$

and

$$Q^{2^{N-1}}P = \left(\frac{x^{2\alpha},\ \ x^{4\alpha}}{1+x^{2\alpha},\ \ x^{2\alpha}}\right)$$

is of period two. Once again, then, $(Q^{(p+1)/2}P)^2=1$. Hence, regardless of what particular value p may have, the relation $(Q^{(p+1)/2}P)^2=1$ is always satisfied. This result has some interesting consequences.

The relations $(2, 3, n; p)$, $(Q^{(p+1)/2}P)^2=1$ define the group designated by H. S. M. Coxeter* as $G^{3,n,p}$. (In this definition, the relation $Q^p=1$ is redundant† and may be omitted.) Because of the symmetry of $G^{3,n,p}$, it follows that if $n \neq p$, there must exist a pair of generators satisfying $(2, 3, p; n)$, $(Q^{(n+1)/2}P)^2=1$. Hence, if we consider all the abstractly distinct definitions of $LF(2, 2^N)$ in terms of two generators of periods two and three, it follows that the totality of values assumed by n is identical with the totality of values assumed by p.

Moreover, suppose that by the adjunction of suitable conditions we could get a complete definition of $LF(2, 2^N)$ in terms of $(2, 3, n; p)$, $(Q^{(p+1)/2}P)^2=1$; and suppose further that $n \neq p$. Let us introduce the substitution $P^2=\bar{Q}$, $Q=\bar{P}^2$ with the additional requirement that $\bar{P}^p=1$. Then $P=\bar{Q}^{(n+1)/2}$, $\bar{P}=Q^{(p+1)/2}$, and the relations

* *The abstract groups $G^{m,n,p}$*, to appear in the Transactions of this Society.

† *Necessary and sufficient conditions*, p. 69.

$$P^n = Q^p = (QP^3)^2 = (QP^2)^3 = (Q^{(p+1)/2}P)^2 = (Q^{(p+3)/2}P^2)^2 = 1$$

become

$$\bar{Q}^n = \bar{P}^p = (\bar{Q}^{(n+3)/2}\bar{P}^2)^2 = (\bar{Q}\bar{P}^2)^3 = (\bar{Q}^{(n+1)/2}\bar{P})^2 = (\bar{Q}\bar{P}^3)^2 = 1,$$

in which the roles of P and Q have been interchanged. We are thus enabled to pass directly to a second complete definition in terms of $(2, 3, p; n)$, $(Q^{(n+1)/2}P)^2 = 1$.

It is interesting to observe the first few special cases of $LF(2, 2^N)$ to see how the results of this paper apply.

When $N = 2$, the group is the icosahedral group $G^{3,5,5}$ which is completely defined by the relations $(2, 3, 5)$. This is the only definition; hence p must be equal to n, a known result.

When $N = 3$, the group* is the simple group of order 504. It has two definitions, based on $(2, 3, 7; 9)$ and $(2, 3, 9; 7)$. Since $G_{504} \equiv G^{3,7,9}$ it is sufficient in each case to add the one relation $(Q^{(p+1)/2}P)^2 = 1$ in order to obtain a complete definition of the group.

No complete definition in terms of two generators has yet been obtained for any $N > 3$. However, Todd has given a complete definition† of $LF(2, 2^N)$ in terms of $N+2$ generators. Since U and R in his definition satisfy $(2, 3, 2^N - 1)$, it follows from the foregoing that these two operators suffice to generate the entire group, with the single exception of the case $N = 2$, and that one of the values assumed by n is $2^N - 1$.

When $N = 4$, there are three definitions, and the paired values of n and p are 15, 17; 17, 15; 17, 17.

As a last instance we mention $N = 5$. Here the six paired values of n and p are 31, 31; 31, 31; 33, 33; 33, 33; 31, 11; 11, 31. The duplication of the pair 31, 31 means that $LF(2, 2^5)$ has two distinct abstract definitions based on $(2, 3, 31; 31)$. Or, to express it differently, $LF(2, 2^5)$ is obtainable in two abstractly distinct ways as a quotient group of $G^{3,31,31}$. A similar remark holds for the duplication of the pair 33, 33.

Quarry Heights, Canal Zone

* *Necessary and sufficient conditions*, p. 70.

† Journal of the London Mathematical Society, vol. 11 (1936), p. 106.