ON BURNSIDE'S PROBLEM. II

BY

R. C. LYNDON

1. Summary. Let B be the Burnside group on q generators, defined by setting equal to 1 the pth power of every element, where p is a prime. The nth lower central quotient, $Q(n) = B_n/B_{n+1}$, is then a direct product of a certain number $\kappa(n)$ of cyclic groups of order p. We write $\kappa(n) = \psi(n) - \delta(n)$, where $\psi(n) = n^{-1} \sum_{d|n} \mu(n/d) q^d$. In I([1]), the number $\delta(n)$ was determined for $q = 2$ and $n \leq p+2$. Here we consider $n = p+3$ and $n = p+4$. The principal conclusions are([2]):

(A) *if $q = 2$ and $p \geq 5$, then $\delta(p+3) = 6p-4$;*

(B) *if $q = 2$ and $p = 5$, then $\kappa(9)$ is* 4, 2, *or* 0, with substantial evidence for the value $\kappa(9) = 4$.

We summarize the general algorithm set forth in I (referring to that paper for details), and consider certain further consequences. The results (A) and (B) are then presented; their proofs, which involve long computations, are indicated in outline.

2. Basic polynomials. Putting $B = F/R$, where F is free on q generators, we may regard $Q(n)$ as a quotient group of the free abelian group F_n/F_{n+1}, of rank $\psi(n)$, and hence as a quotient space of the vector space $V(n)$ of dimension $\psi(n)$ over the field of integers modulo p. $V(n)$ possesses a basis indexed by S_n, the set of all sequences $c = c_1 c_2 \cdots c_n$ $(c_i = 1, 2, \cdots, q)$ that are *standard* in the sense that c is lexicographically earlier than any $c' = c_k c_{k+1} \cdots c_n c_1$ $\cdots c_{k-1}$ for $k \neq 1$. Relative to this basis, each element r in $R \cap F_n$ corresponds to a vector in $V(n)$ with components $D_c^0(r)$, the corresponding nth order Fox derivatives of r evaluated at $F \to 1$. It follows that $\delta(n)$ is the rank of the matrix $[D_c^0(r)]$ where c ranges over S_n and r over $R \cap F_n$.

If $r = \prod u^p$, and $n < 2p$, then $D_c^0(r) \equiv \sum D_c^0(u^p)$, modulo p. And $D_c^0(u^p)$ $\equiv \sum D_{c^1}^0(u) D_{c^2}^0(u) \cdots D_{c^p}^0(u)$, summed over all factorizations $c = c^1 c^2 \cdots c^p$ of c into p nonempty parts. Let the *type* of a factorization be the unordered set $\tau = \{c^1, c^2, \cdots, c^p\}$ of its factors, and let c have $m(c, \tau)$ factorizations of type τ. By the shuffle relations (I, p. 203), all the $D_c^0(u)$ are expressible as polynomials with rational coefficients (whose denominators will not contain p) in the standard derivatives $u_c = D_c^0(u)$ for c in S_m, $m \leq n$. Consequently each $\prod_{i=1}^{p} D_{c^i}^0(u) \equiv \phi_\tau(u^p)$, a polynomial in the standard u_c. For general ϕ, and

$r = \prod u^p$, define $\phi(r) = \sum \phi(u^p)$. Then $D_c^0(r) \equiv \phi_c(r)$ where

$$\phi_c(u^p) = \sum m(c, \tau)\phi_\tau(u^p).$$

For each n, we shall regard the polynomials ϕ as functions from $R \cap F_n$ into the integers modulo p. For example, that r lie in $R \cap F_p$ implies that $\sum u_1^a u_2^b \equiv 0$ for all $a+b=p$; therefore, for $n \geq p$, we may delete from a polynomial ϕ any term $u_1^a u_2^b$ with $a+b=p$. It follows that $\delta(n)$ is the linear rank of the set of functions ϕ_c, and that r, in $R \cap F_n$, will lie in $R \cap F_{n+1}$ if and only if all $\phi_c(r) \equiv 0$[3]. By a *basic set* we mean any basis for the linear set spanned by the functions ϕ_c. The results of I give, for $q=2$, the following basic sets (where it is convenient to introduce the notation $u_{00} = u_{12} - u_1 u_2/2$):

For $n = 1, 2, \cdots, p$, taken all together, the polynomials

$$u_1^a u_2^b, \qquad a + b = p \quad \text{(and, throughout, } a, b \geq 0\text{)};$$

For $n = p+1$, the polynomials

$$u_1^a u_2^b u_{00}, \qquad a + b + 2 = p + 1;$$

For $n = p+2$, the three types of polynomials

$$u_1^a u_2^b u_{00}^2, \qquad a + b + 2 + 2 = p + 2,$$

$$u_1^a u_2^b (u_{112} - u_1 u_{00}/2 - u_1^2 u_2/6 + u_1 u_2/4),$$

for $a+b+3 = p+2$, and an analogous type for 1 and 2 interchanged.

3. Principal polynomials. For fixed p and n, define a *principal monomial* to be a p-fold product of standard derivatives, of total order n. Thus, for $q=2$ and $n = p+3$, the principal monomials are

$$u_1^a u_2^b u_{1112}, \qquad u_1^a u_2^b u_{1122}, \qquad u_1^a u_2^b u_{1222} \qquad (a + b = p - 1),$$

$$u_1^a u_2^b u_{12} u_{112}, \qquad u_1^a u_2^b u_{12} u_{122} \qquad (a + b = p - 2),$$

$$u_1^a u_2^b u_{12}^3 \qquad (a + b = p - 3).$$

It is easily seen, from the method of obtaining the ϕ_τ by the shuffle relations, that a nonprincipal term in a ϕ_c must either be a p'-fold product for $p' > p$, or else have total order $n' < n$. A set of polynomials is a *principal set* if each polynomial contains a single principal term, and no two the same principal monomial; a principal set is *complete* if each principal term occurs in some (unique) polynomial of the set. Denote by $\pi(n)$ the number of principal monomials of order n.

---

[3] More correctly, if $\phi_c(r) = 0$; however, it was shown in I that to every solution of the $\phi_c(r) \equiv 0$ corresponds a solution of the $\phi_c(r') = 0$ with the property that $\phi(r) \equiv \phi(r')$ for all the polynomials under consideration in this note.

For $n=p+1$, $p+2$, and also for $n=p+3$, with $q=2$, it is found that a basic set exists that is also a complete principal set, whence $\delta(n)=\pi(n)$.

For $n\leqq2p$, the polynomials of a principal set define linearly independent functions. Apart from two cases, it is clear that the conditions r in $R\cap F_n$, expressed by polynomials of lower order, play no essential role, and the principal monomials of order n are independent. For $n=2p-1$, in the case of the monomial $\phi=u_1u_{00}^{p-1}$, it must be verified that the values of $\phi(r)=\sum u_1u_{00}^{p-1}$ are not restricted by the conditions, on r in $R\cap F_{2p-1}$, that $\sum u_1^a u_2^b u_{00}^c\equiv0$ for all $a+b+c=p$ and $0\leqq c<p-1$. Similarly, for $n=2p$, it must be noted that $\sum u_{00}^p\equiv\sum u_{00}$ is not restricted by the same conditions, now for $0\leqq c<p$.

The conjecture that, for $p<n<2p$, a basic set can always be chosen to be a complete principal set turns out to fail for $p=5$, $q=2$, $n=9$. One may still conjecture[4] that a basic set can always be chosen principal, though possibly incomplete. Let $\delta'(n)$ be the rank of a maximal principal set in the space of the ϕ_c; at least, $\delta'(n)\leqq\pi(n)$, and the conjecture is that $\delta(n)=\delta'(n)$.

As in I, decompose $V(n)$ into its homogeneous subspaces $V(h,k)$ of degree h in x_1 and $k=n-h$ in x_2; let $\psi(h,k)$ be the dimension of $V(h,k)$. If $\pi(h,k)$ is the number of principal monomials of order h with respect to x_1, and k to x_2, it follows from the independence of the principal monomials, for $n<2p$, that $\pi(n)=\sum\pi(h,k)$, and, analogously, that $\delta'(n)=\sum\delta'(h,k)$. From this follows, at least for $q=2$ and $n\leqq p+3$, the direct decomposition $Q(n)=\sum Q(h,k)$.

By an estimate of $\pi(n)$ we obtain a bound on $\delta'(n)$. For $n=p+d$, and $h,k,\cdots\geqq d$, one sees that $\pi(h,k,\cdots)=\alpha(d)$, where $\alpha(d)$ depends only on d (and q, supposed fixed), and has the generating function

$$\sum\alpha(d)x^d = \prod_{s=1}^{\infty}(1-x^s)^{-\psi(s+1)}.$$

For $q=2$, this gives $1+x+3x^2+6x^3+15x^4+30x^5+65x^6+\cdots$, and one may deduce, for example, that if $p=7$, then

$$\delta'(13) \leqq \pi(13) < 14+8\cdot65 < 630 = \psi(13).$$

In general, for $q=2$, $(p-d+1)\cdot\alpha(d)<\pi(n)<(p+d)\cdot\alpha(d)$, and the results

$$\delta(p) = p-1, \quad \delta(p+1) = p, \quad \delta(p+2) = 3p-1, \quad \delta(p+3) = 6p-4$$

suggest a formula $\delta(p+d)=\alpha(d)\cdot p+\beta(d)$, for $d<p$, where β is nonpositive and depends only on d.

4. **The case $n=p+3$, $q=2$, $p\geqq5$.** We outline the method of the computation, which ran to great length. First, by the shuffle relations the ϕ_r are computed, treating h and k as parameters. Next, the $m(c,\tau)$ are to be determined. Observe that the $m(c,\tau)$ depend only upon the frequencies $(fghi)$, $\cdots$ of

---

[4] By Meier-Wunderli's result, cited in Footnote 1, this conjecture is confirmed in the further case $p=5$, $q=2$, $n=9$.

occurrence of the various kinds of blocks of length 4 (or less) in $c(^5)$; this observation requires consideration of the circumstances of possible overlap of the blocks from which one seeks to form a factorization of type τ. Writing c in the form $c = 0c_1c_2 \cdots c_{p+3}0$, in order to keep track of the "ends," these frequencies can be determined from the set of 14 frequencies $h = (1)$, (12), (112), (122), (1112), (1122), (1212), (1222), (120), (1120), (1220), (012), (0112), (0122). Expressing the $m(c, \tau)$ in terms of these, the general ϕ_c is given by a polynomial $\phi = \sum m(c, \tau)\phi_\tau$ with coefficients depending, a priori, in nonlinear fashion upon the 14 parameters $h, \cdots,$ (01222). In fact, the polynomial ϕ, as a function over $R \cap F_{p+3}$, proves to depend linearly (but non-homogeneously) only upon the six parameters h, $(12) - (112) - (122)$, $(1122) - - (1212)$, (120), (1120), (1220). For fixed h, this gives (in view of the non-homogeneity) at most a six-parameter family of polynomials ϕ; and this family is spanned by a complete principal set.

It remains to check that standard c exist with sufficient variety of the six parameters to span the full family. For $h, k \geq 3$, where $\pi(h, k) = 6$, one easily finds six c with values of these parameters leading to independent ϕ_c. Similarly one finds that $\delta(1, p+2) = \pi(1, p+2) = 1$, $\delta(2, p+1) = \pi(2, p+1) = 3$, and symmetrically in h and k. It results that

$$\delta(p + 3) = 1 + 3 + 6(p - 2) + 3 + 1 = 6p - 4.$$

5. **The case $p = 5$, $q = 2$, $n = 9$.** From the results $\kappa(1, 7) = \kappa(2, 6) = 0$ for $n = 8$, it follows that, for $n = 9$, $\kappa(1, 8) = \kappa(2, 7) = 0$. In view of the symmetry between h and k, only $\delta'(3, 6)$ and $\delta'(4, 5)$ remain to be calculated. For the $\psi(3, 6) = 9$ standard c containing 3 symbols 1 and 6 symbols 2, the $m(c, \tau)$ may be obtained by inspection. Actually, only those τ need be considered that correspond to the ten principal monomials of order 3 in x_1 and 6 in x_2. Moreover, only the coefficient of the principal term of the corresponding ϕ_τ need be determined: for this one may use the shuffle relations, $u_a u_b = \sum u_c$ (summed over all shuffles of a and b), in the reduced form obtained by deleting the left member and any terms on the right arising from improper shuffles. This yields a 9×10 matrix of integers modulo 5, which proves to have rank $\delta'(3, 6) = 9$. An analogously obtained 14×15 matrix yields $\delta'(4, 5) = 12$, whence $\kappa(4, 5)$ is 12, 13, or 14. It follows that $\delta'(9) = 1 + 4 + 9 + 12 + 12 + 9 + 4 + 1 = 52$, that $\delta(9)$ is 52, 54, or 56, and that $\kappa(9)$ is 4, 2, or 0.

UNIVERSITY OF MICHIGAN,
    ANN ARBOR, MICH.

(^{5}) The present observation may be used to greatly shorten one half of the proof of the theorem of J. A. Green, J. London Math. Soc. vol. 27 (1952) p. 476. The remaining part of his proof may be simplified by the observation that, for w in F_n, $c = c_1c_2 \cdots c_n$, and $d = c_nc_{n-1} \cdots c_1$, then $D_e^0(w) = (-1)^{n-1}D_d^0(w)$; proof by induction, using (5.2) of Fox, Ann. of Math. vol. 57 (1953) p. 559.