ON EXCEPTIONAL POLYNOMIALS

Kenneth S. Williams

Let $f(x)$ be a polynomial of degree $d \geq 2$ defined over the finite field k_q with $q = p^n$ elements. Let

$$(1) \qquad f^*(x, y) = \frac{f(x) - f(y)}{x - y} .$$

If $f^*(x, y)$ has no irreducible factor over k_q which is absolutely irreducible, f is called an exceptional polynomial [1]. Davenport and Lewis have noted that when d is small compared with p, a permutation (substitution) polynomial is necessarily an exceptional polynomial. It is the purpose of this paper to prove the converse; that is, we will show the existence of a constant $a(d)$, depending only on d, such that if $f(x)$ is an exceptional polynomial over k_q, where $p \geq a(d)$, then $f(x)$ is a permutation polynomial.

If $f(x)$ is an exceptional polynomial over k_q then, in the terminology of [2], $f(x)$ is an extremal polynomial of index 0. Hence by theorem 1 in [2] we have

$$(2) \qquad |V(f) - q| \leq k(d) ,$$

where the constant $k(d)$ depends only on d and $V(f)$ denotes the number of distinct values of y in k_q for which at least one of the roots of $f(x) = y$ is in k_q. Hence we can write $V(f) = q - w$, where $0 \leq w \leq k(d)$. It suffices to prove that $w = 0$. We assume $w \geq 1$ and obtain a contradiction.

Let the distinct values taken by $f(x)$ in k_q be $r_1, r_2, \ldots, r_{q-w}$ and the distinct values not taken by $f(x)$ be $n_1, n_2, \ldots, n_w$. Let the values r_i $(1 \leq i \leq q-w)$ occur for m_i $(1 \leq i \leq q-w)$ values of x so that $\sum_{i=1}^{q-w} m_i = q$. Now each $m_i \geq 1$ so that for $r = 1, 2, \ldots, q-w$ we have

$$(3) \qquad m_r \leq w + 1 .$$

Now for $t = 1, 2, \ldots, w$ we have

https://doi.org/10.4153/CMB-1968-033-1 Published online by Cambridge University Press

$$\sum_{x \in k_q} \{f(x)\}^t = \sum_{i=1}^{q-w} \sum_{\substack{x \in k_q \\ f(x) = r_i}} \{f(x)\}^t = \sum_{i=1}^{q-w} m_i r_i^t .$$

On the other hand we can write $f(x) = f_o + f_1 x + \ldots + f_d x^d$ where each $f_i (0 \leq i \leq d) \epsilon k_q$. Now if $p \geq a(d)$, where $a(d) = dk(d) + 2$, we have $q-2 \geq p-2 \geq dk(d) \geq dw$ so we can write for $t = 1, 2, \ldots, w$, $\{f(x)\}^t = f_o^{(t)} + f_1^{(t)} x + \ldots + f_{q-2}^{(t)} x^{q-2}$. Then

$$\sum_{x \in k_q} \{f(x)\}^t = \sum_{j=0}^{q-2} f_j^{(t)} \sum_{x \in k_q} x^j .$$

Now $\sum_{x \in k_q} x^j = 0$ for $j = 0, 1, 2, \ldots, q-2$; so

$$\sum_{x \in k_q} \{f(x)\}^t = 0 \qquad (t = 1, 2, \ldots, w).$$

Thus we have

(4) $$\sum_{i=1}^{q-w} m_i r_i^t = 0 \qquad (t = 1, 2, \ldots, w).$$

Now set $m = \max_{1 \leq i \leq q-w} m_i$ so that from (3) we have $1 \leq m \leq w + 1$. If $s_j (1 \leq j \leq m)$ denotes the number of $m_i (1 \leq i \leq q-w)$ with $m_i = j$,

$$s_j = \sum_{\substack{i=1 \\ m_i = j}}^{q-w} 1 ,$$

so that

$$\sum_{j=1}^{m} s_j = \sum_{j=1}^{m} \sum_{\substack{i=1 \\ m_i = j}}^{q-w} 1 = \sum_{i=1}^{q-w} 1 = q - w$$

https://doi.org/10.4153/CMB-1968-033-1 Published online by Cambridge University Press

and

$$\sum_{j=1}^{m} js_j = \sum_{j=1}^{m} j \sum_{\substack{i=1 \\ m_i=j}}^{q-w} 1 = \sum_{j=1}^{m} \sum_{\substack{i=1 \\ m_i=j}}^{q-w} m_i = \sum_{i=1}^{q-w} m_i = q .$$

Now reorder $r_1, \ldots, r_{q-w}$ so that $r_1, \ldots, r_{s_1}$ have $m_1 = \ldots = m_{s_1} = 1$; $r_{s_1+1}, \ldots, r_{s_1+s_2}$ have $m_{s_1+1} = \ldots = m_{s_1+s_2} = 2$; $\ldots$; $r_{s_1+s_2+\ldots+s_{m-1}+1}, \ldots, r_{s_1+\ldots+s_m} = q-w$ have $m_{s_1+\ldots+s_{m-1}+1} = \ldots = m_{s_1+\ldots+s_m} = m$. Hence (for $t = 1, 2, \ldots, w$) (4) becomes

$$\sum_{j=1}^{m} j \sum_{i=s_1+\ldots+s_{j-1}+1}^{s_1+\ldots+s_j} r_i^t = 0.$$

Thus (for $t = 1, \ldots, w$)

$$\sum_{j=1}^{w} n_j^t = \sum_{j=1}^{w} n_j^t + \sum_{j=1}^{m} j \sum_{i=s_1+\ldots+s_{j-1}+1}^{s_1+\ldots+s_j} r_i^t$$

$$= \sum_{x \in k_q} x^t + \sum_{j=1}^{m} (j-1) \sum_{i=s_1+\ldots s_{j-1}+1}^{s_1+\ldots+s_j} r_i^t .$$

Now $1 \leq t \leq w \leq dw \leq dk(d) \leq q-2$ so $\sum_{x \in k_q} x^t = 0$. Hence

(5) $$\sum_{j=1}^{w} n_j^t = \sum_{j=2}^{m} (j-1) \sum_{i=s_1+\ldots+s_{j-1}+1}^{s_1+\ldots+s_j} r_i^t .$$

We next consider the two polynomials, both of degree w,

$$g(\theta) = \prod_{j=1}^{w} (\theta - n_j)$$

and

https://doi.org/10.4153/CMB-1968-033-1 Published online by Cambridge University Press

$$h(\theta) = \prod_{j=2}^{m} \prod_{i=1}^{s_j} (\theta - r_{s_1+\ldots+s_{j-1}+i})^{j-1}.$$

Let $g_i, h_i (i = 0, 1, \ldots, w)$ denote the coefficients of θ^{w-i} in $g(\theta)$ and $h(\theta)$ respectively. Clearly, $g_o = h_o = 1$. Also let $G_t, H_t (t = 1, 2, \ldots, w)$ denote the sum of the t^{th} powers of all of the roots of $g(\theta)$ and $h(\theta)$, respectively. Thus by (5) $G_t = H_t$ $(t = 1, 2, \ldots, w)$. Newton's first w identities for $g(\theta)$ are

$$(6) \qquad \sum_{i=0}^{t-1} G_{t-i} g_i + t g_t = 0 \qquad (t = 1, 2, \ldots, w).$$

Now $p \geq dk(d) + 2 > dk(d) > k(d) \geq w$ so the coefficient of g_t in (6) does not vanish in k_q. Hence the w equations can be solved successively and uniquely for $g_1, \ldots, g_w$ in terms of $G_1, \ldots, G_w$; $g_1 = - G_1$, $g_2 = 2^{-1}(G_1^2 - G_2)$, etc. Similarly we obtain $h_1 = - H_1$, $h_2 = 2^{-1}(H_1^2 - H_2)$, etc., and so as $G_t = H_t$ we have $g_i = h_i$ for $i = 0, 1, 2, \ldots, w$. Hence $g(\theta) \equiv h(\theta)$ and so $\{n_1, \ldots, n_w\}$ must be a rearrangement of $\{r_{s_1+1}, \ldots, r_{q-w}\}$. This is clearly impossible as the r's are distinct from the n's by definition. This completes the proof.

REFERENCES

1. H. Davenport and D. J. Lewis, Notes on congruences (I), Quart. J. Math. Oxford (2) 14 (1963), 51-60.

2. K.S. Williams, On extremal polynomials. Canad. Math. Bull. 10 (1967), 585-594.

Carleton University
Ottawa

https://doi.org/10.4153/CMB-1968-033-1 Published online by Cambridge University Press