A REMARK ON THE CHEBOTAREV THEOREM ABOUT ROOTS OF UNITY

F. Pakovich[1]
Department of Mathematics, Ben Gurion University, P.O.B. 653, Beer-Sheva 84105, Israel
pakovich@math.bgu.ac.il

Received: 2/21/07, Accepted: 4/8/07, Published: 4/12/07

Abstract

Let Ω be a matrix with entries $a_{i,j} = \omega^{ij}$, $1 \le i, j \le n$, where $\omega = e^{2\pi\sqrt{-1}/n}$, $n \in \mathbb{N}$. The Chebotarev theorem states that if n is a prime then any minor of Ω is non-zero. In this note we provide an analogue of this statement for composite n.

Let Ω be a matrix with entries $a_{i,j} = \omega^{ij}$, $1 \le i, j \le n$, where $\omega = e^{2\pi\sqrt{-1}/n}$, $n \in \mathbb{N}$. The Chebotarev theorem states that if n is a prime then any minor of Ω is non-zero. Chebotarev's proof of this theorem and the references to other proofs can be found in [2]. Yet other proofs can be found in recent papers [1] and [3].

For a complex polynomial $P(z)$ denote by $w(P)$ the number of non-zero coefficients of $P(z)$. It is easy to see that the Chebotarev theorem is equivalent to the following statement: if a non-zero polynomial $P(z)$, $\deg P(z) \le n-1$, has k different roots which are n-roots of unity then $w(P) > k$ whenever n is a prime.

A natural question is: How small can $w(P)$ be if n is a composite number ? The example $D_{n,r,l}(z) = z^l(1 + z^r + z^{2r} + \cdots + z^{(\frac{n}{r}-1)r})$, where $r|n$, $0 \le l \le r-1$, shows that $w(P)$ could be as small as $n/(n-k)$. In this note we show that actually it is the "worst" possible case.

Theorem. *Let n be a composite number and $P(z)$ be a non-zero complex polynomial, $\deg P(z) \le n-1$. Suppose that $P(z)$ has exactly k different roots which are n-roots of unity. Then the inequality*

$$w(P) \ge \frac{n}{n-k} \qquad (*)$$

holds. Furthermore, the equality attains if and only if $P(z)$ up to a multiplication by a complex number coincides with $D_{n,r,l}(\omega^j z)$ for some j, $0 \le j \le n-1$, and r, l as above.

Proof. Let $P(z) = p_0 + p_1 z + \ldots + p_{n-1}z^{n-1}$ and let $C = \begin{pmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_{n-1} & p_0 & \cdots & p_{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ p_1 & p_2 & \cdots & p_0 \end{pmatrix}$ be the

[1]Research supported by the ISF, Grant No. 979/05

circulant matrix generated by the coefficients of $P(z)$. We will denote the row vectors of C by $\vec{t_j}$, $0 \leq j \leq n-1$. Set $r = \operatorname{rk} C$. The key observation is that the number k is equal to the number $n - r$. To establish it notice that eigenvectors of C are

$$\vec{f_i} = ((\omega^i)^0, (\omega^i)^1, ..., (\omega^i)^{(n-1)}), \qquad 0 \leq i \leq n-1,$$

and the corresponding eigenvalues are $P(\omega^i)$, $0 \leq i \leq n-1$. Furthermore, the vectors $\vec{f_i}$, $0 \leq i \leq n-1$, form a basis of $\mathbb{C}^n$. The matrix C is diagonal with respect to this basis and therefore $k = n - r$.

It follows that in order to prove inequality (*) it is enough to establish the inequality

$$w(P)\, r \geq n. \tag{**}$$

This inequality essentially is a particular case of Theorem B in [1] and can be established easily as follows ([1]). Let V be a vector space generated by the vectors $\vec{t_j}$, $0 \leq j \leq n-1$, and $R \subseteq \{\vec{t_0}, \vec{t_1}, ..., \vec{t}_{n-1}\}$ consisting of r vectors which generate V. Clearly, for any i, $1 \leq i \leq n$, there exists a vector $\vec{v} \in V$ for which its i-th coordinate is distinct from zero. Since each vector from R has exactly $w(P)$ non zero coordinates it follows that (**) holds.

For a vector $\vec{v} \in \mathbb{C}^n$ denote by $\operatorname{supp}\{\vec{v}\}$ the set consisting of numbers i, $1 \leq i \leq n$, for which the i^{th} coordinate of $\vec{v}$ is non-zero. Observe now that the equality in (**) is attained only if for any two vectors $\vec{v}_1, \vec{v}_2 \in R$ we have $\operatorname{supp}\{\vec{v}_1\} \cap \operatorname{supp}\{\vec{v}_2\} = \emptyset$. This implies easily that $\operatorname{supp}\{\vec{t_0}\}$ consists of numbers all congruent modulo r to the same number l, $0 \leq l \leq r-1$. Therefore, $P(z) = z^l Q(z^r)$ for some polynomial $Q(z) = q_0 + q_1 z + ... + q_{(n/r)-1} z^{(n/r)-1}$ and number l, $0 \leq l \leq r-1$.

Furthermore, since the vectors $\vec{t_0}, \vec{t_r}, \vec{t}_{2r}, ..., \vec{t}_{(n/r)-1}$ have equal supports the equality in (**) implies that any two of them are proportional. Therefore, the rank of the circulant matrix W generated by the coefficients of $Q(z)$ equals 1. This implies that the vector $\vec{q} = \{q_0, q_1, ..., q_{(n/r)-1}\}$ is orthogonal to $(n/r) - 1$ vectors from the collection

$$\vec{g_j} = ((\nu^j)^0, (\nu^j)^1, ..., (\nu^j)^{(n/r)-1}), \qquad 0 \leq j \leq (n/r) - 1,$$

where $\nu = \omega^r$. Since $\vec{g_j}$, $0 \leq j \leq (n/r) - 1$, are linearly independent this implies that there exists $\alpha \in \mathbb{C}$ such that $\vec{q} = \alpha \vec{g_j}$ for some $0 \leq j \leq (n/r) - 1$. □

References

[1] D. Goldstein, R. Guralnick, I. Isaacs, *Inequalities for finite group permutation modules*, Trans. Am. Math. Soc. 357, No.10, 4017-4042 (2005)

[2] P. Stevenhagen, H. Lenstra, *Chebotarev and his density theorem,* Math. Intell. 18, No.2, 26-37 (1996)

[3] T. Tao, *An uncertainty principle for cyclic groups of prime order*, Math. Res. Lett. 12, No.1, 121-127 (2005).