MATH. SCAND. 33 (1973), 18–20

STABILITY IN POLYNOMIAL FACTORIZATION

OLAV KALLENBERG

Consider the linear space $\mathscr{P}$ of all real (or all complex) polynomials $p,q,\ldots$, in any fixed number of variables. Identifying polynomials differing by nonzero numerical factors, we obtain a space $\tilde{\mathscr{P}}$ of equivalence classes $\tilde{p},\tilde{q},\ldots$. Given any norm in $\mathscr{P}$, we define the metric ϱ in $\tilde{\mathscr{P}}$ by

$$\varrho(\tilde{p},\tilde{q}) = \inf\{\|p-q\| : p \in \tilde{p},\ q \in \tilde{q},\ \|p\|=\|q\|=1\}, \qquad \tilde{p},\tilde{q} \in \tilde{\mathscr{P}} .$$

For fixed $p \neq 0$ and $q\,|\,p$, we define $\beta=\beta_{p,q}$ by

$$\beta(\varepsilon) = \sup \varrho(\tilde{q},\tilde{q}'), \qquad \varepsilon > 0 ,$$

where the supremum extends over all $p',q' \in \mathscr{P}$ satisfying

$$\deg p' \leqq \deg p, \quad \varrho(\tilde{p},\tilde{p}') \leqq \varepsilon, \quad q'\,|\,p', \quad \varrho(\tilde{q},\tilde{q}') = \min_{r|p} \varrho(\tilde{r},\tilde{q}') .$$

(Here "deg" denotes the degree when all variables are replaced by t, say. Cf. the Remark at the end.) Furthermore, let $\mu=\mu_{p,q}$ be the greatest multiplicity of any common factor of q and p/q, (and put $\mu=1$ if no common factor exists.)

THEOREM. *As $\varepsilon \to 0$, the quantity $\beta(\varepsilon)\varepsilon^{-1/\mu}$ is bounded above and below by positive numbers.*

This theorem gives the rate of stability in polynomial factorization. (The stability itself is easily established by compactness arguments.) Similar estimates may be obtained for the related quantities α_p and β_p (cf. [1]). The above result may also be stated directly in $\mathscr{P}$, but this requires some sort of norming. In [1] an application was given to the decomposition of finitely supported probability measures.

PROOF. The lower bound is established as in [1], so we may restrict our attention to the upper bound. In the complex, one variable case, let

$$p(x) = (x-\alpha)^m q(x)$$

with $q(\alpha) \neq 0$, and let $\|p-p'\| < \varepsilon$. If α' is one of the m zeros of p' near α, we get

Received March 21, 1972; in revised form February 20, 1973.

$$|(\alpha'-\alpha)^m q(\alpha')| = |p(\alpha')-p'(\alpha')| = O(\varepsilon)\,,$$

and since $1/q(\alpha')$ is bounded, we get $|\alpha-\alpha'|=O(\varepsilon^{1/m})$. Next suppose that $p=qr$, where q and r are relatively prime, and let $p'=q'r'$ be the corresponding factorization of p'. Assume that q and q' have leading coefficients 1. If

$$\|q-q'\| \neq O(\|p-p'\|)\,,$$

consider some sequence $p_n'=q_n'r_n'$ with $p_n' \to p$ such that $\|q-q_n'\|/\|p-p_n'\| \to \infty$. From the relation

$$\frac{p_n'-p}{\|q_n'-q\|} = \frac{q_n'-q}{\|q_n'-q\|}r_n' + q\frac{r_n'-r}{\|q_n'-q\|}$$

it follows by letting $n \to \infty$ through some suitable sub-sequence that $sr+qt=0$ for some $s,t \neq 0$, so $q\,|\,sr$, and finally $q\,|\,s$, which contradicts the fact that $\deg s < \deg q$.

In the complex, several variable case, reduce p to the form

$$p(x,y,\ldots,w) = x^d + x^{d-1}s_1(y,\ldots,w) + \ldots + s_d(y,\ldots,w)$$

by means of a suitable non-singular linear substitution. Let $r \neq 0$ be a polynomial in $y,\ldots,w$ such that, for fixed $y,\ldots,w$ with $r(y,\ldots,w)\neq 0$, each prime of p has only single zeros in x, and the zeros of non-equivalent primes are different. (Use the well-known fact that, if p_1 and p_2 are relatively prime, then $p_1q_1+p_2q_2$ is non-zero and independent of x for some q_1 and q_2.) Applying the one-variable version of the theorem to p, it is seen that, for fixed $y,\ldots,w$ with $r(y,\ldots,w)\neq 0$, the coefficients in q and q' differ by at most $O(\varepsilon^{1/\mu})$. Making sufficiently many choices of $y,\ldots,w$ to determine the coefficients of q (regarded as a polynomial in $x,y,\ldots,w$), we obtain a linear system of equations for the differences of coefficients in q and q' with quantities of magnitude $O(\varepsilon^{1/\mu})$ in the right member. By linearity, the solution has then the same magnitude.

In the case of real polynomials, use the fact that, if a real prime p splits over C, it must split into two non-equivalent conjugate primes (relative to C), both of which determine p uniquely.

REMARK. The theorem was originally stated and proved with the degree of a polynomial regarded as a vector. However, this interpretation leads to new difficulties without increasing the usefulness of the result. In particular, obvious modifications in the proof of Theorem 2 in [1] will make the present version of the theorem equally applicable.

ACKNOWLEDGEMENT. I am very grateful to Prof. C. G. Esseen for directing my attention towards problems in this area, and also to Prof. H. Bergström and the referee for several suggestions leading to essential simplifications.

REFERENCE

1. O. Kallenberg, *Stability in the decomposition of probability measures with finite support*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete, 23 (1972), 216–223.

CHALMERS UNIVERSITY OF TECHNOLOGY
AND
UNIVERSITY OF GÖTEBORG