TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 189, 1974

COUNTING COMMUTATORS(1)

BY
R. J. MIECH

ABSTRACT. Let G be a group generated by x and y, G_2 be the commutator subgroup of G, and G_1 be the group generated by y and G_2. This paper contains explicit expansions of y^{x^m} modulo $[G_2, G_2, G_2]$ and $(xy)^m$ modulo $[G_1, G_1, G_1]$. The motivation for these results stem from the p-groups of maximal class, for a large number of these groups have $[G_1, G_1, G_1] = 1$.

Let G be a group generated by x and y. There are various theorems on the expansion of $(xy)^m$ modulo the commutator of G ([1, p. 50], [2], [3, p. 315]). These results are of a general nature and are not too useful when dealing with the construction of groups whose structure is nontrivial but not too complicated.

The purpose of this paper is to point out that there is a sequence arising from the conjugation process having properties which enable one to prove some results on the expansion y^{x^m} and $(xy)^m$. To be specific let $[a, b]$ be the commutator of a and b, $[a, b] = a^{-1}b^{-1}ab$, $\sigma(0) = y$ and $\sigma(i + 1) = [\sigma(i), x]$ for $i \geq 0$. We have

$$y^{x^0} = y = \sigma(0), \qquad y^x = y[y, x] = \sigma(0)\sigma(1),$$

$$y^{x^2} = \sigma(0)^x\sigma(1)^x = \sigma(0)\sigma(1)\sigma(1)\sigma(2).$$

In general, since $\sigma(i)^x = \sigma(i)\sigma(i + 1)$,

$$y^{x^m} = \sigma[i(m, 1)]\sigma[i(m, 2)] \ldots \sigma[i(m, 2^m)]$$

where $i(m, n)$ is defined by

$$i(0, 1) = 0, \qquad i(m, n) = i(m - 1, [(n + 1)/2]) + (1 + (-1)^n)/2$$

for $m \geq 1$, $n = 1, 2, \ldots, 2^m$.

Some of the properties of this sequence are given by

Theorem 1. *Let* $i(0, 1) = 0$ *and* $i(m, n) = i(m - 1, [(n + 1)/2]) + (1 + (-1)^n)/2$ *for* $m \geq 1$ *and* $n = 1, \ldots, 2^m$. *Suppose that* $n = 2^{q(1)} + 2^{q(2)} + \ldots + 2^{q(t)}$ *where* $0 \leq q(1) < q(2) < \ldots < q(t)$. *Then*

(a) $i(m, n) = q(1) + t - 1$.

(b) *If* m *and* k *are fixed then the solutions of the equation* $i(m, n) = k$ *are* $n = 2^k$

Received by editors July 22, 1971.
AMS (MOS) subject classifications (1970). Primary 20D15; Secondary 20-XX.
Key words and phrases. Commutators.
(1) The preparation of this paper was supported in part by NSF Grants GP-13164 and GP-28698.

and $n = 2^{k-r} + 2^{q(2)} + \ldots + 2^{q(r)} + 2^{j-1}$ *where* $j = k+1, \ldots, m$; $r = 1, \ldots, k$; *and* $k - r = q(1) < q(2) < \ldots < q(r) < j - 1$.

(c) *If* m,k, *and* j *are fixed then the number of integers* n *such that* $2^{j-1} < n \leq 2^j$, $i(m,n) = k$, *is equal to* $\binom{j-1}{k-1}$.

To continue let us fix m, write $i(m,n) = i(n)$ and return to

$$y^{x^m} = y\sigma(i(2)) \cdots \sigma(i(n)) \cdots \sigma(i(2^m)).$$

Let $d_1(n)$ be the number of $\sigma(1)$ lying to the right of $\sigma(i(n))$ in this expansion. That is

$$d_1(n) = |\{\nu : n < \nu \leq 2^m, i(\nu) = 1\}|.$$

Then collecting the $\sigma(1)$ to the left one finds that

$$y^{x^m} = y\sigma(1)^{\binom{m}{1}} \prod_{n \leq 2^m; i(n) \geq 2} \sigma(i(n))[\sigma(i(n)), \sigma(1)^{d_1(n)}].$$

Part (c) of Theorem 1 is used here; the number of $\sigma(1)$ in the expansion is $\binom{m}{1}$. Further "collection" considerations lead to the quantities of

Theorem 2. *Let* ℓ, n, *and* j *be fixed integers with* $2^{j-1} < n \leq 2^j$ *and* $1 \leq \ell \leq i(n)$. *Set* $d_\ell(n) = |\{\nu : n < \nu \leq 2^m, i(\nu) = \ell\}|$ *and* $m_\ell(n) = |\{\nu : 2^{j-1} < \nu < n, i(\nu) = \ell\}|$. *Then*:

(a) $d_\ell(n) = \binom{m}{\ell} - \binom{j}{\ell} + \binom{j-1}{\ell-1} - m_\ell(n)$.

(b) *For* $n = 2^j$, $m_\ell(2^j) = \binom{j-1}{\ell-1}$.

For $2^{j-1} < n < 2^j$, *that is*, $n = 2^{q(1)} + \ldots + 2^{q(n)} + 2^{j-1}$,

$$m_\ell(n) = \sum_{t=0}^{r-1} \binom{q(r-t)}{\ell - 1 - t}.$$

(c)

$$\sum_{2^{j-1} < n \leq 2^j; i(n) = k} m_\ell(n) = \sum_{a=1}^{\ell} \sum_{x=k-a-1}^{j-a-1} \binom{j-2-x}{a-1} \binom{x}{k-a-1} \binom{x}{\ell - a}.$$

Incidentally the condition $1 \leq \ell < i(n)$ of Theorem 2 arises from the commutator collecting process. If we have a product of commutators $\ldots \sigma[i(n)] \ldots \sigma(\ell) \ldots$ only those $\sigma(\ell)$ with $\ell < i(n)$ are collected to the left of $\sigma[i(n)]$. The inequality $\ell < i(n)$ shall be used several times in the proof of Theorem 2.

As an application of Theorems 1 and 2 we shall prove two results which are needed to construct some p-groups of maximal class [4]. These are

Theorem 3. *Let* G *be a group generated by* x *and* y, G_2 *be the commutator subgroup of* G, *and* $K_2 = [G_2, G_2, G_2]$. *Let* $\sigma(0) = y$ *and* $\sigma(i+1) = [\sigma(i), x]$ *for* $i \geq 0$. *Set*

$$a(k,\ell,t) = \binom{\ell}{t}\binom{k+t}{\ell} - \binom{k+2t-\ell-1}{t-1}\binom{k+t}{k+2t-\ell},$$

$$A(m,k,\ell) = \binom{m}{k}\binom{m}{\ell} - \sum_{t=0}^{\ell} a(k,\ell,t)\binom{m}{k+t},$$

$$P(m) = \prod_{k=2}^{m-1}\prod_{\ell=1}^{k-1}[\sigma(k),\sigma(\ell)]^{A(m,k,\ell)}.$$

Then for any nonnegative integer m

$$y^{x^m} \equiv y\sigma(1)^{\binom{m}{1}}\ldots\sigma(m)^{\binom{m}{m}}P(m) \bmod K_2.$$

Theorem 4. *Let G, G_2, $\sigma(i)$, and $a(k,\ell,t)$ be defined as in Theorem 3. Let G_1 be the group generated by y and G_2 and $K_1 = [G_1, G_1, G_1]$. Set*

$$b(k,\ell,t) = \binom{\ell+1}{t}\binom{k+t}{\ell+1} + \binom{k+2t-\ell-1}{t-1}\binom{k+t}{k+2t-\ell},$$

$$B(p,k,\ell) = \sum_{t=0}^{\ell+1} b(k,\ell,t)\binom{p}{k+1+t},$$

$$Q(p) = \prod_{k=1}^{p-1}\prod_{\ell=0}^{k-1}[\sigma(k),\sigma(\ell)]^{B(p,k,\ell)}.$$

Then for any nonnegative integer p

$$(xy)^p \equiv x^p y^p \sigma(1)^{\binom{p}{2}}\ldots\sigma(p-1)^{\binom{p}{p}}Q(p) \bmod K_1.$$

Proof of Theorem 1. Part (a) of Theorem 1 can be proved by induction on m. The argument depends on the parity of n. If n is even then $q(1) \geq 1$ and we have:

$$[(n+1)/2] = 2^{q(1)-1} + \ldots + 2^{q(t)-1}, \qquad (1+(-1)^n)/2 = 1.$$

Thus, by the induction hypothesis,

$$i(m,n) = i\left(m-1, \left[\frac{n+1}{2}\right]\right) + \frac{1+(-1)^n}{2} = (q(1)-1) + (t-1) + 1$$

$$= q(1) + t - 1.$$

If n is odd then $q(1) = 0$ and we have $[(n+1)/2] = 1 + 2^{q(2)-1} + \ldots + 2^{q(t)-1}$, $(1+(-1)^n)/2 = 0$. If $q(2) \geq 2$ then

$$i(m,n) = i\left(m-1, \left[\frac{n+1}{2}\right]\right) = 0 + t - 1 = q(1) + t - 1.$$

If $q(2) = 1$ and there is an integer $i \leq t-1$ such that $q(2) = 1, q(3) = 2, \cdots, q(i) = i-1$ and $q(i+1) > i$, then $[(n+1)/2] = 2^{i-1} + 2^{q(i+1)-1} + \ldots + 2^{q(t)-1}$ and

$$i(m,n) = i\left(m-1,\left[\frac{n+1}{2}\right]\right) = (i-1)+(t-i+1-1) = t-1$$

$$= q(1)+t-1.$$

Finally if $q(j) = j-1$ for $j = 2,\ldots,t$ then $[(n+1)/2] = 2^{t-1}$ and

$$i(m,n) = i\left(m-1,\left[\frac{n+1}{2}\right]\right) = (t-1)+1-1 = q(1)+t-1.$$

This completes the proof of part (a) of Theorem 1.

Part (b) of Theorem 1 follows directly from part (a).

To prove (c) fix r in (b). Then the number of integers n such that $n = 2^{k-r}+2^{q(2)}+\ldots+2^{q(r)}+2^{j-1}$ and $k-r+1 \le q(2) < \cdots < q(r) \le j-2$ is equal to

$$\binom{j-2-k+r}{r-1}.$$

Summing on r we get

$$\sum_{r=1}^{k}\binom{j-2-k+r}{r-1} = \binom{j-1}{k-1},$$

which proves (c).

Proof of Theorem 2(a). Part (a) of Theorem 2 is a consequence of (c) of Theorem 1. The number of ν such that $2^j < \nu \le 2^m$, $i(\nu) = l$, is equal to

$$\sum_{u=j+1}^{m}\binom{u-1}{l-1} = \binom{m}{l}-\binom{j}{l}.$$

The number of ν such that $n < \nu \le 2^j$ is equal to $\binom{j-1}{l-1} - m_l(n)$. Thus

$$d_l(n) = \binom{m}{l}-\binom{j}{l}+\binom{j-1}{l-1}-m_l(n).$$

Proof of Theorem 2(b). The first part of (b) is obvious; the second is not. Suppose that $2^{j-1} < n < 2^j$ so that $n = 2^{q(1)}+\ldots+2^{q(r)}+2^{j-1}$. We need to count the number of ν such that $2^{j-1} < \nu < n$ and $i(\nu) = l$. To this end we shall first describe the ν that are less than n. After this has been done the count will follow.

To begin, since $2^{j-1} < \nu < 2^j$ we have

$$\nu = 2^{k(1)}+\ldots+2^{k(t)}+2^{j-1} \tag{1}$$

where $t \ge 1$. Next, in view of the inequality

$$\nu = 2^{k(1)}+\ldots+2^{k(t)}+2^{j-1} < 2^{q(1)}+\ldots+2^{q(r)}+2^{j-1} = n, \tag{2}$$

let

$$D(0) = \{(h(1), \ldots, h(t)) : t \geq 1, 0 \leq h(1) < \cdots < h(t) < q(r)\}$$

and for $u = 1, 2, \ldots, r-1$

$$D(u) = \{(h(1), \ldots, h(t)) | t \geq u, 0 \leq h(1) < \cdots < h(t-u) < q(r-u), \\ h(t-u+1) = q(r-u+1), \ldots, h(t) = q(r)\}.$$

Then the v of the form (1) which satisfy (2) are those v where $(h(1), \ldots, h(t))$ is in $D(0), D(1), \ldots,$ or $D(r-1)$. This is easy to see for if (2) holds then, since $2^{q(1)} + \ldots + 2^{q(r)} \leq 2^{q(r)} - 1$, we must have $h(t) \leq q(r)$. The v where $h(t) < q(r)$ are those whose exponents come from $D(0)$; the v where $h(t) = q(r)$ and $h(t-1) < q(r-1)$ are those whose exponents come from $D(1)$, etc.

Consider next the quantity t appearing in the definition of the $D(u)$. In $D(0)$ we have $0 \leq h(1) < \ldots < h(t) < q(r)$. Thus $t - 1 \leq h(t) < q(r)$ or $t \leq q(r)$. Similarly in $D(u)$, $u \geq 1$, we have $t \leq q(r-u) + u$. So for $u = 0, 1, \ldots, r-1$ let

$$D_t(u) = \{(h(1), \ldots, h(t)) | 0 \leq h(1) < \ldots < h(t-u) < q(r-u), \\ h(t-u+1) = q(r-u+1), \ldots, h(t) = g(r)\}$$

with the conventions that if $u = 0$ the second set of conditions, the equalities, is to be dropped while if $u \geq 1$ and $t = u$ the first set of conditions is to be ignored. We then have

$$D(0) = \bigcup_{t=1}^{q(r)} D_t(0), \qquad D(u) = \bigcup_{t=u}^{q(r-u)+u} D_t(u).$$

Finally recall that we are assuming that $\ell < i(n)$. Since $n = 2^{q(1)} + \ldots + 2^{q(r)} + 2^{j-1}$ we have $\ell < i(n) = q(1) + k$ which implies that $q(i) > \ell - r + i - 1$, i.e.

$$q(r-u) > \ell - u - 1. \tag{3}$$

We shall now count the v with $i(v) = \ell$ stemming from a fixed $D_t(u)$. Suppose first that $u = 0$. Then:

$$v = 2^{h(1)} + \ldots + 2^{h(t)} + 2^{j-1}, \qquad 0 \leq h(1) < h(2) < \ldots < h(t) < q(r),$$

$$i(v) = h(1) + t = \ell.$$

The last relation yields $h(1) = \ell - t \geq 0$. Since the number of integral $(x_1, \ldots, x_n)$ with $a \leq x_1 < \ldots < x_n < b$ is equal to $\binom{b-a}{n}$ the number of $(h(2), \ldots, h(t))$ such that $h(1) + 1 = \ell - t + 1 \leq h(a) < \ldots < h(t) < q(r)$ is equal to $\binom{q(r)-\ell-1+t}{t-1}$. We want next to sum on t. We have $t \leq q(r)$ from the definition of

$D(0)$. We also have $h(1) = l - t \geq 0$ so $t \leq l$ and $t \leq q(r)$. By (3), $l - 1 < q(r)$ or $l \leq q(r)$. Thus the summation is from $t = 1$ to $t = l$. Summing we have

$$\sum_{t=1}^{l} \binom{q(r) - l - 1 + t}{q(r) - l} = \binom{q(r)}{l-1},$$

and this is the number of $\nu < n$ with $i(\nu) = l$ coming from $D(0)$.

Suppose next that $u \geq 1$. The case $t = u$ is slightly different from the rest so we shall treat it separately. If $t = u$ the set of inequalities appearing in the definition of $D_u(u)$ is vacuous so there is but one ν from $D_u(u)$,

$$\nu = 2^{h(1)} + \ldots + 2^{h(u)} + 2^{j-1},$$

where $h(1) = q(r - u + 1), \ldots, h(u) = q(r)$. We would also have

$$i(\nu) = h(1) + u = q(r - u + 1) + u = l.$$

But, by (3), $q(r - u + 1) > l - u$. Thus there are no ν with $i(\nu) = l$ stemming from $D_u(u)$.

The argument on the sets $D_t(u)$, $u \geq 1$, $t \geq u + 1$, is similar to the $D_t(0)$ case. One finds that the number of ν with $i(\nu) = l$ coming from $D(u)$ is equal to $\binom{q(r-u)}{l-1-u}$. We then have

$$m_l(n) = \sum_{t=0}^{r-1} \binom{q(r-t)}{l-1-t},$$

which completes the proof of Theorem 2(b).

Proof of Theorem 2(c). We have upon replacing $t + 1$ by a in the sum for $m_l(n)$,

$$(4) \qquad \sum_{2^{j-1} < n \leq 2^j; i(n) = k} m_l(n) = \sum_{2^{j-1} < n \leq 2^j; i(n) = k} \sum_{a=1}^{r} \binom{q(r-a+1)}{l-a}$$

where for $j \geq k + 1$ the n in the index of summation are those of the form $n = 2^{k-r} + 2^{q(2)} + \ldots + 2^{q(r)} + 2^{j-1}$ with $r = 1, 2, \ldots, k$ and $k - r = q(1) < q(2) < \ldots < q(r) \leq j - 2$. (We shall suppose $j \geq k + 1$ in what follows for the case $j = k$ of Theorem 2(c) is fairly trivial.)

Let S_1 be that part of the right-hand side of (4) where $a = r$. Then $q(r - a + 1) = q(1) = k - r$ and

$$S_1 = \sum_{2^{j-1} < n \leq 2^j; i(n) = k} \binom{k-r}{l-r} = \sum_{r=1}^{k} \binom{k-r}{l-r} \psi(r)$$

where $\psi(r)$, being the number of $(q(1), \ldots, q(r))$ with $k - r = q(1) < q(2) < \ldots < q(r) \leq j - 2$, is equal to $\binom{j-k-2+r}{r-1}$. Thus

$$S_1 = \sum_{r=1}^{k} \binom{k-r}{l-r}\binom{j-k-2+r}{r-1} = \binom{j-1}{l-1}.$$

The last equation follows from the identity

$$\sum_{j=0}^{n} \binom{N+j}{N}\binom{M+n-j}{M} = \binom{M+N+1+n}{M+N+1},$$

which can be proved by equating coefficients in the two expansions of $(1+y)^{-M}(1+y)^{-N}$.

To continue let S_2 denote the remaining terms of the right-hand side of (4). That is,

$$S_2 = \sum_{2^{j-1}<n\leq 2^j; i(n)=k} \sum_{a=1}^{r-1} \binom{q(r-a+1)}{l-a}.$$

Now fix a, fix r, fix $q(r-a+1)$ and set $x = q(r-a+1)$. Then the number of n with $n = 2^{k-r} + 2^{q(1)} + \ldots + 2^{q(r)} + 2^{j-1}$ and

$$\begin{aligned} k-r = q(1) < q(2) < \ldots < q(r-a) < q(r-a+1) \\ = x < q(r-a+2) < \ldots < q(r) \leq j-2 \end{aligned}$$

contributing a $\binom{q(r-a+1)}{l-a}$ to S_2 is equal to

$$\binom{x-1-k+r}{r-a-1}\binom{j-2-x}{a-1}.$$

Keeping a and x fixed and summing on r we get the quantity

$$\sum_{r=a+1}^{k} \binom{x-1-k+r}{r-a-1}\binom{j-2-x}{a-1} = \binom{x}{k-a-1}\binom{j-2-x}{a-1}.$$

Thus

$$S_2 = \sum_{a=1}^{l} \sum_{x} \binom{x}{k-a-1}\binom{j-2-x}{a-1}\binom{x}{l-a}$$

where the range of x is to be determined.

To determine this range note that since $q(1) < q(2) < \ldots < q(r)$ we have $q(v) \geq q(1) + v - 1$ and $q(r) \geq q(r-v) + v$. That is

$$q(r-a+1) \geq q(1) + r - a = k - r + r - a = k - a$$

and

$$q(r-a+1) \leq q(r) - a + 1 \leq j - 2 - a + 1 = j - a - 1.$$

Consequently $k - a \leq q(r - a + 1) = x \leq j - a - 1$ and

$$S_2 = \sum_{a=1}^{l} \sum_{x=k-a}^{j-a-1} \binom{x}{k-a-1}\binom{j-2-x}{a-1}\binom{x}{l-a}.$$

Note finally that if we extend the range of summation above by letting $x = k - a - 1$ the terms thus added are equal to

$$\sum_{a=1}^{l} \binom{j-1-k+a}{a-1}\binom{k-a-1}{l-a} = \binom{j-1}{l-1} = S_1.$$

Bringing these results together we have

$$\sum_{2^{j-1}<n\leq 2^j;i(n)=k} m_l(n) = S_1 + S_2$$
$$= \sum_{a=1}^{l} \sum_{x=k-a-1}^{j-a-1} \binom{j-2-x}{a-1}\binom{x}{k-a-1}\binom{x}{l-a}.$$

This completes the proof of part (c) of Theorem 2.

Lemma 1. *Let* $A(m,k,l) = \sum_{2\leq n\leq 2^m;i(n)=k} d_l(n)$. *Then*

$$A(m,k,l) = \binom{m}{k}\binom{m}{l} - D_1 - D_2$$

where

$$D_1 = \sum_{j=k}^{m} \binom{j-1}{k-1}\binom{j-1}{l},$$

$$D_2 = \sum_{a=1}^{l} \sum_{x=k-a-1}^{m-1-a} \binom{x}{k-a-1}\binom{x}{l-a}\binom{m-1-x}{a}.$$

Proof. First of all,

$$A(m,k,l) = \sum_{j=k}^{m} \sum_{2^{j-1}<n\leq 2^j;i(n)=k} d_l(n).$$

Secondly, $d_l(n) = \binom{m}{l} - \binom{j-1}{l} - m_l(n)$. Finally, the number of n such that $i(n) = k$, $2^{j-1} < n \leq 2^j$ is equal to $\binom{j-1}{k-1}$. If we put these results together we get Lemma 1.

Lemma 2. *If* $x \geq b \geq a$ *then*

$$\binom{j}{a}\binom{j}{b} = \sum_{u=0}^{a} \binom{a}{u}\binom{a+b-u}{a}\binom{j}{a+b-u}$$

and

$$\sum_{j=k}^{m} \binom{j}{a}\binom{j}{b} = \sum_{u=0}^{a} \binom{a}{u}\binom{a+b-u}{a}\binom{m+1}{a+b+1-u}.$$

To prove the first equation multiply $\binom{j}{b} = \sum_{u=0}^{a} \binom{a}{u}\binom{j-a}{b-u}$ by $\binom{j}{a}$ and rearrange in the obvious way. The second equation is a consequence of the first.

We are now in a position to prove Theorem 3. The first step in the proof is

Lemma 3. *Let $A(m,k,l)$ be defined as in Lemma 1. Then*

$$A(m,k,l) = \binom{m}{k}\binom{m}{l} - \sum_{t=0}^{l} a(k,l,t)\binom{m}{k+t}$$

where $a(k,l,t) = \sum_{\nu=0}^{l-t} \binom{l-\nu}{t}\binom{k-1+t-\nu}{l-\nu}$.

Proof. By Lemma 2,

$$D_1 = \sum_{j=k-1}^{m-1} \binom{j}{k-1}\binom{j}{l} = \sum_{u=0}^{l} \binom{l}{u}\binom{l+k-1-u}{l}\binom{m}{l+k-u}.$$

Similarly

$$D_2 = \sum_{a=1}^{l} \sum_{x=k-a-1}^{m-1-a} \sum_{u=0}^{l-a} \binom{l-a}{u}\binom{k-a-1+l-a-u}{l-a} \cdot \binom{x}{k-a-1+l-a-\nu}\binom{m-1-x}{a}$$

$$= \sum_{a=1}^{l} \sum_{u=0}^{l-a} \binom{l-a}{u}\binom{k-a-1+l-a-u}{l-a}\binom{m}{k+l-a-u}.$$

Next, note that if we extend the range of summation in D_2 to $a = 0$ and call the resulting sum D_2' then $D_2' = D_2 + D_1$. Furthermore if we rearrange D_2' by bringing together those terms where $l - a - u = t$ then

$$D_2' = \sum_{t=0}^{l} \left[\sum_{a,u;\, l-a-u=t} \binom{l-a}{t}\binom{k+t-1-a}{l-a}\right]\binom{m}{k+t}$$

$$= \sum_{t=0}^{l} a(k,l,t)\binom{m}{k+t}.$$

Since $A(m,k,l) = \binom{m}{k}\binom{m}{l} - D_2'$ this completes the proof of Lemma 3.

Lemma 4. *Let $a(k,l,t)$ be defined as in Lemma 3. Then*

$$a(k,l,t) = \binom{l}{t}\binom{k+t}{l} - \binom{k+2t-l-1}{t-1}\binom{k+t}{k+2t-l}.$$

Proof. Consider the quantity

$$S = \binom{l}{l-t}\binom{k+t}{l} - a(k,l,t)$$

$$= \binom{l}{l-t}\binom{k+t}{l} - \sum_{\nu=0}^{l-t} \binom{l-\nu}{l-\nu-t}\binom{k-1+t-\nu}{l-\nu}.$$

Note that

$$S = \binom{l}{l-t}\left[\binom{k+t}{l} - \binom{k+t-1}{l}\right] - \sum_{\nu=1}^{l-t}\binom{l-\nu}{l-\nu-t}\binom{k-1+t-\nu}{l-\nu}$$

$$= \binom{l-1}{l-t}\binom{k+t-1}{l-1} + \binom{l-1}{l-t-1}\binom{k+t-1}{l-1}$$

$$- \sum_{\nu=1}^{l-t}\binom{l-\nu}{l-\nu-t}\binom{k-1+t-\nu}{l-\nu}.$$

Thus, by induction,

$$S = \sum_{\omega=1}^{j}\binom{l-\omega}{l-t-\omega+1}\binom{k+t-\omega}{l-\omega} + \binom{l-j}{l-t-j}\binom{k+t-j}{l-j}$$

$$- \sum_{\nu=j}^{l-t}\binom{l-\nu}{l-t-\nu}\binom{k-1+t-\nu}{l-\nu}.$$

Consequently

$$S = \sum_{\omega=1}^{l-t+1}\binom{l-\omega}{l-t+1-\omega}\binom{k+t-\omega}{l-\omega}$$

$$= \binom{k+2t-l-1}{t-1}\sum_{\omega=1}^{l-t+1}\binom{k+t-\omega}{k+2t-l-1}$$

$$= \binom{k+2t-l-1}{t-1}\binom{k+t}{k+2t-l}.$$

Lemma 4 follows from this equation.

To prove Theorem 3, let us return to the discussion following Theorem 1 where we had

$$y^{x^m} = y\sigma(1)^{(\overset{m}{1})} \prod_{n\le 2^m;\, i(n)\ge 2} \sigma(1(n))[\sigma(i(n)), \sigma(1)^{d_1(n)}].$$

Since $\sigma(1), \sigma(2), \ldots$ are in G_2 we have

$$[\sigma(i(n)), \sigma(1)^{d_1(n)}] \equiv [\sigma(i(n)), \sigma(1)]^{d_1(n)} \bmod K_2$$

where $K_2 = [G_2, G_2, G_2]$. In addition, for $a, b \ge 1$, $\sigma(a)$ and $[\sigma(b), \sigma(1)]$ commute modulo K_2. Thus we have

$$y^{x^m} \equiv y\sigma(1)^{(\overset{m}{1})} P_1 P_1' \bmod K_2$$

where $P_1 = \prod_{n\le 2^m;\, i(n)\ge 2} \sigma(i(n))$, $P_1' = \prod_{k=2}^{m-1} [\sigma(k), \sigma(1)]^{A(m,k,1)}$, $A(m,k,1) = \sum_{n\le 2^m;\, i(n)=k} d_1(n)$. Inductively one gets

$$y^{x^m} \equiv y\sigma(1)^{(\overset{m}{1})} \ldots \sigma(m)^{(\overset{m}{m})} P(m) \bmod K_2$$

where

$$P(m) = \prod_{l=1}^{m-2} \prod_{k=l+1}^{m-1} [\sigma(k), \sigma(l)]^{A(m,k,l)}, \qquad A(m,k,l) = \sum_{n \le 2^m; i(n)=k} d_l(n),$$

$$d_l(n) = |\{\nu : n < \nu \le 2^m, i(\nu) = l\}|.$$

Theorem 3 now follows from Lemmas 1, 3, and 4.

Theorem 4 is a consequence of Theorem 3. To start the proof of Theorem 4 we have

Lemma 5. *Let* $R(m) = \sigma(1)^{\binom{m}{1}} \dots \sigma(m)^{\binom{m}{m}}$, $S(p) = \prod_{l=1}^{p-3} P(p-l)$,

$$T(j) = \prod_{l=1}^{p-1} \prod_{\nu=j+1}^{p-l} [\sigma(\nu), \sigma(j)]^{\binom{p-l}{\nu-j}\binom{p-l}{j+1}}.$$

Then

$$(xy)^p \equiv x^p y^p \sigma(1)^{\binom{p}{2}} \dots \sigma(p-1)^{\binom{p}{p}} S(p) T(0) \dots T(p-2) \bmod K_1.$$

Proof. By Theorem 3 and the fact that, for any $i, j, k \ge 0$, $\sigma(i)$ and $[\sigma(j), \sigma(k)]$ commute modulo K_1 we have

$$\begin{aligned}(xy)^p &= x^p \prod_{l=1}^{p} y^{x^{p-l}} \equiv x^p \prod_{l=1}^{p} y R(p-l) P(p-l) \bmod K_2 \\ &\equiv x^p y^p \left[\prod_{l=1}^{p-1} R(p-l)^{y^{p-l}}\right] S(p) \bmod K_1.\end{aligned}$$

Now

$$\begin{aligned}\prod_{l=1}^{p-1} R(p-l)^{y^{p-l}} &= \prod_{l=1}^{p-1} \prod_{\nu=1}^{p-l} \sigma(\nu)^{\binom{p-l}{\nu}} [\sigma(\nu)^{\binom{p-l}{\nu}}, y^{p-l}] \\ &\equiv \left[\prod_{l=1}^{p-1} \prod_{\nu=1}^{p-l} \sigma(\nu)^{\binom{p-l}{\nu}}\right] T(0) \bmod K_1.\end{aligned}$$

Finally, collecting $\sigma(1), \sigma(2), \dots, \sigma(j)$ in the last double product one gets

$$\begin{aligned}&\prod_{l=1}^{p-1} \sigma(1)^{\binom{p-l}{1}} \cdots \sigma(p-l)^{\binom{p-l}{p-l}} \\ &\quad\equiv \sigma(1)^{\binom{p}{2}} \cdots \sigma(j)^{\binom{p}{j+1}} \\ &\qquad \cdot \left[\prod_{l=1}^{p-j-1} \sigma(j+1)^{\binom{p-l}{j+1}} \cdots \sigma(p-l)^{\binom{p-l}{p-l}}\right] T(j) \cdots T(1) \bmod K_1 \\ &\quad\equiv \sigma(1)^{\binom{p}{2}} \cdots \sigma(p-1)^{\binom{p}{p}} T(p-2) \cdots T(1) \bmod K_1.\end{aligned}$$

If these results are brought together we have Lemma 5.

Lemma 6. *Let $T(j)$ be defined as in Lemma 5. Then*

$$\prod_{\lambda=0}^{p-2} T(\lambda) = \prod_{k=1}^{p-1} \prod_{\lambda=0}^{k-1} [\sigma(k), \sigma(\lambda)]^{\psi(k,\lambda)}$$

where $\psi(k,\lambda) = \sum_{t=0}^{\lambda+1} \binom{\lambda+1}{t}\binom{k+t}{\lambda+1}\binom{p}{k+1+t}$.

Proof. We have

$$\prod_{\lambda=0}^{p-2} T(\lambda) = \prod_{\lambda=0}^{p-2} \prod_{l=1}^{p-1} \prod_{k=\lambda+1}^{p-l} [\sigma(k), \sigma(\lambda)]^{\binom{p-l}{k}\binom{p-l}{\lambda+1}}$$
$$= \prod_{k=1}^{p-1} \prod_{\lambda=0}^{k-1} [\sigma(k), \sigma(\lambda)]^{\psi(k,\lambda)}$$

where $\psi(k,\lambda) = \sum_{l=1}^{p-k} \binom{p-l}{k}\binom{p-l}{\lambda+1}$. Applying the second part of Lemma 2 to $\psi(k,\lambda)$ one gets the stated result.

Lemma 7. *Let $S(p)$ be defined as in Lemma 5. Then*

$$S(p) = \prod_{k=1}^{p-1} \prod_{\lambda=0}^{k-1} [\sigma(k), \sigma(\lambda)]^{\vartheta(k,\lambda)}$$

where

$$\vartheta(k,\lambda) = \sum_{t=0}^{\lambda} \left[\binom{\lambda}{t}\binom{k+t}{\lambda} - a(k,\lambda,t)\right]\binom{p}{k+1+t}.$$

Proof. We have

$$S(p) = \prod_{l=1}^{p-3} P(p-l) = \prod_{l=1}^{p-3} \prod_{k=2}^{p-l-1} \prod_{\lambda=1}^{k-1} [\sigma(k), \sigma(\lambda)]^{A(p-l,k,\lambda)}$$
$$= \prod_{k=2}^{p-2} \prod_{\lambda=1}^{k-1} [\sigma(k), \sigma(\lambda)]^{\vartheta(k,\lambda)}$$

where

$$\vartheta(k,\lambda) = \sum_{l=1}^{p-k-1} A(p-l,k,\lambda)$$
$$= \sum_{l=1}^{p-k} \left[\binom{p-l}{k}\binom{p-l}{\lambda} - \sum_{t=0}^{\lambda} a(k,\lambda,t)\binom{p-l}{k+t}\right].$$

The range of summation can be extended to $l = p-k$ since $A(k,k,\lambda) = 0$. Applying Lemma 2 we get

$$\vartheta(k,\lambda) = \sum_{t=0}^{\lambda} \left[\binom{\lambda}{t}\binom{k+t}{\lambda} - a(k,\lambda,t)\right]\binom{p}{k+1+t}.$$

Since $\vartheta(k,0) = 0$ for $k = 1,\ldots,p-1$ and $\vartheta(p-1,\lambda) = 0$ for $\lambda = 0,\ldots,p-2$, this proves Lemma 8.

By the last four lemmas

$$(xy)^p \equiv x^p y^p \sigma(1)^{\binom{p}{2}} \dots \sigma(p-1)^{\binom{p}{p}} \prod_{k=1}^{p-1} \prod_{\lambda=0}^{k-1} [\sigma(k), \sigma(\lambda)]^{B(p,k,\lambda)} \bmod K_1$$

where

$$B(p,k,\lambda) = \sum_{t=0}^{\lambda+1} \left[\binom{\lambda+1}{t} \binom{k+t}{\lambda+1} + \binom{k+2t-\lambda-1}{t-1} \binom{k+t}{k+2t-\lambda} \right] \cdot \binom{p}{k+1+t}.$$

This proves Theorem 4.

I would like to thank the referee for several valuable suggestions on this paper.

References

1. N. Blackburn, *On a special class of p-groups*, Acta Math. **100** (1958), 45–92. MR 21 #1349.

2. P. Hall, *A contribution to the theory of groups of prime power orders*, Proc. London Math. Soc. **36** (1933), 29–95.

3.B. Huppert, *Endliche Gruppen* I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR 37 #302.

4. R. Miech, *Some p-groups of maximal class*, Trans. Amer. Math. Soc. **189** (1974), 1–47.

Department of Mathematics, University of California, Los Angeles, California 90024