BULL. AUSTRAL. MATH. SOC. 12E10
VOL. 12 (1975), 81-87. (20E35, 20F50)

Polynomials associated with groups of exponent four

M.F. Newman, K.W. Weston, and Tah-Zen Yuan

Complicated groups of exponent four have been constructed from the ring of polynomials in associating non-commuting indeterminates with coefficients from the field of two elements. The justification of these constructions depends on a computational reduction result. In this note a further reduction is obtained. The expressions involved seem to have an interesting combinatorial structure.

The proofs that such groups of exponent four have the claimed properties depend on showing that certain polynomials do not lie in a particular ideal T (described below). This ideal T is one of a set introduced by Bruck [4] in connection with the study of the Burnside questions. In particular T was used by Bachmuth, Mochizuki and Walkup [2] in showing that there are insoluble groups of exponent five. In this note we describe a generating set for the ideal T which makes it easier to work with. Specifically it reduces the amount of computational effort needed to decide whether a given polynomial lies in T or not.

Let $K[X]$ be the ring of polynomials in a set X of associating non-commuting indeterminates with coefficients from a commutative ring K with multiplicative identity 1. (It is no harder to deal with this case.) If Y is an ordered finite subset of X, the monomial which is the product of the elements of Y in the given order is also denoted Y. Let $S(Y)$ denote the sum of the monomials Z where Z runs through all the non-empty sub-ordered-sets of Y; so $S(Y) = y + z + yz$ for $Y = (y, z)$.

Received 11 October 1974.

Let $T(Y)$ be the homogeneous component of degree one in each element of Y of $(S(Y))^3$; so $T(Y) = 0$ for $Y = (y, z)$ and

$$T(Y) = xyz + xzy + yxz + yzx + zxy + zyx$$

for $Y = (x, y, z)$. Let T be the ideal generated by all the $T(Y)$. In the papers quoted a slightly larger ideal is called T. There T also contains all polynomials obtained by substituting elements of X for elements of Y in the $T(Y)$. So there, for instance, $2xxy + 2xyx + 2yxx$ is included. It is easy to see that the results here carry over to that ideal.

The polynomials $T(Y)$ quickly become long sums of monomials as $|Y|$ increases. In characteristic zero $T(Y)$ is the sum of $3^n - 3\cdot 2^n + 3$ monomials where $n = |Y|$. The second column of the table below gives the length of $T(Y)$ in characteristic two for $|Y|$ up to nine. It is, therefore, desirable to find generating sets for T which consist of shorter polynomials. A first result of this kind was obtained in [5] (for the field of two elements); this is stated as Theorem A below. The extent of the improvement can be seen by comparing the second and third columns of the table. The length of the shorter polynomial is $2^{n-2} + 4$. The calculations in [1] and [3] use these polynomials. In Theorem B an even shorter generating set for T is given. The fourth column of the table refers to this set; the length of these polynomials is given by

$$(2 + n - 2[n/2])\cdot 2^{[n/2]}$$

where [ ] denotes the integer part of.

https://doi.org/10.1017/S0004972700023650 Published online by Cambridge University Press

Lengths of polynomials in characteristic two

n	$T(Y)$ $\lvert Y\rvert = n$	$C(Z, Y) + C(Y^*, Z^*)$ $\lvert Y\rvert + \lvert Z\rvert = n$	
		$\lvert Z\rvert = 2$	$\lvert Y\rvert \le \lvert Z\rvert \le \lvert Y\rvert + 1$
3	6	6	6
4	12	8	8
5	92	12	12
6	302	20	16
7	1312	36	24
8	4294	68	32
9	15 110	132	48
10		260	64
11			96

For Y, Z ordered finite subsets of X let $C(Y, Z)$ be the sum of all the monomials WZW' where W runs through all (including the empty set) sub-ordered-sets of Y and W' is the complement of W in Y with order induced from Y ; thus

$$C(Y, Z) = xyZ + xZy + yZx + Zxy$$

for $Y = (x, y)$. Finally let Y^* be the monomial which is the product of the elements of Y in reverse order.

THEOREM A. *The ideal T is generated by the polynomials*

$$C(Z, Y) - (-1)^{|Y|}C(Y^*, Z^*)$$

where Y, Z run through all ordered non-empty finite subsets of X such that Y, Z are disjoint, $|Z| = 2$ and $3 \le |Y| + |Z|$.

THEOREM B. *The ideal T is generated by the polynomials*

$$C(Z, Y) - (-1)^{|Y|+|Z|}C(Y^*, Z^*)$$

where Y, Z run through all ordered finite subsets of X such that Y, Z are disjoint and $|Y| \le |Z| \le |Y| + 1$.

These theorems are proved together.

LEMMA 1. *For every ordered finite subset Y of X ,*

https://doi.org/10.1017/S0004972700023650 Published online by Cambridge University Press

$$(S(Y))^3 = \sum T(W) + R$$

where the sum is taken over all sub-ordered-sets W *of* Y *and* R *is a sum of monomials each of which has a repeated factor from* X .

Proof. Let $U(Y)$ be the sum of monomials in $(S(Y))^3$ with no repeated factor from X . Clearly $\sum T(W)$ is a sub-sum of $U(Y)$. For y in Y the result of putting $y = 0$ in $U(Y) - \sum T(W)$ is, inductively, the zero polynomial. Hence $U(Y) - \sum T(W)$ must be a sum of monomials of degree one in each element of Y . But $T(Y)$ is the sum of *all* such monomials. Therefore $U(Y) = \sum T(W)$ as required.

Let Y be an ordered finite subset of X with first element x and let Z be the complement of x in Y . Let $B(x, Z)$ be the homogeneous component of degree one in each element of Y of

$$(S(Z))^2x + S(Z)xS(Z) + x(S(Z))^2 ;$$

thus $B(x, Z) = T(Y)$ for $Y = (x, y, z)$. A proof similar to that of Lemma 1 yields the following.

LEMMA 2. *For* x, Z *as above*

$$(S(Z))^2x + S(Z)xS(Z) + x(S(Z))^2 = \sum B(x, W) + R$$

where the sum is taken over all sub-ordered-sets W *of* Z *and* R *is a sum of monomials with a repeated factor.*

Let $T(n)$ be the ideal generated by all $T(Y)$ with $|Y| \leq n$ and R the ideal generated by all monomials with a repeated factor.

LEMMA 3. *For* $|Z| = n$,

$$T(xZ) \equiv B(x, Z) \text{ modulo } T(n) .$$

Proof. Work modulo $T(n) + R$. By Lemma 1,

https://doi.org/10.1017/S0004972700023650 Published online by Cambridge University Press

$$T(xZ) \equiv \big(S(xZ)\big)^3$$
$$\equiv \big(x+S(Z)+xS(Z)\big)^3$$
$$\equiv x\big(S(Z)\big)^2 + S(Z)xS(Z) + \big(S(Z)\big)^2x + S(Z)x\big(S(Z)\big)^2 + \big(S(Z)\big)^2xS(Z)$$

since $\big(S(Z)\big)^3$ belongs to $T(n) + R$. Multiplying this congruence on the right by $S(Z)$ gives

$$0 \equiv S(Z)x\big(S(Z)\big)^2 + \big(S(Z)\big)^2xS(Z) + \big(S(Z)\big)^2x\big(S(Z)\big)^2 ,$$

$$0 \equiv \big(S(Z)\big)^2x\big(S(Z)\big)^2 .$$

Hence $T(xZ) \equiv x\big(S(Z)\big)^2 + S(Z)xS(Z) + \big(S(Z)\big)^2x$. The result follows from Lemma 2 since $T(xZ)$ is a sum of monomials with no repeated factor.

Observe that for Z non-empty

$$B(x, Z) = C(Z, x) + \sum C(x, WW') - 3C(x, Z)$$

where the sum is taken over all sub-ordered-sets W of Z and W' is the complement of W in Z. Let

$$B(Y, Z) = C(Z, Y) - (-1)^{|Y|} \sum C(Y^*, WW') + (-1)^{|Y|}3C(Y^*, Z) .$$

If $|Z| = 2$, then $B(Y, Z) = C(Z, Y) - (-1)^{|Y|}C(Y^*, Z^*)$. So Theorem A can be proved by establishing a suitable link between values of B.

A first step towards this is a link between values of C.

LEMMA 4. *If x is an element of an ordered finite subset X_0 of X and Y is the ordered set of predecessors of x in X_0 and Z is the set of successors of x in X_0, then*

$$C(xZ, Y) = C(Z, Yx) + xC(Z, Y) .$$

Proof. From the definition $C(xZ, Y) = \sum WYW'$ where the sum is taken over all sub-ordered sets W of xZ. Hence

$$C(xZ, Y) = \sum_{x\in W} WYW' + \sum_{x\in W'} WYW'$$
$$= x \sum VYV' + \sum V(Yx)V'$$

https://doi.org/10.1017/S0004972700023650 Published online by Cambridge University Press

where both sums are taken over all sub-ordered-sets V of Z. The result follows.

LEMMA 5. *With the notation as in Lemma 4 and Y, Z non-empty*

$$B(Y, xZ) \equiv B(Yx, Z) \text{ modulo } T(|Y|+|Z|) .$$

Proof. From the definition

$$B(Y, xZ) = C(xZ, Y) + (-1)^{|Y|}\left(3C(Y^*, xZ) - \sum C(Y^*, WW')\right)$$

where the sum is taken over all sub-ordered-sets W of xZ. Hence

$$B(Y, xZ) = C(xZ, Y) + (-1)^{|Y|}\left(3C(Y^*, xZ) - \sum C(Y^*, xVV') - \sum C(Y^*, VxV')\right)$$

where both sums are taken over all sub-ordered-sets V of Z. Now $B(x, Z) = \sum (xVV'+VxV'+VV'x) - 3xZ - 3Zx$ lies in $T(|Y|+|Z|)$ so

$$B(Y, xZ) \equiv C(xZ, Y) + (-1)^{|Y|}\left(\sum C(Y^*, VV'x) - 3C(Y^*, Zx)\right)$$

since C is linear in the second place. Using Lemma 4 gives

$$\begin{aligned} B(Y, xZ) &\equiv C(Z, Yx) + (-1)^{|Y|}\left(\sum C(xY^*, VV') - 3C(xY^*, Z)\right) \\ &\quad + xC(Z, Y) + (-1)^{|Y|}\left(-x \sum C(Y^*, VV') + 3xC(Y^*, Z)\right) \\ &\equiv B(Yx, Z) + xB(Y, Z) \\ &\equiv B(Yx, Z) \end{aligned}$$

as required.

Let n be an integer, at least 2, and Y, Z disjoint subsets of X with $|Y| = n - 1$ and $|Z| = 2$, then

$$T(YZ) \equiv C(Z, Y) - (-1)^{|Y|}C(Y^*, Z^*) \text{ modulo } T(n) .$$

A simple induction over n completes the proof of Theorem A.

In the notation of Lemma 4, and using Lemma 4,

$$\begin{aligned} C(Z, Yx) - (-1)^{|Y|+|Z|+1}C(xY^*, Z^*) &= C(xZ, Y) - (-1)^{|Y|+|Z|+1}C(Y^*, Z^*x) \\ &\quad - x\left(C(Z, Y) - (-1)^{|Y|+|Z|}C(Y^*, Z^*)\right) . \end{aligned}$$

Another simple induction over n and repeated use of this yield Theorem B.

https://doi.org/10.1017/S0004972700023650 Published online by Cambridge University Press

References

[1] Seymour Bachmuth and Horace Y. Mochizuki, "A criterion for non-solvability of exponent 4 groups", *Comm. Pure Appl. Math.* 26 (1973), 601-608.

[2] S. Bachmuth, H.Y. Mochizuki and D.W. Walkup, "Construction of a nonsolvable group of exponent 5 ", *Word Problems. Decision problems and the Burnside problem in group theory*, 39-66 (Studies in Logic and the Foundations of Mathematics, 71. North-Holland, Amsterdam, London, 1973).

[3] S. Bachmuth, H.Y. Mochizuki and K. Weston, "A group of exponent 4 with derived length at least 4 ", *Proc. Amer. Math. Soc.* 39 (1973), 228-234.

[4] R.H. Bruck, *Engel conditions in groups and related questions* (Lecture Notes. Third Summer Research Institute of the Austral. Math. Soc., Canberra, 1963).

[5] Tah-Zen Yuan, "On the solvability of the freest group of exponent 4 ", (Dissertation, University of Notre Dame, Notre Dame, Indiana, 1969).

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT;

Department of Mathematics,
University of Wisconsin-Parkside,
Kenosha,
Wisconsin, USA;

Metropolitan Milwaukee Association of Commerce,
Milwaukee,
Wisconsin, USA.