ON THE DISTRIBUTION OF THE ROOTS OF A POLYNOMIAL WITH INTEGRAL COEFFICIENTS

ROBERT BREUSCH

The following question has been raised by D. H. Lehmer[1] in connection with prime number problems: "If ϵ is a positive quantity, to find a polynomial of the form $f(z)\equiv z^r+a_1z^{r-1}+\cdots+a_r$ where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and $1+\epsilon$." Lehmer calls this absolute value $\Omega(f)$. Since, for $f(z)=z^2-z-1$, $\Omega(f)=1.6\cdots$, we may assume $\epsilon<1$, and therefore $a_r=\pm 1$. Then $\Omega(f)$ may be written in the form $\prod_{n=1}^r |z_n|^{[|z_n|]}$, where the z_n are the roots of $f(z)$. It is shown in this paper that no nonreciprocal polynomial $f(z)$ exists with $\Omega(f)<1.179$. Lehmer himself gives an example of a reciprocal polynomial of degree 10 for which $\Omega(f)$ is less than this, namely $1.176\cdots$; no nonreciprocal polynomial seems to be known for which $\Omega(f)<1.32$. Thus the present result is still far from being a complete answer to the question.

Let $f(z)\equiv z^r+a_1z^{r-1}+\cdots\pm 1$ be a nonreciprocal polynomial with integral coefficients, irreducible in the rational field. The proof makes use of the resultant $R(f, g)$ of $f(z)$ and the polynomial $g(z)\equiv\pm z^rf(1/z)=z^r+\cdots$. All the roots of $g(z)$ are of the form $z_n^*\equiv\bar{z}_n^{-1}$ where the $\bar{z}_n$ are the conjugates of the roots z_n of $f(z)$. Since $f(z)$ and $g(z)$ are irreducible and different, have integral coefficients and highest coefficients 1, $|R(f, g)|\equiv\prod_{n=1}^r\prod_{m=1}^r|z_n-z_m^*|$ must be not less than 1.

$$|R(f, g)|\equiv\prod_{n=1}^{r}\prod_{m>n}|z_n-z_m^*|\cdot|z_m-z_n^*|\cdot\prod_{n=1}^{r}|z_n-z_n^*|\equiv P_1\cdot P_2.$$

If $\Omega(f)=k$, it will be shown in Lemma 2 that $P_1<k^{2r}\cdot r^r$, and in Lemma 3 that $P_2\leqq(4(k-1)/r)^r$.

LEMMA 1. *$P_1\equiv\prod_{n=1}^r\prod_{m>n}|z_n-z_m^*|\cdot|z_m-z_n^*|$ has the greatest value compatible with the two conditions* (I) $\prod_{n=1}^r|z_n|=1$, (II) $\prod_{n=1}^r|z_n|^{[|z_n|]}=k$ $(1<k<2)$ *for* $|z_1|=k$, $|z_2|=\cdots=|z_{r-1}|=1$, $|z_r|=1/k$.

PROOF. For $n=1, 2, \cdots, r$, call b_n values of the z_n for which P_1 takes its greatest value when restricted by conditions I and II.

Presented to the Society, April 28, 1951; received by the editors January 2, 1951.

[1] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. vol. 34 (1933) p. 476.

Assume that at least two of the b's are absolutely greater than 1, for example, $|b_1|>1$, $|b_2|>1$. P_1 may be rewritten in the form

$$P_1 \equiv \left| (z_1 - \bar{z}_2^{-1})(\bar{z}_2 - z_1^{-1}) \cdot \prod_{n=3}^{r} (z_1 - \overset{*}{z_n})(\bar{z}_n - z_1^{-1})(\bar{z}_2 - z_n^{-1})(z_n - \bar{z}_2^{-1}) \right.$$
$$\left. \cdot \prod_{n=3}^{r} \prod_{m>n} (z_n - \overset{*}{z_m})(z_m - \overset{*}{z_n}) \right| .$$

The expression within the absolute bars is now an analytic function of z_1 and $\bar{z}_2$ (but not of the remaining z's). Calling this expression $F(z_1, \bar{z}_2, z_3, \cdots, z_r)$, and introducing $A \equiv b_1\bar{b}_2$ (with $1<|A|\leqq k$), our assumption implies that $F(z, A/z, b_3, \cdots, b_r)$ which is analytic in $1\leqq|z|\leqq|A|$ takes its largest value in this region for $z=b_1$. But this is impossible, for b_1 is by assumption an interior point of this region, because $1<|b_1|<|A|$.

Interchanging the z_n with the z_n^* does not change P_1; thus not two of the $|b_n^*|$ can be greater than 1, that is, not two of the $|b_n|$ can be less than 1.

Therefore (by proper arrangement of the subscripts) P_1 takes its greatest value for $z_1=ke^{i\theta_1}$, $z_1^*=(1/k)e^{i\theta_1}$, $z_r=(1/k)e^{i\theta_r}$, $z_r^*=ke^{i\theta_r}$, $z_n=e^{i\theta_n}$, $z_n^*=z_n$ $(1<n<r)$.

LEMMA 2. $P_1<k^{2r}\cdot r^r$.

PROOF. Using the values found in Lemma 1, we get, for $1<n<r$,

$$|z_1 - \overset{*}{z_n}| \cdot |z_n - \overset{*}{z_1}| = |ke^{i\theta_1} - e^{i\theta_n}| \cdot \frac{1}{k} \cdot |ke^{i\theta_n} - e^{i\theta_1}|$$
$$= \frac{1}{k}|z_1 - z_n|^2$$

(since $|ke^{i\theta_n}-e^{i\theta_1}| = |e^{i\theta_n}-ke^{i\theta_1}|$). Similarly, for $1<n<r$,

$$|z_r - \overset{*}{z_n}| \cdot |z_n - \overset{*}{z_r}| = k\cdot|z_r - z_n|^2,$$
$$|z_1 - \overset{*}{z_r}| \cdot |z_r - \overset{*}{z_1}| = |e^{i\theta_1} - e^{i\theta_r}|^2 < |z_1 - z_r|^2.$$

Therefore

$$P_1 < |z_1 - z_r|^2 \cdot \prod_{n=2}^{r-1} |z_1 - z_n|^2 \cdot |z_r - z_n|^2 \cdot \prod_{n=2}^{r-1} \prod_{n<m<r} |z_n - z_m|^2$$
$$= \prod_{n=1}^{r} \prod_{m>n} |z_n - z_m|^2.$$

The function

$$G(z) \equiv \frac{1}{z^{2r}}\left(z - \frac{z_1 z_r}{z}\right)^2 \cdot \prod_{n=2}^{r-1} (z - z_n)^2 \cdot \left(\frac{z_1 z_r}{z} - z_n\right)^2 \cdot \prod_{n=2}^{r-1} \prod_{n<m<r} |z_n - z_m|^2$$

is analytic for $1 \leqq |z| \leqq \infty$, and has therefore its greatest absolute value in this region for $|z| = 1$. But for $|z| = 1$, $|G(z)|$ is the absolute value of the discriminant of the polynomial whose r roots z, $z_1 z_r/z$, z_2, $\cdots$, z_{r-1}, all lie on the unit circle. This is known[2] to be not greater than r^r. Therefore $|G(z)| < r^r$ for $|z| > 1$, and $P_1 < |z_1^{2r}| \cdot |G(z_1)| < k^{2r} \cdot r^r$.

LEMMA 3. *If the z_n satisfy conditions* I *and* II *of Lemma* 1, *then* $P_2 \equiv \prod_{n=1}^{r} |z_n - z_n^*| \leqq (4(k-1)/r)^r$.

PROOF. If $|z_n| = 1 + \epsilon_n \geqq 1$ for $n = 1, 2, \cdots, s$, and $|z_n^*| = |z_n|^{-1} = 1 + \epsilon_n > 1$ for $n = s+1, \cdots, r$, then $|z_n - z_n^*| = \big| |z_n| - |z_n|^{-1} \big| = 1 + \epsilon_n - 1/(1+\epsilon_n) \leqq 2\epsilon_n$ for $n = 1, 2, \cdots, r$. Also, since $\prod_{n=1}^{s} (1+\epsilon_n) = k$, and $\prod_{n=s+1}^{r} (1+\epsilon_n) = k$, $1 + \sum_{n=1}^{s} \epsilon_n \leqq k$, $1 + \sum_{n=s+1}^{r} \epsilon_n \leqq k$, and $\sum_{n=1}^{r} \epsilon_n \leqq 2(k-1)$. Therefore $P_2 \leqq \prod_{n=1}^{r} (2\epsilon_n) \leqq (4(k-1)/r)^r$.

THEOREM. *If $f(z)$ is a nonreciprocal irreducible polynomial with integral coefficient and highest coefficient* 1, *then* $\Omega(f) = k > 1.179$.

PROOF. If r is the degree of $f(z)$, the statement is obviously correct for $|a_r| > 1$, since $k \geqq |a_r|$. Thus we may assume $|a_r| = 1$. Then by Lemmas 2 and 3, $|R(f, g)| \equiv P_1 P_2 < k^{2r} r^r (4(k-1)/r)^r = (4k^2(k-1))^r$. This must be not less than 1; therefore $4k^2(k-1) \geqq 1$, $k > 1.179$.

AMHERST COLLEGE

[2] I. Schur, *Ueber die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. vol. 1 (1918) p. 385.