ON THE IRREDUCIBILITY OF CERTAIN POLYNOMIALS

ALFRED BRAUER AND GERTRUDE EHRLICH

Introduction. G. Pólya[1] has proved the following theorem:

If for n integral values of x, the integral polynomial $P(x)$ of degree n has values which are different from zero and, without regard to sign, less than

$$G_1 = \frac{(n - [n/2])!}{2^{n-[n/2]}},$$

then $P(x)$ is irreducible in the field of rational numbers. (Here, as in the following, a polynomial with rational integral coefficients is called an "integral polynomial.")

This result was improved for positively definite polynomials by Hildegard Ille[2] and for arbitrary polynomials by T. Tatuzawa.[3] The latter obtained the larger bound

$$G_2 = (2^{-n}(n - 1)!)^{1/2}$$

instead of G_1. Moreover he proved the following theorem:

If for l integral values of x where $n > l > n/2$, the integral polynomial $P(x)$ of degree n takes values which are different from zero and, without regard to sign, less than

$$H_1 = (l - 1)!^{1/l}/2,$$

then $P(x)$ is irreducible in the field of rational numbers.

In the following, the results of Tatuzawa will be improved further by a slight modification of his method. Instead of G_2 we obtain the larger bound

$$G = \frac{(n - 1)!}{2^{n-1}[(n - 2)/2]!}.$$

We have

$$\frac{G}{G_2} \sim \left(\frac{2n}{\pi}\right)^{1/4} \quad \text{for even } n \text{ and} \quad \frac{G}{G_2} \sim \left(\frac{n^3}{2\pi}\right)^{1/4} \quad \text{for odd } n.$$

Presented to the Society, April 27, 1946; received by the editors November 12, 1945.

[1] *Verschiedene Bemerkungen zur Zahlentheorie*, Jber. Deutschen Math. Verein. vol. 28 (1919) pp. 31–40.

[2] *Einige Bemerkungen zu einem von G. Pólya herrührenden Irreduzibilitätskriterium*, Jber. Deutschen Math. Verein. vol. 35 (1926) pp. 204–208.

[3] *Über die Irreduzibilität gewisser ganzzahliger Polynome*, Proc. Imp. Acad. Tokyo vol. 15 (1939) pp. 253–254.

It follows from this theorem in particular that the integral polynomials

$$P(x) = A(x - x_1)(x - x_2) \cdots (x - x_n) + t$$

are irreducible if $x_\mu \neq x_\nu$ and $1 \leqq |t| < G$. This result contains for $n > 4$, $A = 1$, and $t = \pm 1$ a theorem of I. Schur,[4] and for arbitrary A and $t = \pm 1$ a theorem of H. L. Dorwart and O. Ore.[5] For $n \leqq 4$ there are exceptions.[6] The application of Pólya's bound gives this result only for $n > 6$, that of Tatuzawa for $n > 5$, while our bound gives the exact degrees for which these theorems hold.

Moreover, we improve the second theorem of Tatuzawa. Instead of H_1 we obtain the larger bound

$$H = \left[\frac{l+1}{2}\right] \quad \text{for} \quad l \geqq 7, \qquad H = \frac{3}{2} \quad \text{for} \quad l = 6 \text{ and } 5.$$

It is of interest that this bound cannot be improved further. If the absolute value of $P(x_\lambda)$ for $\lambda = 1, 2, \cdots, 1$ is not less than H, but only less than or equal to H, then our result does not remain correct. It will be shown that for every $n > 2$ such polynomials exist which are reducible in the field of rational numbers.

It follows from our theorem that the integral polynomials of degree n

$$P(x) = (x - x_1)(x - x_2) \cdots (x - x_l)h(x) + t$$

are irreducible if $l > 4$, $n > l > n/2$, $x_\lambda \neq x_\mu$, and $1 \leqq |t| < H$. This gives for $t = \pm 1$ a theorem of Dorwart and Ore.[7]

Finally a criterion of a new type is obtained. $P(x)$ is irreducible if the absolute value of $P(x_\nu)$ is different from zero and less than a certain bound $S_1 > G$ for n different integers x_ν, but less than another smaller constant S_2 for l of these x_ν. More exactly, the following theorem is proved.

Let $P(x)$ be an integral polynomial of degree n; let k, l, and h be integers satisfying the following conditions: $k \geqq [(n+1)/2]$, $n > l > n/2$, $l > 12$ or $l = 11$ or 9,

$$l > h, \qquad n \geqq k + h - 1.$$

[4] Aufgabe 226, Archiv der Mathematik und Physik (3) vol. 13 (1908) p. 367. Lösung by W. Flügel, ibid. vol. 15 (1909) pp. 271–272. Cf. G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, vol. 2, Berlin, 1925, pp. 136, 346–347.

[5] *Criteria for the irreducibility of polynomials*, Ann. of Math. vol. 34 (1933) pp. 81–94, 195.

[6] See, for instance, loc. cit. footnote 5, pp. 86, 195.

[7] Loc. cit. footnote 5.

If for n different integers $x_1, x_2, \cdots, x_n$

$$0 < |P(x_\nu)| < 2^{-k}\prod_{\kappa=1}^{k}\left[\frac{\kappa n - 1}{k}\right] \qquad (\nu = 1, 2, \cdots, n),$$

and for l of these x_ν, say $x^{(1)}, x^{(2)}, \cdots, x^{(l)}$

$$|P(x^{(\lambda)})| < 2^{-h}\prod_{\mu=1}^{h}\left[\frac{\mu l - 1}{h}\right] \qquad (\lambda = 1, 2, \cdots, l),$$

then $P(x)$ is irreducible in the field of rational numbers.

1. Bounds for the absolute value of polynomials at given points. We first prove the following theorem of Tatuzawa.

THEOREM 1. *Let $f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k$ be a polynomial of degree k, let $x_1 < x_2 < \cdots < x_{k+1}$ be arbitrary numbers, and d_κ the length of the smallest interval which contains $\kappa+1$ of these numbers ($\kappa = 1, 2, \cdots, k$). Then*

$$\max_{\kappa=1,2,\cdots,k+1} |f(x_\kappa)| \geqq 2^{-k}|a_0| d_1d_2\cdots d_k.$$

PROOF. For $k=1$ we have

$$|f(x_1) - f(x_2)| = |a_0(x_1 - x_2)| = |a_0| d_1,$$

hence

$$\max\{|f(x_1)|, |f(x_2)|\} \geqq 2^{-1}\{|f(x_1)| + |f(x_2)|\}$$
$$\geqq 2^{-1}|f(x_1) - f(x_2)| = 2^{-1}|a_0| d_1.$$

This proves the theorem for $k=1$. Let us now assume that it is already proved for polynomials of degree less than k.

We divide $f(x)$ by the polynomials $(x-x_1)(x-x_2)\cdots(x-x_k)$ and $(x-x_2)(x-x_3)\cdots(x-x_{k+1})$, respectively. Then

$$\begin{aligned} f(x) &= a_0(x - x_1)(x - x_2)\cdots(x - x_k) + g(x) \\ &= a_0(x - x_2)(x - x_3)\cdots(x - x_{k+1}) + h(x) \end{aligned} \tag{1}$$

where $g(x)$ and $h(x)$ are polynomials of degree less than k with the highest coefficients

$$b_0 = a_1 + a_0(x_1 + x_2 + \cdots + x_k)$$

and

$$c_0 = a_1 + a_0(x_2 + x_3 + \cdots + x_{k+1}),$$

respectively, hence $b_0 - c_0 = a_0(x_1 - x_{k+1})$,

$$\begin{aligned} \max(|b_0|, |c_0|) &\geqq 2^{-1}(|b_0| + |c_0|) \\ &\geqq 2^{-1}|b_0 - c_0| = 2^{-1}|a_0| d_k. \end{aligned} \tag{2}$$

On the other hand it follows from (1) that

$$\begin{aligned} \max_{\kappa=1,2,\cdots,k+1} |f(x_\kappa)| &\geqq \max_{\kappa=1,2,\cdots,k} |g(x_\kappa)|, \\ \max_{\kappa=1,2,\cdots,k+1} |f(x_\kappa)| &\geqq \max_{\kappa=2,3,\cdots,k+1} |h(x_\kappa)|. \end{aligned} \tag{3}$$

Since $g(x)$ and $h(x)$ are of lower degree than k, our theorem may be applied to them. The lengths of the smallest intervals which contain κ of the points $x_1, x_2, \cdots, x_k$ or κ of the points $x_2, x_3, \cdots, x_{k+1}$ are both not smaller than $d_{\kappa-1}$. Hence

$$\max_{\kappa=1,2,\cdots,k} |g(x_\kappa)| \geqq 2^{-k+1}|b_0| d_1 d_2 \cdots d_{k-1},$$

$$\max_{\kappa=2,3,\cdots,k+1} |h(x_\kappa)| \geqq 2^{-k+1}|c_0| d_1 d_2 \cdots d_{k-1},$$

and by (3) and (2)

$$\begin{aligned} \max_{\kappa=1,2,\cdots,k+1} |f(x_\kappa)| &\geqq 2^{-k+1} d_1 d_2 \cdots d_{k-1}\{\max(|b_0|, |c_0|)\} \\ &= 2^{-k}|a_0| d_1 d_2 \cdots d_k. \end{aligned}$$

THEOREM 2. *Let* $f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k$ *be a polynomial of degree* k *and* $x_1 < x_2 < \cdots < x_n$ *a set of more than* k *integers. Then*

$$\max_{\nu=1,2,\cdots,n} |f(x_\nu)| \geqq 2^{-k}|a_0| \prod_{\kappa=1}^{k} \left[\frac{\kappa n - 1}{k}\right].$$

PROOF. We consider those $k+1$ of the integers x_ν whose subscripts are 1 and the k numbers

$$1 + \left[\frac{\rho n - 1}{k}\right] \qquad (\rho = 1, 2, \cdots, k),$$

and denote these x_ν in increasing order by $x_0', x_1', \cdots, x_k'$. The difference of two consecutive elements x_ν is at least 1, hence for $k \geqq \beta > \alpha > 0$

$$x_\beta' - x_\alpha' \geqq \left[\frac{\beta n - 1}{k}\right] - \left[\frac{\alpha n - 1}{k}\right]. \tag{4}$$

Since for every r and s

$$\left[\frac{r + s}{k}\right] \geqq \left[\frac{r}{k}\right] + \left[\frac{s}{k}\right],$$

we have

$$\left[\frac{\beta n - 1}{k}\right] \geqq \left[\frac{(\beta - \alpha)n - 1}{k}\right] + \left[\frac{\alpha n}{k}\right],$$

hence by (4)

$$(5)\qquad \begin{aligned} x_\beta' - x_\alpha' &\geqq \left[\frac{(\beta - \alpha)n - 1}{k}\right] + \left[\frac{\alpha n}{k}\right] - \left[\frac{\alpha n - 1}{k}\right] \\ &\geqq \left[\frac{(\beta - \alpha)n - 1}{k}\right]. \end{aligned}$$

It is obvious that (5) holds also for $\alpha = 0$. If the length of the smallest interval which contains $\kappa+1$ of the numbers $x_0', x_1', \cdots, x_k'$ is denoted by d_k', then by (5)

$$d_\kappa' \geqq \left[\frac{\kappa n - 1}{k}\right] \qquad (\kappa = 1, 2, \cdots, k),$$

hence, by Theorem 1,

$$\max_{\nu=1,2,\cdots,n} |f(x_\nu)| \geqq \max_{\kappa=0,1,\cdots,k} |f(x_\kappa')| \geqq 2^{-k} |a_0| \prod_{\kappa=1}^{k} \left[\frac{\kappa n - 1}{k}\right].$$

2. **Criteria for irreducibility.** Theorem 2 will be used now to obtain criteria for irreducibility of polynomials.

THEOREM 3. *Let $P(x)$ be a polynomial of degree n with integral rational coefficients. If for n integral values $x_1, x_2, \cdots, x_n$ the absolute value of $P(x_\nu)$ for $\nu = 1, 2, \cdots, n$ is less than*

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

but different from 0, then $P(x)$ is irreducible in the field of rational numbers.

PROOF. If $P(x)$ is reducible, then it contains a factor $f(x)$ of degree k with integral coefficients where $n > k \geqq [(n+1)/2]$. It follows now from Theorem 2 that

$$(6)\qquad M = \max_{\nu=1,2,\cdots,n} |f(x_\nu)| \geqq 2^{-k} \prod_{\kappa=1}^{k} \left[\frac{\kappa n - 1}{k}\right].$$

We set for fixed n

$$(7)\qquad \phi(k) = \phi(k, n) = 2^{-k} \prod_{\kappa=1}^{k} \left[\frac{\kappa n - 1}{k}\right].$$

Let us first assume that $k = [(n+1)/2]$. For even values of n we have

$$\left[\frac{\kappa n - 1}{k}\right] = \left[\frac{\kappa n - 1}{n/2}\right] = \left[\frac{2\kappa n - 2}{n}\right] = 2\kappa - 1 \quad (\kappa = 1, 2, \cdots, k),$$

hence by (7)

$$\begin{aligned}\phi\{[(n+1)/2]\} &\geqq 2^{-k}\prod_{\kappa=1}^{k}(2\kappa - 1) = 2^{-n/2}\cdot 1\cdot 3\cdot 5\cdots(n-1) \\ &= \frac{(n-1)!}{2^{n/2+(n-2)/2}[(n-2)/2]!} = \frac{(n-1)!}{2^{n-1}\{[(n-2)/2]!\}} = G.\end{aligned} \tag{8}$$

If n is odd, then

$$\begin{aligned}\left[\frac{\kappa n - 1}{k}\right] = \left[\frac{\kappa n - 1}{(n+1)/2}\right] &= \left[\frac{2\kappa n - 2}{n+1}\right] \\ &= \left[\frac{(2\kappa - 1)(n+1) + n - 2\kappa - 1}{n+1}\right],\end{aligned}$$

hence

$$\left[\frac{\kappa n - 1}{k}\right] = \begin{cases} 2\kappa - 1 & \text{for } \kappa = 1, 2, \cdots, (n-1)/2, \\ 2\kappa - 2 & \text{for } \kappa = (n+1)/2, \end{cases}$$

and by (7)

$$\begin{aligned}\phi\{[(n+1)/2]\} &\geqq 2^{-(n+1)/2}(n-1)\prod_{\kappa=1}^{(n-1)/2}(2\kappa - 1) \\ &= \frac{(n-1)!}{2^{(n+1)/2+(n-3)/2}\{[(n-3)/2]!\}} = \frac{(n-1)!}{2^{n-1}\{[(n-2)/2]!\}} = G.\end{aligned} \tag{9}$$

It follows from (8) and (9) that

$$\phi\left(\left[\frac{n+1}{2}\right]\right) \geqq G. \tag{10}$$

Now we maintain that

$$\phi(k+1) \geqq \phi(k) \quad \text{for} \quad \left[\frac{n+1}{2}\right] \leqq k \leqq n - 2. \tag{11}$$

For this purpose we want to prove that

$$\left[\frac{(\kappa+1)n - 1}{k+1}\right] \geqq \left[\frac{\kappa n - 1}{k}\right] \qquad (\kappa = 2, 3, \cdots, k). \tag{12}$$

We divide $\kappa n - 1$ by k:

$$\kappa n - 1 = qk + r \qquad (0 \leqq r < k),$$

hence $\kappa n > qk$ and $n > q$ since $\kappa \leqq k$. It follows that

$$\left[\frac{(\kappa+1)n-1}{k+1}\right] = \left[\frac{qk+r+n}{k+1}\right] = \left[\frac{q(k+1)+r+n-q}{k+1}\right]$$
$$\geqq q = \left[\frac{\kappa n - 1}{k}\right].$$

This proves (12). Moreover we have for $\kappa = 1$

$$\left[\frac{2n-1}{k+1}\right] \geqq \left[\frac{2n-1}{n-1}\right] = 2 = 2\left[\frac{n-1}{k}\right] \tag{13}$$

because it is sufficient for the proof of (11) to assume that $k+1 \leqq n-1$ and $k \geqq [(n+1)/2]$. Multiplying (13) and (12) for $\kappa = 2, 3, \cdots, k$ we obtain

$$\prod_{\kappa=1}^{k}\left[\frac{(\kappa+1)n-1}{k+1}\right] \geqq 2\prod_{\kappa=1}^{k}\left[\frac{\kappa n-1}{k}\right],$$

hence, since $[(n-1)/(k+1)] = 1$,

$$2^{-k-1}\prod_{\kappa=1}^{k+1}\left[\frac{\kappa n-1}{k+1}\right] = 2^{-k-1}\left[\frac{n-1}{k+1}\right]\prod_{\kappa=1}^{k}\left[\frac{(\kappa+1)n-1}{k+1}\right]$$
$$\geqq 2^{-k}\prod_{\kappa=1}^{k}\left[\frac{\kappa n-1}{k}\right].$$

This proves (11). It follows now from (6), (7), (11), and (10) that

$$M \geqq G.$$

Since $P(x)/f(x)$ is a polynomial with integral coefficients and $P(x_\nu) \neq 0$, we obtain

$$\max_{\nu=1,2,\cdots,n} |P(x_\nu)| \geqq \max_{\nu=1,2,\cdots,n} |f(x_\nu)| = M \geqq G.$$

This contradicts our assumption, and the theorem is proved.

The bound of Tatuzawa is

$$G_2 = (2^{-n}(n-1)!)^{1/2}$$

and our bound by (8) and (9)

$$G = \frac{(n-1)!}{2^{n-1}\{[(n-2)/2]!\}} = \begin{cases} 2^{-n/2}\cdot 1\cdot 3\cdot 5\cdots(n-1) & \text{for even } n, \\ 2^{-(n+1)/2}(n-1)\cdot 1\cdot 3\cdot 5\cdots(n-2) & \text{for odd } n. \end{cases}$$

Now we have by the formula of Wallis

$$\frac{1\cdot 3\cdot 5\cdots(2m-1)}{2\cdot 4\cdot 6\cdots(2m-2)}\sim\left(\frac{4m}{\pi}\right)^{1/2}.$$

For even n we obtain

$$\frac{G}{G_2}=\left(\frac{1\cdot 3\cdot 5\cdots(n-1)}{2\cdot 4\cdot 6\cdots(n-2)}\right)^{1/2}\sim\left(\frac{2n}{\pi}\right)^{1/4},$$

and for odd n

$$\frac{G}{G_2}=\frac{1}{2^{1/2}}\left(\frac{(n-1)\cdot 1\cdot 3\cdot 5\cdots(n-2)}{2\cdot 4\cdot 6\cdots(n-3)}\right)^{1/2}\sim\left(\frac{n}{2}\right)^{1/2}\left(\frac{2n}{\pi}\right)^{1/4}=\left(\frac{n^3}{2\pi}\right)^{1/4}.$$

Moreover, we have $G>G_2$ for $n>3$.

COROLLARY. *The integral polynomials*

$$A(x-x_1)(x-x_2)\cdots(x-x_n)+t \tag{14}$$

are irreducible in the field of rational numbers if $x_\mu\neq x_\nu$ *and* $1\leqq|t|<G$.

We have $G>1$ for $n>4$. Therefore the polynomials (14) are irreducible for $t=\pm 1$ and $n>4$. This is, as already mentioned in the introduction, for $A=1$ a theorem of Schur, and for arbitrary A a theorem of Dorwart and Ore.

We can formulate Theorem 3 also in the following form:

THEOREM 3a. *Let* $P(x)$ *be an integral polynomial of degree* n. *If for* n *different integers* $x_1, x_2, \cdots, x_n$

$$0<|P(x_\nu)|<2^{-k}\prod_{\kappa=1}^{k}\left[\frac{\kappa n-1}{k}\right]=\phi(k)\qquad(\nu=1,2,\cdots,n)$$

where $k\geqq[(n+1)/2]$, *then* $P(x)$ *cannot contain a factor* $f^*(x)$ *of degree* k^* *with* $k\leqq k^*<n$.

PROOF. If $P(x)$ contains such a factor, then by (6), (7), and (11)

$$\max_{\nu=1,2,\cdots,n}|P(x_\nu)|\geqq\max_{\nu=1,2,\cdots,n}|f^*(x_\nu)|\geqq\phi(k^*)\geqq\phi(k).$$

This contradicts our assumption.

THEOREM 4. *Let* $P(x)$ *be a polynomial of degree* n *with integral coefficients,* l *an integer with* $l\geqq 5$, *and* $n>l>n/2$. *If for* l *different integers* $x_1, x_2, \cdots, x_l$

$$0<|P(x_\lambda)|<H\qquad(\lambda=1,2,\cdots,l)$$

where $H=[(l+1)/2]$ for $l\geqq 7$, $H=3/2$ for $l=6$ and 5, *then* $P(x)$ *is irreducible in the field of rational numbers.*

PROOF. If $P(x)$ is reducible, then it must contain a factor $g(x)$ of degree k less than or equal to $n/2$ with integral coefficients. Here $k>1$. For a linear polynomial takes each value only once, hence the l integers $g(x_1), g(x_2), \cdots, g(x_l)$ must be different. However, only the $2[(l-1)/2]$ values $\pm 1, \pm 2, \cdots, \pm[(l-1)/2]$ are possible because

$$0 < | g(x_\lambda) | \leqq | P(x_\lambda) | < H \leqq \left[\frac{l+1}{2}\right] \qquad (\lambda = 1, 2, \cdots, l).$$

This gives a contradiction since $l>2\,[(l-1)/2]$.

It follows from Theorem 2 that

$$(15) \qquad \max_{\lambda=1,2,\cdots,l} | g(x_\lambda) | \geqq 2^{-k} \prod_{\kappa=1}^{k} \left[\frac{\kappa l - 1}{k}\right].$$

We denote the right-hand side of (15), for a given l, similarly as in (10), by $\phi(k)$ and maintain that

(16) $\phi(k+1)\geqq\phi(k)$ for $2\leqq k\leqq(l-3)/2$ and for $l/2\leqq k\leqq l-2$.

It follows from the proof of Theorem 3 that (16) holds for $l/2\leqq k \leqq l-2$ if we write l instead of n since $[(l+1)/2]=l/2$ for even l and $k\neq l/2$ for odd l.

Now we consider the case $k\leqq(l-3)/2$. Here we have

$$(17) \qquad \left[\frac{l-1}{k+1}\right] \geqq \left[\frac{l-1}{(l-1)/2}\right] = 2.$$

Moreover, it follows from (12) that

$$(18) \qquad \left[\frac{(\kappa+1)l-1}{k+1}\right] \geqq \left[\frac{\kappa l - 1}{k}\right] \qquad (\kappa = 1, 2, \cdots, k).$$

We proved (12) only for $\kappa\geqq 2$; but the proof remains correct for $\kappa=1$. It follows now from (18) and (17) that

$$2^{-k-1}\prod_{\kappa=0}^{k}\left[\frac{(\kappa+1)l-1}{k+1}\right] = 2^{-k-1}\prod_{\kappa=1}^{k+1}\left[\frac{\kappa l-1}{k+1}\right] \geqq 2^{-k}\prod_{\kappa=1}^{k}\left[\frac{\kappa l-1}{k}\right],$$

hence $\phi(k+1)\geqq\phi(k)$ for $k\leqq(l-3)/2$, and (16) is proved.

We now consider the remaining value $k=[(l-1)/2]$. We maintain that also here

$$\phi(k+1) \geqq \phi(k) \quad \text{for} \quad l > 12 \text{ and } l = 11, 9. \tag{19}$$

For even l we have $k=(l-2)/2$. It follows from (7) and (8) that for $l>12$

$$\begin{aligned} \phi(k+1) &= \phi\left\{\left[\frac{l+1}{2}\right]\right\} \geqq 2^{-l/2}\cdot 1\cdot 3\cdot 5\cdot 7\cdot \prod_{\kappa=5}^{k+1}\left[\frac{\kappa l-1}{k+1}\right] \\ &= 2^{-l/2}\cdot 1\cdot 3\cdot 5\cdot 7\cdot \prod_{\kappa=4}^{k}\left[\frac{(\kappa+1)l-1}{k+1}\right] \end{aligned} \tag{20}$$

and

$$\begin{aligned} \phi(k) &= \phi\left\{\left[\frac{l-1}{2}\right]\right\} \\ &= 2^{-(l-2)/2}\left[\frac{l-1}{(l-2)/2}\right]\left[\frac{2l-1}{(l-2)/2}\right]\left[\frac{3l-1}{(l-2)/2}\right]\prod_{\kappa=4}^{k}\left[\frac{\kappa l-1}{k}\right] \\ &= 2^{-(l-2)/2}\left[\frac{2l-2}{l-2}\right]\left[\frac{4l-2}{l-2}\right]\left[\frac{6l-2}{l-2}\right]\prod_{\kappa=4}^{k}\left[\frac{\kappa l-1}{k}\right]. \end{aligned}$$

Now $[(6l-2)/(l-2)]=6$ since $6l-2<7(l-2)$ for $l>12$. Similarly $[(2l-2)/(l-2)]=2$ and $[(4l-2)/(l-2)]=4$, hence

$$\phi(k) \geqq 2^{-(l-2)/2}\cdot 2\cdot 4\cdot 6\cdot \prod_{\kappa=4}^{k}\left[\frac{\kappa l-1}{k}\right]. \tag{21}$$

Since $3\cdot 5\cdot 7>2\cdot 2\cdot 4\cdot 6$, it follows from (20), (21), and (12) that (19) holds for even $l>12$.

Now, let l be odd. Here we have by (7) and (9) for $l>7$

$$\begin{aligned} \phi(k+1) &= \phi\left(\frac{l+1}{2}\right) = 2^{-(l+1)/2}\cdot 1\cdot 3\cdot 5\cdot 7\cdot \prod_{\kappa=5}^{k+1}\left[\frac{\kappa l-1}{k+1}\right] \\ &= 2^{-(l+1)/2}\cdot 1\cdot 3\cdot 5\cdot 7\cdot \prod_{\kappa=4}^{k}\left[\frac{(\kappa+1)l-1}{k+1}\right] \end{aligned} \tag{22}$$

and

$$\begin{aligned} \phi(k) &= \phi\left(\frac{l-1}{2}\right) \\ &= 2^{-(l-1)/2}\left[\frac{2l-2}{l-1}\right]\left[\frac{4l-2}{l-1}\right]\left[\frac{6l-2}{l-1}\right]\prod_{\kappa=4}^{k}\left[\frac{\kappa l-1}{k}\right] \\ &= 2^{-(l-1)/2}\cdot 2\cdot 4\cdot 6\cdot \prod_{\kappa=4}^{k}\left[\frac{\kappa l-1}{k}\right] \end{aligned} \tag{23}$$

since $6l-2<7(l-1)$. It follows from (22), (23), and (12) that (19) holds for odd $l>7$, too.

Now we have by (16) and (19)

$$\phi(k+1) \geqq \phi(k) \quad \text{for} \quad 2 \leqq k \leqq l-2, \text{ and } l > 12, l = 11, 9. \tag{24}$$

By direct calculation we obtain

$$\begin{aligned} &\phi(5) > \phi(6) > \phi(4) \quad \text{for} \quad l = 12, \\ &\phi(4) > \phi(5) > \phi(3) \quad \text{for} \quad l = 10, \\ &\phi(3) > \phi(4) > \phi(2) \quad \text{for} \quad l = 8 \text{ and } l = 7. \end{aligned} \tag{25}$$

By (24) and (25) we have for $l \geqq 7$

$$\phi(k) \geqq \phi(2) = \left[\frac{2l-1}{2}\right]\left[\frac{l-1}{2}\right] > \left[\frac{l+1}{2}\right] = H \qquad (3 \leqq k < l), \tag{26}$$

and by direct calculation

$$\phi(k) \geqq 3/2 = H \quad \text{for} \quad l = 6 \text{ and } 5 \qquad (2 \leqq k < l), \tag{27}$$

hence, by (15), (26), and (27),

$$\max_{\lambda=1,2,\cdots,l} | P(x_\lambda) | \geqq \max_{\lambda=1,2,\cdots,l} | g(x_\lambda) | \geqq \phi(k) \geqq H. \tag{28}$$

This contradicts our assumption, and $P(x)$ must be irreducible.

Theorem 4 cannot be improved further. If we assume instead of

$$0 < | P(x_\lambda) | < [(l+1)/2] \qquad (\lambda = 1, 2, \cdots, l)$$

only

$$0 < | P(x_\lambda) | \leqq [(l+1)/2] \qquad (\lambda = 1, 2, \cdots, l),$$

then $P(x)$ may be reducible.

This is shown by the following examples

$$P(x) = x\left\{h(x) \prod_{\lambda=1}^{l/2} (x^2 - \lambda^2) + 1\right\} \quad \text{for even } l,$$

$$P(x) = x\left\{h(x) \left(x - \frac{l+1}{2}\right) \prod_{\lambda=1}^{(l-1)/2} (x^2 - \lambda^2) + 1\right\} \quad \text{for odd } l,$$

where $h(x)$ is an arbitrary integral polynomial of degree $n-l-1$. We have here $P(x)=x$ for $x=\pm 1, \pm 2, \cdots, \pm l/2$ for even l, and $x=\pm 1, \pm 2, \cdots, \pm(l-1)/2, +(l+1)/2$ for odd l. At l integral points these polynomials take values which are different from zero and, without regard to sign, less than or equal to $[(l+1)/2]$; but they are reducible.

COROLLARY. *Let $h(x)$ be an arbitrary integral polynomial of degree $n-1$ and $x_1, x_2, \cdots, x_l$ different integers. The integral polynomial $P(x)$ of degree n,*

$$P(x) = (x - x_1)(x - x_2) \cdots (x - x_l)h(x) + t,$$

is irreducible in the field of rational numbers if $l \geqq 5$, $n > l > n/2$ and $1 \leqq |t| < H$ where $H = [(l+1)/2]$ for $l \geqq 7$ and $H = 3/2$ for $l = 6$ and 5.

For the proof of Theorem 4 for $l > 12$ it is sufficient to prove only (26) instead of (24). We proved here (24) in order to obtain the following theorem.

THEOREM 4a. *Let $P(x)$ be an integral polynomial of degree n; let h and l be integers satisfying the following conditions:*

$$n > l > n/2, \qquad l > h \geqq 2, \quad \text{and} \quad l > 12, \text{ or } l = 11, 9.$$

If for l different integers $x_1, x_2, \cdots, x_l$

$$0 < |P(x_\lambda)| < \phi(h) = 2^{-h} \prod_{\mu=1}^{h} \left[\frac{\mu l - 1}{h} \right],$$

then $P(x)$ cannot contain a factor of degree h^* with $h \leqq h^* \leqq n/2$.

PROOF. If $P(x)$ contains a factor of degree h^*, then by (28) and (24)

$$\max_{\lambda=1,2,\cdots,l} |P(x_\lambda)| \geqq \max_{\lambda=1,2,\cdots,l} |g(x_\lambda)| \geqq \phi(h^*) \geqq \phi(h).$$

This contradicts our assumption.

A similar theorem can be obtained for $l = 12$, 10, 8, and 7.

By combining Theorems 3a and 4a the following theorem is obtained.

THEOREM 5. *Let $P(x)$ be an integral polynomial of degree n, and k, l, and h integers satisfying the following conditions:*

$$k \geqq [(n+1)/2], \qquad n > l > n/2, \ l > 12 \text{ or } l = 11 \text{ or } 9,$$
$$l > h, \qquad n \geqq k + h - 1.$$

If for n different integers $x_1, x_2, \cdots, x_n$

$$0 < |P(x_\nu)| < 2^{-k} \prod_{\kappa=1}^{k} \left[\frac{\kappa n - 1}{k} \right] \qquad (\nu = 1, 2, \cdots, n),$$

and for l of these x_ν, say $x^{(1)}, x^{(2)}, \cdots, x^{(l)}$,

$$| P(x^{(\lambda)}) | < 2^{-h} \prod_{\mu=1}^{h} \left[\frac{\mu l - 1}{h} \right] \qquad (\lambda = 1, 2, \cdots, l),$$

then $P(x)$ *is irreducible in the field of rational numbers.*

PROOF. If $P(x)$ is reducible, then

$$P(x) = f(x) \cdot g(x).$$

If the degree of $f(x)$ is $k^* \geqq n/2$, then the degree of $g(x)$ is $n-k^*$. It follows from Theorem 3a that $k^* \leqq k-1$, and from Theorem 4a that $n-k^* \leqq h-1$, hence $n \leqq k+h-2$. This gives a contradiction.

UNIVERSITY OF NORTH CAROLINA