IRREDUCIBILITY OF POLYNOMIALS WITH LOW ABSOLUTE VALUES

BY
R. J. LEVIT

1. **Introduction.** We shall be concerned with irreducibility criteria of the following form: *An integral polynomial* (i.e., polynomial with integral coefficients) $P_n(x)$ *of degree n is irreducible over the rational field if there are m distinct integers* $x_1, x_2, \ldots, x_m$ *for which* $0 < |P_n(x_i)| < \Gamma(m, n)$, *where* $\Gamma(m, n)$ *is a specified function of m and n only*. The first such criterion was given by G. Pólya [4] for $m=n$. In a comprehensive paper [1], which includes an account of the earlier results, A. Brauer and G. Ehrlich established the highest bounds $\Gamma(m, n)$ to date—namely,

$$\Gamma(n, n) = G(n) = \frac{(n-1)!}{2^{n-1}[(n-2)/2]!}, \tag{1-1a}$$

$$\Gamma(m, n) = [(m+1)/2] \qquad (n/2 < m \leqq n-1, m \geqq 7). \tag{1-1b}$$

They showed that the bound (1-1b) is the best possible and went on to consider the effect of excluding polynomials with factors of certain degrees. In particular, their bound for polynomials without rational zeros is

$$\Gamma(m, n) = [(m-1)/2](m-1)/4 \qquad (n/2 < m \leqq n-1). \tag{1-2}$$

In the present paper we improve the values of $\Gamma(m, n)$ in (1-1a) and (1-2) by utilizing a lower bound derived in [2] for the maximum absolute value of a polynomial on a finite set. For $m=n$ and $m=n-1$ we obtain

$$\Gamma(n, n) = B_n = 2^{1-N}(\tfrac{1}{2}[n/2])_N; \quad \Gamma(n-1, n) = B_n' = 2^{1-N}(\{[n/2]-1\}/2)_N,$$

where $N=[(n+1)/2]$ and $(x)_i$ denotes the factorial,

$$(x)_i = x(x+1)\cdots(x+i-1) \qquad (i = 1, 2, \ldots).$$

$B_n > G(n)$ when $n>5$. B_n' exceeds the bound (1-2) (for $m=n-1$) when $n>7$. For $n/2<m\leqq n-2$, Theorem 4 below yields a bound which coincides with (1-2) for odd m but is slightly higher for even $m>6$. This bound is the best possible for polynomials without rational zeros.

In the concluding section we determine the forms of the polynomials covered by the various criteria.

Presented to the Society, April 2, 1949 under the title *A criterion for the irreducibility of polynomials in the rational field* and November 30, 1967; received by the editors January 4, 1967.

(1) For any real number x, $[x]$ denotes the greatest integer $\leqq x$.

2. **The values of a monic polynomial on a finite set.** In this section the coefficient domain for all polynomials is understood to be the real field. We need the following result from another paper [2, Corollary 4].

LEMMA 1-1. *Let $c_1 < c_2 < \cdots < c_n$ be real numbers, $d = \max_i (c_{i+1} - c_i)$, $L = c_n - c_1$; and let $q_k(x)$ be a monic polynomial of degree $k > 0$. If $L > d(k-1)$,*

$$\max_{i=1,2,\ldots,n} |q_k(c_i)| \geqq 2^{1-2k} \prod_{i=1}^{k} \{L + d(2i - k - 1)\}. \tag{2-1}$$

This leads to a theorem which is the basis of the irreducibility criteria.

THEOREM 1. *Let $x_1 < x_2 < \cdots < x_n$ be integers, and let $q_k(x)$ be a monic polynomial of degree k. If $n > k > 0$, then*

$$\max_{i=1,2,\ldots,n} |q_k(x_i)| \geqq B(k, n) = 2^{1-k} \left(\frac{n-k}{2}\right)_k. \tag{2-2}$$

For the proof we need, in addition to Lemma 1-1, some results of de la Vallée Poussin [5, Chapter VI] concerning Tchebichef approximation on finite sets. Given an arbitrary real function f defined at the points $c_1 < c_2 < \cdots < c_n$ $(n > 1)$ and a positive integer $m \leqq n-2$, there is a unique polynomial $p_m^*(x) = p_m^*(x; c_1, \ldots, c_n)$ such that, as $p_m(x)$ ranges over the set of all polynomials of degree $\leqq m$, the deviation, $\max_i |f(c_i) - p_m(c_i)|$, assumes its minimum value $\rho_{f,m}(c_1, \ldots, c_n)$ when $p_m(x) = p_m^*(x)$. That is,

$$\max_{i=1,2,\ldots,n} |f(c_i) - p_m(c_i)| \geqq \max_{i=1,2,\ldots,n} |f(c_i) - p_m^*(c_i)| = \rho_{f,m}(c_1, \ldots, c_n). \tag{2-3}$$

With the aid of the definition,

$$\omega_i(c_1, \ldots, c_n) = |c_i - c_1| \cdots |c_i - c_{i-1}|\, |c_i - c_{i+1}| \cdots |c_i - c_n|,$$

$\rho_{f,n-2}(c_1, \ldots, c_n)$ can be expressed explicitly by the formula,

$$\rho_{f,n-2}(c_1, \ldots, c_n) = \frac{\left| \sum_{i=1}^{n} (-1)^i f(c_i)/\omega_i(c_1, \ldots, c_n) \right|}{\sum_{i=1}^{n} 1/\omega_i(c_1, \ldots, c_n)} \tag{2-4}$$

while for $m < n-2$

$$\rho_{f,m}(c_1, \ldots, c_n) = \rho_{f,m}(c_{I_1}, c_{I_2}, \ldots, c_{I_{m+2}}), \tag{2-5}$$

where $I_1, I_2, \ldots, I_{m+2}$ are distinct integers from among $1, 2, \ldots, n$ chosen so that the right member is a maximum.

Proofs of the foregoing are given in [5, Chapter 6]. We apply them now to the function $f(x) = x^k$, $k < n$. The numerator in (2-4) is $|[c_1, c_2, \ldots, c_n]_f|$, where $[c_1, \ldots, c_n]_f$ is the divided difference of order $n-1$ for the function f. (The required properties of divided differences may be found in [3].) For $f(x) = x^{n-1}$,

$[c_1, \ldots, c_n]_f = 1$. Consequently, if we write ρ_k for $\rho_{f,k-1}$ when $f(x) = x^k$, (2-4) reduces to

$$\rho_{n-1}(c_1, \ldots, c_n) = \frac{1}{\sum_{i=1}^{n} 1/\omega_i(c_1, \ldots, c_n)}. \tag{2-6}$$

LEMMA 1-2. *Let $q_k(x)$ be a monic polynomial of degree $k > 0$, and let $c_1 < c_2 < \cdots < c_n$ be real numbers, $n > k$. Then,*

$$\max_{i=1,2,\ldots,n} |q_k(c_i)| \geqq \rho_k(c_{I_1}, c_{I_2}, \ldots, c_{I_{k+1}}), \tag{2-6.5}$$

where $I_1, I_2, \ldots, I_{k+1}$ are distinct integers from among $1, 2, \ldots, n$ chosen so that the right member is a maximum. There is a unique polynomial $q_k^*(x) = q_k^*(x; c_1, \ldots, c_n)$ such that equality holds in (2-6.5).

Proof. Set $p_{k-1}(x) = x^k - q_k(x)$. Then by (2-3), (2-5),

$$\max_{i=1,2,\ldots,n} |q_k(c_i)| = \max_{i=1,2,\ldots,n} |c_i^k - p_{k-1}(c_i)| \geqq \max_{i=1,2,\ldots,n} |c_i^k - p_{k-1}^*(c_i)|$$
$$= \rho_k(c_1, \ldots, c_n) = \rho_k(c_{I_1}, c_{I_2}, \ldots, c_{I_{k+1}}).$$

Equality holds only for the polynomial $q_k^*(x) = x^k - p_{k-1}^*(x)$.

The case $n = k+1$ leads to the following result of Pólya [4, p. 32].

$$\max_{i=1,2,\ldots,k+1} |p_k(x_i)| \geqq \frac{k!}{2^k}, \tag{2-7}$$

where $p_k(x)$ is an integral polynomial of exact degree k and $x_1, x_2, \ldots, x_{k+1}$ are any $k+1$ distinct integers.

LEMMA 1-3. *Let $c_1 < c_2 < \cdots < c_n$ and $e_1 < e_2 < \cdots < e_n$ be real numbers such that*

$$e_{i+1} - e_i \geqq c_{i+1} - c_i \qquad (i = 1, 2, \ldots, n-1). \tag{2-8}$$

If $i_1, i_2, \ldots, i_{k+1}$ are any $k+1$ distinct integers from among $1, 2, \ldots, n$, then

$$\rho_k(e_{i_1}, e_{i_2}, \ldots, e_{i_{k+1}}) \geqq \rho_k(c_{i_1}, c_{i_2}, \ldots, c_{i_{k+1}}). \tag{2-9}$$

Moreover, for any monic polynomial $q_k(x)$ of degree k,

$$\max_{i=1,2,\ldots,n} |q_k(e_i)| \geqq \max_{i=1,2,\ldots,n} |q_k^*(c_i; c_1, \ldots, c_n)|. \tag{2-10}$$

Proof. (2-8) implies that $e_j - e_i \geqq c_j - c_i$ for $1 \leqq i < j \leqq n$. Hence, $\omega_i(e_1, \ldots, e_n) \geqq \omega_i(c_1, \ldots, c_n)$ and (2-9) follows by (2-6). Next, from among $1, 2, \ldots, n$ choose two sets of $k+1$ distinct integers, $I_1, I_2, \ldots, I_{k+1}$ and $J_1, J_2, \ldots, J_{k+1}$, which respectively maximize

$$\rho_k(c_{I_1}, c_{I_2}, \ldots, c_{I_{k+1}}) \quad \text{and} \quad \rho_k(e_{J_1}, e_{J_2}, \ldots, e_{J_{k+1}}).$$

Then,

$$\begin{aligned}\max_{i=1,2,\ldots,n} |q_k(e_i)| &\geqq \rho_k(e_{J_1}, e_{J_2}, \ldots, e_{J_{k+1}}) \geqq \rho_k(e_{I_1}, e_{I_2}, \ldots, e_{I_{k+1}}) \\ &\geqq \rho_k(c_{I_1}, c_{I_2}, \ldots, c_{I_{k+1}}) = \max_{i=1,2,\ldots,n} |q_k^*(c_i; c_1, \ldots, c_n)|\end{aligned}$$

by Lemma 1-2, (2-9), and Lemma 1-2 again.

We are now ready to prove Theorem 1. Since the x_i are integers, (2-8) is satisfied if we take $e_i = x_i$, $c_i = i$. By Lemmas 1-3 and 1-1 we have

$$\max_{i=1,2,\ldots,n} |q_k(x_i)| \geqq \max_{i=1,2,\ldots,n} |q_k^*(i)| \geqq 2^{1-2k} \prod_{i=1}^{k} (n-k+2i-2) = 2^{1-k} \left(\frac{n-k}{2}\right)_k.$$

3. Irreducibility criteria.

THEOREM 2. *Let $P_n(x)$ be an integral polynomial of exact degree n, and let $N = [(n+1)/2]$. If there are n integers, $x_1 < x_2 < \cdots < x_n$ such that*

(3-1) $$0 < |P_n(x_i)| < B_n = 2^{1-N}(\tfrac{1}{2}[n/2])_N \qquad (i = 1, 2, \ldots, n),$$

then $P_n(x)$ is irreducible over the field of rational numbers.

Proof. Since, for $n \leqq 4$, $B_n \leqq 1$ and (3-1) is vacuous, we assume $n \geqq 5$. It will be convenient to prove the following lemma.

LEMMA 2. *Let $x_1 < x_2 < \cdots < x_n$ be integers, $n \geqq 5$, and let $p_k(x)$ be an integral polynomial of exact degree k, $n/2 \leqq k \leqq n-1$. Then*

(3-2) $$\max_{i=1,2,\ldots,n} |p_k(x_i)| \geqq B_n.$$

The proof of the theorem will then follow immediately; for, if $P_n(x)$ were reducible, there would be a factorization, $P_n(x) = p_k(x)\pi(x)$, in which $p_k(x)$ and $\pi(x)$ are integral polynomials and $p_k(x)$ has leading coefficient $a \neq 0$ and degree k in the range, $n/2 \leqq k \leqq n-1$. $\pi(x_i)$ is an integer and is not zero, since $P_n(x_i) \neq 0$. Hence, $|\pi(x_i)| \geqq 1$, and so by the lemma

$$\max_{i=1,2,\ldots,n} |P_n(x_i)| \geqq \max_{i=1,2,\ldots,n} |p_k(x_i)| \geqq B_n,$$

contrary to (3-1). Therefore, $P_n(x)$ cannot be reducible.

We turn now to the proof of the lemma. For $B(k, n)$ as defined in (2-2), $B_n = B(N, n)$. We wish to show that for $n \geqq 8$

(3-3) $$B(k, n) \geqq B(N, n) \qquad (k = N, N+1, \ldots, n-1).$$

We find directly that

$$\frac{B(k+2, n)}{B(k, n)} = \frac{(n-1)^2 - (k+1)^2}{16}$$

and hence that

(3-4) $$B(k+2, n) > B(k, n) \qquad (k \leqq n-3, n \geqq 10).$$

It is also readily shown that

$$B(k+1, n)/B(k, n) > (n-k-1)/4$$

and hence that $B(k+1, n) > B(k, n)$ when $k \leqq n-5$. But $N \leqq n-5$ for $n \geqq 10$; so

$$B(N+1, n) > B(N, n) \qquad (n \geqq 10). \tag{3-5}$$

Combining (3-4) and (3-5), we see that (3-3) holds for $n \geqq 10$. It continues to hold for $n=9, 8$, as can be verified by direct evaluation of $B(k, n)$ for each k concerned. Now let $q_k(x) = p_k(x)/a$. Then, since $|a| \geqq 1$, we have

$$\max_{i=1,2,\ldots,n} |p_k(x_i)| = |a| \max_{i=1,2,\ldots,n} |q_k(x_i)| \geqq B(k, n) \geqq B(N, n) = B_n \tag{3-6}$$

for $n/2 \leqq k \leqq n-1$, $n \geqq 8$, by Theorem 1 and (3-3). This establishes (3-2) for $n \geqq 8$ and also, when $k=N$, for $n=7, 6, 5$. We verify it for each value of k individually in the remaining cases as follows.

$n=7, k=5$: $\max_{i=1,2,\ldots,7} |p_5(x_i)| \geqq B(5, 7) = \frac{15}{2} > B_7$ by Theorem 1.

$n=7, k=6$: $\max_{i=1,2,\ldots,7} |p_6(x_i)| \geqq \frac{6!}{2^6} > B_7$ by (2-7).

$n=6, k=4$: $\max_{i=1,2,\ldots,6} |p_4(x_i)| \geqq \rho_4(x_1, x_2, x_4, x_5, x_6) \geqq \rho_4(1, 2, 4, 5, 6) = 4 > B_6$ by Lemmas 1-2, 1-3, and (2-6).

$n=6, k=5$: $\max_{i=1,2,\ldots,6} |p_5(x_i)| \geqq \frac{5!}{2^5} > B_6$ by (2-7).

$n=5, k=4$: $\max_{i=1,2,3,4,5} |p_4(x_i)| \geqq \frac{4!}{2^4} = B_5$ by (2-7).

This completes the proof of Lemma 2 and hence of Theorem 2.

Comparing B_n with the bound $G(n)$ in (1-1a), we find that

$$\frac{B_n}{G(n)} = \prod_{i=0}^{N-1} \frac{N+2i}{N+i} \quad (n \text{ even}); \qquad \frac{B_n}{G(n)} = \frac{1}{2} \prod_{i=0}^{N-1} \frac{N+2i-1}{N+i-1}$$

$$= \frac{3(3N-5)}{4(2N-3)} \prod_{i=0}^{N-3} \frac{N+2i-1}{N+i-1} \quad (n \text{ odd}).$$

Thus, $B_n > G(n)$ for even n and for odd $n \geqq 7$. $B_5 = G(5) = \frac{3}{2}$, while, for $n<5$, $B_n \leqq 1$, $G(n) < 1$, so that the theorem is vacuous with either bound.

If $P_n(x)$ has no rational zeros, we can restrict the degree of its factor $p_k(x)$ to the range, $N \leqq k \leqq n-2$; and, by slightly modifying the proof of Theorem 2, obtain the following criterion requiring only $n-1$ points.

THEOREM 3. *Let $P_n(x)$ be an integral polynomial of exact degree n having no rational zeros. If there are $n-1$ integers, $x_1 < x_2 < \cdots < x_{n-1}$, such that*

(3-7) $$0 < |P_n(x_i)| < B(N, n-1) = 2^{1-N}(\{[n/2]-1\}/2)_N \qquad (i = 1, 2, \ldots, n-1),$$

where $N=[(n+1)/2]$, *then* $P_n(x)$ *is irreducible over the field of rationals.*

For fewer than $n-1$ points (but more than $n/2$) we have

THEOREM 4. *Let* $P_n(x)$ *be an integral polynomial of exact degree n having no rational zeros, and let m be an integer in the range,* $n/2<m\leqq n-2$. *If there are m integers,* $x_1<x_2<\cdots<x_m$, *such that*

(3-8) $$0 < |P_n(x_i)| < A_m = [\{(m-1)^2+4\}/8] \qquad (i = 1, 2, \ldots, m),$$

then $P_n(x)$ *is irreducible over the field of rationals. Moreover, if*

(3-9) $$0 < |P_n(x_i)| < A_m+1 \qquad (i = 1, 2, \ldots, m),$$

$P_n(x)$ *is irreducible when m satisfies the following condition*:

CONDITION U. $u=m-1$ *is a solution of the Pell-type equation,* $u^2-2v^2=-1$, *for some integer v.*

Proof. We assume $m\geqq 5$, since for lower values the theorem is vacuous. If $P_n(x)$ were reducible, it would have a factor $\pi_k(x)$ with integral coefficients and degree k in the range, $2\leqq k\leqq n/2$. We shall show that

(3-10) $$\max_{i=1,2,\ldots,m} |\pi_k(x_i)| \geqq A_m \qquad (k = 2, 3, \ldots, [n/2])$$

and that, when m satisfies Condition U, (3-10) is a strict inequality. The theorem then follows as in the proof of Theorem 2 from Lemma 2. Let $\pi_k(x)$ have leading coefficient a, and let $q_k(x)=\pi_k(x)/a$. Consider first the case $k=2$ of (3-10). Defining $M=[(m+1)/2]$, we have by Lemmas 1-2, 1-3

(3-11) $$\max_{i=1,2,\ldots,m} |\pi_2(x_i)| \geqq \max_{i=1,M,m} |q_2(x_i)| \geqq \rho_2(x_1, x_M, x_m) \geqq \rho_2(0, M-1, m-1).$$

In fact, since $\pi_2(x_i)$ is an integer, $\max_i |\pi_2(x_i)|\geqq[\rho_2(0, M-1, m-1)]^*$, where $[r]^*$ denotes the least integer $\geqq r$. By means of (2-6) we find that

(3-12) $$\begin{aligned} \rho_2(0, M-1, m-1) &= (m-1)^2/8 \quad (m \text{ odd}),\\ \rho_2(0, M-1, m-1) &= m(m-2)/8 \quad (m \text{ even}),\end{aligned}$$

and hence that $[\rho_2(0, M-1, m-1)]^*\geqq A_m$. Thus, (3-10) is established for $k=2$.

For $k>2$, since $m>n/2\geqq k$, we have by Theorem 1

(3-13) $$\max_{i=1,2,\ldots,m} |\pi_k(x_i)| = |a| \max_{i=1,2,\ldots,m} |q_k(x_i)| \geqq B(k, m).$$

This implies (3-10) as a strict inequality for $3\leqq k<m$, $m\geqq 7$, because

$$\frac{B(k, m)}{A_m} \geqq 4^{2-k}\prod_{i=0}^{k-3} (2i+m-k),$$

and the right member exceeds one for $3 \leqq k < m-4$ as well as for $k = m-4$, $m-3$, $m-2$ when $m \geqq 8$ and for $k = m-1$ when $m \geqq 9$. Direct computation shows that $B(k, m) > A_m$ in all other cases in which $m \geqq 7$. For $m = 6, 5$ (which do not satisfy Condition U) (3-10) continues to hold (though not necessarily strictly). This is proved by treating each value of k individually as in Lemma 2.

Suppose now that m does satisfy Condition U but that equality holds in (3-10). This is possible only for $k = 2$, as we have just seen. m is even, since $(m-1)^2 = 2v^2 - 1$ for some integer v. By (3-11) and (3-12)

$$\max_{i=1,M,m} |q_2(x_i)| = \rho_2(0, M-1, m-1) = m(m-2)/8 \tag{3-14}$$

and

$$\rho_2(x_1, x_M, x_m) = \rho_2(0, M-1, m-1). \tag{3-15}$$

By (2-6) we see that, since the x_i are integers, (3-15) can hold only if $x_i = x_1 + i - 1$ $(i = 1, 2, \ldots, m)$. Then we note that (3-14) is satisfied by

$$q_2(x) = (x-x_1)^2 - (m-1)(x-x_1) + m(m-2)/8, \tag{3-16}$$

and by Lemma 1-2 this is the only monic quadratic polynomial satisfying (3-14). Its discriminant is $D_m = \{(m-1)^2+1\}/2 = v^2$. Therefore, $q_2(x)$ and hence $P_n(x)$ have rational zeros, contrary to hypothesis. Thus, when m satisfies Condition U, equality cannot hold in (3-10). We then have $\max_i |P_n(x_i)| \geqq \max_i |\pi_k(x_i)| \geqq A_m + 1$. Since this contradicts (3-9), $P_n(x)$ cannot be reducible. This completes the proof.

The bounds in Theorem 4 cannot be improved. If in place of (3-8)

$$0 < |P_n(x_i)| \leqq A_m \qquad (i = 1, 2, \ldots, m) \tag{3-17}$$

when m does not satisfy Condition U; or in place of (3-9)

$$0 < |P_n(x_i)| \leqq A_m + 1 \qquad (i = 1, 2, \ldots, m), \tag{3-18}$$

when m does satisfy Condition U, then $P_n(x)$ may be reducible. To show this, let $Q(x) = x^2 - (m-1)x + A_m$ and $R(x) = 1 + x^{(m)}\phi_{n-m-2}(x)$, where $x^{(m)}$ is the descending factorial, $x^{(m)} = x(x-1)\ldots(x-m+1)$, and $\phi_{n-m-2}(x)$ is an arbitrary monic integral polynomial of the degree indicated by the subscript. For $i = 1, 2, \ldots, m$, $|Q(i-1)| \leqq A_m$ while $R(i-1) = 1$. Consequently, (3-17) is satisfied for $x_i = i-1$ by the reducible polynomial,

$$P_n(x) = Q(x)R(x). \tag{3-19}$$

$R(x)$ has no rational zeros, since its leading and constant coefficients are both one, and $R(\pm 1) \neq 0$. Hence, the polynomial (3-19) has a rational zero if and only if the discriminant D_m of $Q(x)$ is a square. Now, $D_m = \{(m-1)^2 - s\}/2$, where $s = 0$ when $m \equiv 1 \pmod 4$, $s = 4$ when $m \equiv 3 \pmod 4$, and $s = -1$ when m is even. Consequently, when $m \equiv 1 \pmod 4$, D_m is never a square. In the other two cases, if D_m is a square, we use instead of (3-19)

$$P_n(x) = (Q(x)-1)R(x), \tag{3-20}$$

which has no rational zeros, since D_m and the discriminant of the polynomial $Q(x)-1$ cannot both be squares. When $m\equiv 3 \pmod 4$, $|Q(i-1)-1|\leqq A_m$ $(i=1, 2, \ldots, m)$; so (3-20) satisfies (3-17) with $x_i=i-1$. When m is even, D_m is a square if and only if m satisfies Condition U. In that case, (3-20) satisfies (3-18) with $x_i=i-1$, since, for m even, $|Q(i-1)-1|\leqq A_m+1$ $(i=1, 2, \ldots, m)$.

4. **Characterization of polynomials meeting the criteria.**

THEOREM 5. *Let a and $x_1<x_2<\cdots<x_n$ be integers, and let $g_k(x)$ be an integral polynomial of degree $k<n/2$ such that*

$$\text{(4-1)} \qquad 0 < |g_k(x_i)| < B_n = 2^{1-N}(\tfrac{1}{2}[n/2])_N \qquad (i = 1, 2, \ldots, n),$$

where $N=[(n+1)/2]$. Then the polynomial,

$$\text{(4-2)} \qquad P_n^*(x) = a(x-x_1)(x-x_2)\cdots(x-x_n)+g_k(x),$$

is irreducible over the rational field; and every polynomial $P_n(x)$ meeting the criterion (3-1) *has this form.*

Proof. Since $P_n^*(x_i)=g_k(x_i)$ for $i=1, 2, \ldots, n$, (4-1) implies that $P_n^*(x)$ satisfies (3-1) and hence is irreducible by Theorem 2. Conversely, let $P_n(x)$ be an integral polynomial of degree n having leading coefficient a and satisfying (3-1). Dividing $P_n(x)$ by $\pi_n(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$, we obtain $P_n(x)=a\pi_n(x)+g_k(x)$, where $g_k(x)$ is an integral polynomial of degree $k<n$. Then $g_k(x_i)=P_n(x_i)$ for $i=1, 2, \ldots, n$; so (4-1) follows from (3-1). Moreover, $k<n/2$; for, if $k\geqq n/2$, we would have by Lemma 2 $\max_{i=1,\ldots,n} |g_k(x_i)|\geqq B_n$, contrary to (4-1).

In particular, the polynomial $a(x-x_1)(x-x_2)\cdots(x-x_n)+t$ is irreducible if t is an integer such that $1\leqq|t|<B_n$. Various special cases of this result are well-known. (References are given in [1].)

Similar considerations in connection with Theorems 4 and 5 respectively yield

COROLLARY 5-1. *Let a, b and $x_1<x_2<\cdots<x_{n-1}$ be integers, $a\neq 0$, and let $g_k(x)$ be an integral polynomial of degree $k<n/2$ such that*

$$0 < g_k(x_i) < B(N, n-1) = 2^{1-N}(\{[n/2]-1\}/2)_N \qquad (i = 1, 2, \ldots, n-1).$$

If the polynomial,

$$(ax+b)(x-x_1)(x-x_2)\cdots(x-x_{n-1})+g_k(x),$$

has no rational zero, it is irreducible over the rational field; and every polynomial $P_n(x)$ meeting the criterion (3-7) *has this form.*

COROLLARY 5-2. *Let a, b and $x_1<x_2<\cdots<x_m$ be integers such that*

$$0 < |ax_i+b| < A_m = [\{(m-1)^2+4\}/8] \qquad (i = 1, 2, \ldots, m)$$

when m does not satisfy Condition U, *and*

$$0 < |ax_i+b| < A_m+1 \qquad (i = 1, 2, \ldots, m)$$

when m does satisfy Condition U. *Let* $h_j(x)$ *be an integral polynomial of degree* j, $2 \leqq j < m$. *If the polynomial,*

$$(x-x_1)(x-x_2)\cdots(x-x_m)h_j(x)+ax+b,$$

has no rational zero, it is irreducible over the rational field; and every polynomial $P_n(x)$ *meeting the criterion* (3-8) *or* (3-9) *has this form with* $j=n-m$.

References

1. A. Brauer and G. Ehrlich, *On the irreducibility of certain polynomials*, Bull. Amer. Math. Soc. **52** (1946), 844–856.

2. R. J. Levit, *A variant of Tchebichef's minimax problem*, Proc. Amer. Math. Soc. **18** (1967), 925–932.

3. L. M. Milne-Thomson, *The calculus of finite differences*, Macmillan, London, 1933, Chapter I.

4. G. Pólya, *Verschiedene Bemerkungen zur Zahlentheorie*, Jber. Deutsch. Math.-Verein. **28** (1919), 31–40.

5. C. de la Vallée Poussin, *Leçons sur l'approximation des fonctions d'une variable réelle*, Gauthier-Villars, Paris, 1919.

San Francisco State College,
San Francisco, California