ON EXTREMAL POLYNOMIALS

Kenneth S. Williams

(received April 9, 1967)

Let \( p \) denote a prime number and let \( k \) denote the finite field of \( p \) elements. Let \( f(x) \in k[x] \) be of fixed degree \( d \geq 2 \).

We suppose that \( p \) is also fixed, large compared with \( d \), say, \( p \geq p_o(d) \). By \( V(f) \) we denote the number of distinct values of \( f(x), x \in k \). We call \( f \) maximal \(^1\) if \( V(f) = p \) and quasi-maximal \(^2\) if \( V(f) = p + O(1) \). Clearly a maximal polynomial is quasi-maximal but it is not known under what conditions the converse holds. As \( dV(f) \geq p \), the minimum possible value of \( V(f) \) is \( \geq \left[ \frac{p-1}{d} \right] + 1 \).

When \( f(x) = x^d \) and \( p \equiv 1 \) (mod \( d \)), \( V(f) = \frac{p-1}{d} + 1 \), so \( \left[ \frac{p-1}{d} \right] + 1 \) is in fact the actual minimum. If \( V(f) = \left[ \frac{p-1}{d} \right] + 1 \) we call \( f \) a minimal polynomial and if \( V(f) = \frac{p}{d} + O(1) \) a quasi-minimal polynomial. Clearly a minimal polynomial is a quasi-minimal polynomial and Mordell has noted in an addendum to [7] that the converse is true for \( p \geq p_o(d) \). It seems reasonable to conjecture that a quasi-maximal polynomial is maximal for \( p \geq p_o(d) \).

It is the purpose of this paper to generalize the ideas of quasi-maximal and quasi-minimal. We set

\[
(1) \quad f^*(x, y) = \frac{f(x) - f(y)}{x - y}
\]

\(^1\) Dickson [6] calls such a polynomial a substitution polynomial.

\(^2\) We shall see later that these are the exceptional polynomials of Davenport and Lewis [5]. (See Corollary 1 and Theorem 2.)

and call \( f(x) \) an extremal polynomial of index \( \ell \) if, in the (unique) decomposition of \( f^\phi(x, y) \) into irreducible factors in \( \mathbb{Q}_p[x, y] \), there are \( \ell \) linear factors and no non-linear absolutely irreducible factors. Clearly \( 0 \leq \ell \leq d-1 \). For example, \( f(x) = x^4 \) is extremal of index 1 when \( p \equiv 3 \pmod{4} \) since

\[
\frac{x^4 - y^4}{(x-y)(x+y)} = x^2 + y^2
\]

is irreducible but not absolutely irreducible. When \( p \equiv 1 \pmod{4} \) there exists \( w \in \mathbb{Q}_p \) such that \( w^2 = -1 \) so that

\[
\frac{x^4 - y^4}{x-y} = (x+y)(x+wy)(x-wy);
\]

hence \( f(x) = x^4 \) is extremal of index 3 in this case. On the other hand, \( f(x) = x^3 + x \) is not an extremal polynomial as

\[
\frac{(x^3 + x) - (y^3 + y)}{x-y} = x^2 + xy + y^2 + 1
\]

is absolutely irreducible in \( \mathbb{Q}_p[x, y] \) for any prime \( p > 3 \).

**Theorem 1.** If \( f(x) \) is extremal of index \( \ell \) then

\[
V(f) = \frac{p}{\ell + 1} + O(1) .
\]

**Proof.** As \( f(x) \) is extremal of index \( \ell \) we can write

\[
f^\phi(x, y) = \prod_{i=1}^{\ell} g_i(x, y) \prod_{j=1}^{m} h_j(x, y),
\]

where each \( g_i(x, y) \) is linear so that \( \ell \) (possibly 0) is the index of \( f \) and each \( h_j(x, y) \) is irreducible but not absolutely irreducible in \( \mathbb{Q}_p[x, y] \). Clearly no two of \( g_1, g_2, \ldots, g_\ell \) are associates and none is associated with \( (x-y) \). Let
and suppose that some \( a_i = 0 \). Then

\[
f(x) - f(y) = (x-y)(b_i y + c_i)g(x, y)
\]

for some \( g(x, y) \in k[x, y] \). Now \( b_i \neq 0 \), otherwise \( g_i \) would not be linear, so on taking \( y = -c_i/b_i \) we have

\[
f(x) = f(-c_i/b_i) = \text{constant},
\]

contradicting \( d \geq 2 \). Hence no \( a_i = 0 \) and similarly no \( b_i = 0 \).

Set \( a = \prod a_i, \quad d_i = b_i/a_i \) and \( e_i = c_i/a_i \) so that

\[
f^*(x, y) = \prod a_i \prod (x + d_i y + e_i) \prod h_i(x, y).
\]

Now let \( N_r \) denote the number of solutions of

\[
f(x_1) = f(x_2) = \ldots = f(x_r)
\]

with \( x_i \neq x_j \) \((i \neq j, 1 \leq i, j \leq r)\). This system has the same number of solutions as the system

\[
f^*(x_1, x_2) = f^*(x_1, x_3) = \ldots = f^*(x_1, x_r) = 0
\]

i.e.,

\[\prod a_i \prod (x_1 + d_i x_2 + e_i) \prod h_j(x_1, x_2) = \ldots \]

\[\prod a_i \prod (x_1 + d_i x_r + e_i) \prod h_j(x_1, x_r) = 0\]

with \( x_i \neq x_j \) \((i \neq j, 2 \leq i, j \leq r)\). Now it is known (see for example \([1]\)) that if \( f(x, y) \in k[x, y] \) is irreducible but not absolutely irreducible then \( f(x, y) = 0 \) has \( O(1) \) solutions. Hence \( N_r \),

587
differs from the number $N'_r$ of solutions, with $x_i \neq x_j$ $(i \neq j, \ 2 \leq i, j \leq r)$, of

$$
\prod_{i=1}^{l} (x_{i_1} + d_i x_{z_i} + e_i) = \ldots = \prod_{i=1}^{l} (x_{i_r} + d_r x_{r_i} + e_r) = 0
$$

by only $O(1)$. Since for any $i$ and $j$ with $i \neq j$, $1 \leq i, j \leq l$

$$x_{i_1} + d_i y + e_i = x_{j_1} + d_j y + e_j = 0$$

has 0 or 1 solutions ($g_i, g_j$ are not associates)

$$N'_r = \sum_{1 \leq i_2, \ldots, i_r \leq l} N(i_2, i_3, \ldots, i_r) + O(1),$$

where $N(i_2, i_3, \ldots, i_r)$ denotes the number of solutions of

$$(2) \quad x_{i_2} + d_{i_2} x_{i_2} + e_{i_2} = \ldots = x_{i_r} + d_{i_r} x_{i_r} + e_{i_r} = 0$$

with $x_i \neq x_j$ $(i \neq j, 2 \leq i, j \leq r)$. Now

$$x_{i_1} + d_{i_1} x_{m_1} + e_{i_1} = x_{i_1} + d_{i_1} x_{n_1} + e_{i_1} = 0$$

with $i_m = i_n$ gives $x_m = x_n$ so

$$N'_r = \sum_{1 \leq i_2, \ldots, i_r \leq l} N(i_2, \ldots, i_r) + O(1).$$

Let $N'(i_2, \ldots, i_r)$ denote the number of solutions of (2) without the conditions $x_i \neq x_j$ $(i \neq j, 2 \leq i, j \leq r)$. As

$$x_{i_k} + d_{i_k} x_{k} + e_{i_k} = 0 \quad (2 \leq k \leq r)$$

588
has one solution $x_k$ for each $x_i$,

$$N'(i_2, i_3, \ldots, i_r) = p.$$ 

Now, as the number of solutions of

$$\begin{cases} 
  x_{i} + d_{i} x_{m} + e_{i} = x_{i} + d_{i} x_{n} + e_{i} = 0 \\
  \frac{x_{m}}{x_{n}} = 1
\end{cases}$$

(where $m \neq n$, $2 \leq m$, $n \leq r$) is 0 or 1,

$$N(i_2, \ldots, i_r) = N'(i_2, \ldots, i_r) + O(1)$$

giving

$$N_r = p \sum_{1 \leq i_2, \ldots, i_r \leq \ell} 1 + O(1)$$

$$= \ell (\ell - 1) \ldots (\ell - (r - 2)) \frac{1}{p} + O(1).$$

Now let $M_r (r = 1, 2, \ldots, d)$ denote the number of $y \in k_p$ for which the equation $f(x) = y$ has precisely $r$ distinct roots in $k$. Then

$$V(f) = \sum_{r=1}^{d} M_r, \quad p = \sum_{r=1}^{d} r M_r,$$

(3)

and

$$N_r = \sum_{s=r}^{d} s(s-1) \ldots (s-(r-1)) M_s (r = 2, 3, \ldots, d).$$

(4)
Thus
\[
\sum_{r=2}^{d} \frac{(-1)^r}{r!} N_r = \sum_{s=2}^{d} \left\{ \sum_{r=2}^{s} \frac{(-1)^r}{r!} s(s - 1) \ldots (s - (r - 1)) \right\} M_s
\]
\[
= \sum_{s=2}^{d} \{ (1 - 1)^s - (1 - s) \} M_s
\]
\[
= \sum_{s=1}^{d} (s-1) M_s
\]
\[
= p - V(f)
\]
so that
\[
V(f) = p - \sum_{r=2}^{d} \frac{(-1)^r}{r!} N_r
\]
\[
= p - p \sum_{r=2}^{d} \frac{(-1)^r}{r!} \ell(\ell - 1) \ldots (\ell - (r - 2)) + O(1)
\]
\[
= p \{ 1 - \sum_{r=2}^{\ell + 1} \frac{(-1)^r}{r!} \ell(\ell - 1) \ldots (\ell - (r - 2)) \} + O(1)
\]
\[
= \frac{p}{\ell + 1} \sum_{r=1}^{\ell + 1} (-1)^{r-1} \binom{\ell + 1}{r} + O(1)
\]
\[
= \frac{p}{\ell + 1} \{ 1 - (1 - 1)^{\ell + 1} \} + O(1)
\]
\[
= \frac{p}{\ell + 1} + O(1)
\]
as required.

**COROLLARY 1.** If \( f(x) \) is extremal of index 0 then \( f \) is quasi-maximal.

**COROLLARY 2.** If \( f(x) \) is extremal of index \( d - 1 \) then \( f \) is quasi-minimal.
We now prove the converses of corollaries 1 and 2.

THEOREM 2. If \( f(x) \) is quasi-maximal then \( f(x) \) is extremal of index 0.

Proof. As \( f(x) \) is quasi-maximal

\[
V(f) = p + O(1).
\]

Set \( M = M_2 + \ldots + M_d \) so that from (3) we have

\[
M_1 + M = p + O(1), \quad M_1 + 2M \leq p.
\]

Eliminating \( M_1 \) we have \( M = O(1) \) so that each \( M_i (i \geq 2) \) is \( O(1) \). Hence \( N_2 = O(1) \). Now if \( f^*(x, y) \) has \( t \) absolutely irreducible factors (linear or non-linear) in \( k[x, y] \) then by a result of Lang and Weil (see for example Lemma 8 in [4]), \( f^*(x, y) = 0 \) has \( tp + O(p^{1/2}) \) solutions. Hence \( t = 0 \) as required.

THEOREM 3. If \( f(x) \) is quasi-minimal then \( f(x) \) is extremal of index \( d - 1 \).

Proof. This was proved by Mordell in [7].

Finally we calculate the number \( V_n(f) \) of residues of an extremal polynomial in the sequence \( 1, 2, \ldots, h \), where \( h \leq p \). (Here we are identifying the elements of \( k \) with the residues \( 1, 2, \ldots, p \mod p \).) We require a lemma.

LEMMA. If \( f(x) \) is an extremal polynomial of index \( \ell \) then, for \( r = 2, \ldots, d \),

\[
\sum_{x_1, \ldots, x_r = 0}^{p-1} e(tf(x_r)) = O(p^{1/2}),
\]

uniformly in \( t \neq 0 \), the implied constant depending only on \( d \). (\( e(u) \) denotes \( \exp(2\pi iu/p) \)).
Proof. From the proof of the estimation of $N_r$ in
Theorem 1 we see that

$$p-1 \sum_{x_1, \ldots, x_r = 0} e(tf(x_r)) = \sum_{1 \leq i, \ldots, i \leq r} \sum_{x_1 + i, x_2 + e_1^i, \ldots, x_r + e^i_r} e(tf(x_r)) + O(1)$$

$$f(x_1) = \ldots = f(x_r)$$

$$= O(\sum_{x_r = 0} e(tf(x_r)))$$

$$= O(p^{1/2})$$

by a deep result of Carlitz and Uchiyama [3].

THEOREM 4. If $f(x)$ is an extremal polynomial of
index $\ell$ the number $V_h(f)$ of residues of $f(x) \pmod{p}$ in the
set $\{1, 2, \ldots, h\}$ is given by

$$\frac{h}{\ell+1} + O(p^{1/2} \log p).$$

Proof. Let $N_r(h)$ ($r = 2, 3, \ldots, d$) denote the number of
solutions of

$$f(x_1) = f(x_2) = \ldots = f(x_r) = y$$

with $y \in \{1, 2, \ldots, h\}$ and $x_i \neq x_j$ ($i \neq j$). Then

$$N_r(h) = \sum_{y=1}^h \sum_{x_1, \ldots, x_r} 1,$$

where the dash (') denotes summation over $x_1, \ldots, x_r$ satisfying

$$x_i \neq x_j (i \neq j)$$

and $f(x_1) = \ldots = f(x_r) = y$. Thus
by the lemma and the familiar result

$$pN_r(h) = \sum_{y=1}^{p} x_1, \ldots, x_r \sum_{z=1}^{p} e(t(y-z))$$

$$= h \sum_{y=1}^{p} x_1, \ldots, x_r \sum_{t=1}^{p-1} \left\{ \sum_{y=1}^{p} x_1, \ldots, x_r e(ty) \right\}$$

$$\times \left\{ \sum_{z=1}^{h} (-tz) \right\}$$

$$= hN_r + O(p^{1/2} \cdot p \log p),$$

by the lemma and the familiar result

$$\sum_{t=1}^{p-1} h \sum_{z=1}^{p} e(-tz) \leq p \log p.$$ 

Hence appealing to Theorem 1 we obtain

$$N_r(h) = \ell(\ell - 1) \ldots (\ell - (r - 2)) h + O(p^{1/2} \log p).$$

Now if $M_r(h)$ denotes the number of $y \in \{1, 2, \ldots, h\}$ for which the equation $f(x) = y$ has precisely $r$ distinct roots in $k_p$, we have

$$V_h(f) = \sum_{r=1}^{d} M_r(h)$$

and

$$\sum_{r=1}^{d} rM_r(h) = h + O(p^{1/2} \log p).$$

The first of these is obvious and the second is due to Mordell [8].
Corresponding to (4) we have

$$N_r(h) = \sum_{s=r}^{d} s(s-1) \ldots (s - (r-1))M_s(h)$$

593
and the rest of the proof is the same as in Theorem 1 with $V_h(f)$, $M_r(h)$, $N_r(h)$, $h$ replacing $V(f)$, $M_r$, $N_r$, $r$ respectively. This proves a conjecture of the author [9] in the case of extremal polynomials. When the index $\ell$ is $\geq 1$ it shows that the least positive non-residue of $f(x) \pmod{p}$ is $O(p^{1/2} \log p)$. This has been proved for more general polynomials, without obtaining an asymptotic formula for $V_h(f)$, by Bombieri and Davenport [2], using the recent work of Bombieri on the $L$-functions corresponding to multiple exponential sums.

REFERENCES


Carleton University, Ottawa