PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 33, Number 2, June 1972

ON POLYNOMIALS WHICH COMMUTE WITH A GIVEN POLYNOMIAL

WILLIAM M. BOYCE

ABSTRACT. By extending a theorem of Jacobsthal, the following result is obtained: if g is a nonlinear polynomial, there is an integer $J(g)\geqq 1$ such that for each $m>0$ there are either $J(g)$ or zero distinct polynomials of degree m which commute with g. A formula is given for computing $J(g)$ from the coefficients of g.

We say that a pair of polynomials f, g *commute* if $f(g(x))=g(f(x))$ for all x. Fifty years ago, J. F. Ritt [4] proved that commuting polynomials must be, within a linear homeomorphism, either both powers of x, both iterates of the same polynomial, or both Tchebycheff polynomials. Yet Ritt's proof is so complicated and relies on such deep results from analysis that there is still interest in what can be proved about commuting polynomials without resorting to his methods (see [1], [2], [3]). In this paper we offer results extending the algebraic, nonanalytic approach to the problem.

A principal result presented here concerns the number of polynomials of degree $m>0$ which commute with a given polynomial g of degree $n>1$. We show that there is an integer $J(g)\geqq 1$ such that for each $m>0$, either $J(g)$ or zero distinct polynomials of degree m commute with g. In addition we show how $J(g)$ may be computed from the coefficients of g. Our main tool is Theorem 1, which is an extension of Theorem 19 of Jacobsthal [3]. Although Jacobsthal claims for Theorem 19 only the result that $J(g)\leqq n-1$, in his proof he gives an algorithm for computing any mth degree polynomial which commutes with g from its leading coefficient, and we find that just a small addition to his proof produces a much stronger theorem.

Our notation is mostly taken from Jacobsthal, as follows: g and f are polynomials of degrees $n>1$ and $m>0$ respectively,

$$g(x)=\sum_{i=0}^{n} b_i x^{n-i}, \quad f(x)=\sum_{i=0}^{m} a_i x^{m-i}, \qquad a_0 b_0 \neq 0,$$

Presented to the Society, September 1, 1971; received by the editors August 25, 1971.
AMS 1970 *subject classifications*. Primary 12A20, 30A20; Secondary 10A30, 13F20, 20M20.
Key words and phrases. Commuting functions, commuting polynomials, common fixed point, Tchebycheff polynomials, functional composition.

and

$$(g(x))^p = \sum_{k=0}^{np} B_{p,k}x^{np-k}, \qquad (f(x))^p = \sum_{k=0}^{mp} A_{p,k}x^{mp-k}.$$

New notation includes

$$\alpha = a_0, \quad \beta = b_1/nb_0, \quad \text{and} \quad h(x) = \sum_{i=0}^{m} c_i x^{m-i}.$$

The expression "$a(x)=o(x^k)$" signifies $\lim_{|x|\to\infty} a(x)x^{-k}=0$.

THEOREM 1. *Given g and $m>0$, there is a unique monic polynomial h of degree m such that if $\alpha^{n-1}=(b_0)^{m-1}$, then $f(x)=\alpha h(x)-\beta$ is the unique polynomial of degree m with leading coefficient α for which $f(g(x))=g(f(x))+o(x^{(n-1)m})$.*

PROOF. As stated above, the proof is basically that of Jacobsthal's Theorem 19. He obtains the $m+1$ coefficients a_i of f by matching the coefficients of the $m+1$ highest powers of x in $f(g(x))$ and $g(f(x))$. (Thus the highest unmatched power is $(n-1)m-1$, and the difference is $o(x^{(n-1)m})$.) The matching equation for degree mn is

$$a_0(b_0)^m = b_0(a_0)^n,$$

which is satisfied by the choice $a_0=\alpha$ ($c_0=1$), and we proceed by induction. Jacobsthal shows that the equation for degree $mn-(q+1)$ has the form

$$C_{q+1} = b_0A_{n,q+1} = b_0(n(a_0)^{n-1}a_{q+1} + D_{q+1})$$

where C_{q+1} and D_{q+1} are functions of n, m, the coefficients of g (the b_i), and the a_i with $i\leqq q$; except that for $q+1=m$ there is an additional term,

$$b_1(a_0)^{n-1} = nb_0\beta(a_0)^{n-1},$$

on the right-hand side. From this he concludes that each a_{q+1} is uniquely determined by the condition that the $mn-i$ degree coefficients of $f(g(x))$ and $g(f(x))$ match for $i\leqq q+1$ once a_0 is chosen, and so there are at most as many f which commute with g as there are roots a_0 of $(a_0)^{n-1}=(b_0)^{m-1}$.

But let us add the induction hypothesis that $a_i=\alpha c_i$ for $i\leqq q$, where c_i depends only on the b_j, the coefficients of g. Then C_{q+1} is a sum of terms $a_kB_{k,q+1}$ with $k\leqq q$, which by the induction hypothesis may be written as $\alpha c_kB_{k,q+1}$. But then $C_{q+1}=\alpha C'_{q+1}$ where C'_{q+1} does not depend on any a_i. Also D_{q+1} is a linear combination of terms of the form

$$\prod_{i=0}^{q} a_i^{\lambda_i}, \qquad \sum_{i=0}^{q} \lambda_i = n,$$

and by the induction hypothesis these become

$$\prod_{i=0}^{q} (\alpha c_i)^{\lambda_i} = \alpha^{\sum \lambda_i} \prod_{i=0}^{q} c_i^{\lambda_i} = \alpha^n D,$$

so $D_{q+1}=\alpha^n D'_{q+1}$ where D'_{q+1} depends on no a_i. But when we use the fact that $\alpha=a_0$ and $(a_0)^{n-1}=\alpha^{n-1}=(b_0)^{m-1}$, the matching equation for a_{q+1} becomes

$$\alpha C'_{q+1} = b_0(n(b_0)^{m-1}a_{q+1} + \alpha(b_0)^{m-1}D'_{q+1}).$$

Then defining

$$c_{q+1} = (C'_{q+1}(b_0)^{-m} - D'_{q+1})/n$$

gives the desired result that $a_{q+1}=\alpha c_{q+1}$ when $q+1<m$. In the exceptional case $q+1=m$, the additional term changes the expression to the desired $a_m=\alpha c_m-\beta$. Thus $f(x)=\alpha h(x)-\beta$ as was claimed.

COROLLARY (JACOBSTHAL [3]). *A polynomial which commutes with a given nonlinear polynomial is uniquely identified by its degree and leading coefficient. Thus at most* $(n-1)$ *polynomials of degree* $m>0$ *commute with a given nonlinear polynomial.*

PROOF. If f commutes with g then the procedure given in Theorem 1 must derive f from its degree and leading coefficient, since

$$f(g(x)) - g(f(x)) = 0 = o(x^k).$$

THEOREM 2. *If there is a polynomial* f *of degree* $m>0$ *which commutes with* g, *then the polynomials of degree* m *which commute with* g *are exactly those of the form* $uf(x)+(u-1)\beta$ *where* u *satisfies* $u^{n-1}=1$ *and*

$$g(ux + (u-1)\beta) = ug(x) + (u-1)\beta \tag{1}$$

for all x.

PROOF. If f and f' commute with g, then by Theorem 1,

$$f(x) = a_0h(x) - \beta, \qquad f'(x) = a'_0h(x) - \beta,$$

so

$$f'(x) = u(a_0h(x) - \beta) + (u-1)\beta = uf(x) + (u-1)\beta$$

where $u=a'_0/a_0$. Since $(a'_0)^{n-1}=(b_0)^{m-1}=(a_0)^{n-1}$, we have $u^{n-1}=1$. Given x, let z be a solution of $f(z)=x$. Then since g commutes with both f and f',

$$\begin{aligned} g(ux + (u-1)\beta) &= g(uf(z) + (u-1)\beta) = g(f'(z)) = f'(g(z)) \\ &= uf(g(z)) + (u-1)\beta = ug(f(z)) + (u-1)\beta \\ &= ug(x) + (u-1)\beta. \end{aligned}$$

Conversely, if f commutes with g and u satisfies (1), then working backwards we see that g commutes with $f'(x)=uf(x)+(u-1)\beta$.

REMARK. We note that $u=1$ satisfies (1) trivially.

COROLLARY. *Let $J(g)\geqq 1$ be the number of u which satisfy $u^{n-1}=1$ and* (1). *Then for each $m>0$ there are either $J(g)$ or zero distinct polynomials of degree m which commute with g.*

DEFINITION. $j(g)=\mathrm{GCD}\{i-1 \mid b_{n-i}\neq 0\}$.

THEOREM 3. *If $b_1=0$, then $J(g)=j(g)$, and if there is an f of degree $m>0$ which commutes with g, then the mth degree polynomials which commute with g are exactly those of the form uf, where u is a $j(g)$th root of unity.*

PROOF. Since $\beta=b_1/nb_0$, $b_1=0$ implies $\beta=0$, and then (1) becomes simply $g(ux)=ug(x)$. Then when

$$g(ux)=\sum_{i=0}^{n} b_{n-i}(ux)^i=\sum_{i=0}^{n} b_{n-i}u^ix^i=ug(x)=\sum_{i=0}^{n} b_{n-i}ux^i,$$

for each i, we have $b_{n-i}u^i=b_{n-i}u$ or $b_{n-i}u(u^{i-1}-1)=0$. Thus either $b_{n-i}=0$ or $u^{i-1}=1$ for each i. Let k be the order of u, the least positive integer such that $u^k=1$. Then $k \mid (i-1)$ for each i for which $b_{n-i}\neq 0$, so $k \mid j(g)$. On the other hand, each $j(g)$th root of unity satisfies $g(ux)=ug(x)$, so $J(g)=j(g)$, and Theorem 2 shows that uf commutes with g if and only if f does.

COROLLARY (BERTRAM [1]). *If f commutes with T_n, the Tchebycheff polynomial of degree n, then $f=T_m$ if n is even and $f=\pm T_m$ if n is odd.*

PROOF. The coefficients of a Tchebycheff polynomial are alternatively nonzero and zero, so $j(T_n)=1$ if n is even and $j(T_n)=2$ if n is odd. But T_m commutes with T_n, and $-T_m$ commutes with T_n if n is odd, so the possibilities for mth degree polynomials commuting with T_n are exhausted by $\pm T_m$.

We see from Theorem 3 that the theory is much simpler when g has second coefficient zero. But we can always reduce a problem to this case, since $g(x-\beta)$ always has second coefficient zero, hence $g_\beta(x)=g(x-\beta)+\beta$ has second coefficient zero. The commutativity relations are maintained when we reduce g to g_β, since g commutes with f if and only if g_β commutes with $f_\beta(x)=f(x-\beta)+\beta$.

THEOREM 4. *The unit u satisfies* (1) *if and only if $g_\beta(ux)=ug_\beta(x)$, so $J(g)=J(g_\beta)=j(g_\beta)$, and u satisfies* (1) *if and only if u is a $J(g)$th root of unity. Thus if an mth degree polynomial f commutes with g, then the mth degree polynomials commuting with g are exactly those of the form $uf(x)+(u-1)\beta$, where u is a $j(g_\beta)$th root of unity.*

PROOF. We need only show that u satisfies (1) if and only if $g_\beta(ux)=ug_\beta(x)$; the remainder of the theorem follows from Theorems 2 and 3. So if u satisfies (1), we have

$$\begin{aligned} g_\beta(ux) &= g(ux-\beta)+\beta = g(u(x-\beta)+(u-1)\beta)+\beta \\ &= [ug(x-\beta)+(u-1)\beta]+\beta = u[g(x-\beta)+\beta] = ug_\beta(x), \end{aligned}$$

and if $g_\beta(ux)=ug_\beta(x)$, then

$$\begin{aligned} g(ux+(u-1)\beta) &= g(u(x+\beta)-\beta) = g_\beta(u(x+\beta))-\beta \\ &= ug_\beta(x+\beta)-\beta = u[g(x)+\beta]-\beta \\ &= ug(x)+(u-1)\beta. \end{aligned}$$

Thus the equivalence is shown.

AN EXAMPLE. Let

$$g(x) = x^4-4x^3+6x^2-4x+2 = (x-1)^4+1.$$

Then $\beta=-1$. We see that

$$f(x) = x^2-2x+2 = (x-1)^2+1$$

commutes with g, since $g_\beta(x)=x^4$ and $f_\beta(x)=x^2$. Then $J(g)=j(g_\beta)=3$. Choose $\omega=\frac{1}{2}(-1+\sqrt{3}\,i)$ so that $\omega^3=1$. Then

$$\omega f(x)+(\omega-1)(-1) = \omega(x-1)^2+1 = \omega x^2-2\omega x+(\omega+1)$$

commutes with g.

REMARK. The (multivalued) mapping from the nth degree polynomials into those of mth degree described in Theorem 1 might have interesting properties. For instance, if $m\geqq n$ then applying Theorem 1 to g and then to the resulting f yields g again if the leading coefficients agree. However, in general it will be impossible to regenerate g if $m<n$, as is illustrated by $(x^3+1)\to(x^2)\to(x^3)$. Might some sort of iteration of this mapping always converge to a pair of commuting polynomials?

We appreciate the assistance of H. S. Witsenhausen.

ADDED IN PROOF. We are indebted to L. I. Wade for pointing out to us that in [5] and [6] Ritt's results are derived algebraically for polynomials over fields of characteristic zero. These papers have not previously been referenced in the commuting functions literature.

REFERENCES

1. E. A. Bertram, *Polynomials which commute with a Tchebycheff polynomial*, Amer. Math. Monthly **68** (1971), 650–653.

2. H. D. Block and H. P. Thielman, *Commutative polynomials*, Quart. J. Math. Oxford Ser. (2) **2** (1951), 241–243. MR **13**, 552.

3. E. J. Jacobsthal, *Über vertauschbare Polynome*, Math. Z. **63** (1955), 243–276. MR **17**, 574.

4. J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.

5. H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

6. Howard Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.

BELL TELEPHONE LABORATORIES, INCORPORATED, MURRAY HILL, NEW JERSEY 07974