MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 184
OCTOBER 1988, PAGES 837-839

A Remark on a Paper by Wang: Another Surprising Property of 42

By J. A. Abbott and J. H. Davenport

Abstract. We give a counterexample to a bound quoted in Wang's paper on polynomial factorization over algebraic number fields. We also give an alternative to that bound which seems not to have been published before.

Currently the best algorithms for factorizing polynomials over algebraic number fields perform a factorization over a finite field, refine this factorization by Hensel lifting to a suitable prime power, and finally deduce the true factorization. It is thus necessary to estimate how far the modular factorization has to be lifted so we can be sure of deducing the true irreducible factors. This estimate comes from a bound on the "sizes" of coefficients of the factors.

We introduce some notation: f is the polynomial to be factorized over the field $\mathbf{Q}(\theta)$, where θ is an algebraic integer of degree m with minimal polynomial $m_\theta(x) \in \mathbf{Z}[x]$. Let $\|\theta\| = \max\{|\phi(\theta)| : \phi\colon \mathbf{Q}(\theta) \to \mathbf{C}\}$ (noting that the product of the $\phi(\theta)$ is the trailing coefficient, so at least one $|\phi(\theta)|$ is at least one). If $R = \sum_{j=0}^{d} c_j x^j$ is a polynomial with complex coefficients, define $\|R\|_2 = \sqrt{\sum |c_j|^2}$, following [2]. Recall Gauss's Lemma: let O be the ring of integers in $\mathbf{Q}(\theta)$; if $f(x) \in O[x]$ factorizes in $\mathbf{Q}(\theta)[x]$ then the factors can be taken to lie in $O[x]$. So we compute [1] the defect: the largest denominator, Δ, that occurs in O, i.e., $O \subseteq \frac{1}{\Delta}\mathbf{Z}[\theta]$. In fact, an integer multiple of Δ will suffice [4]. We now know how big the denominator can be, so we estimate the numerator. We can regard $f(x)$ as an element of $\mathbf{C}[x]$ and determine the maximum magnitude, B, of any coefficient of any factor in $\mathbf{C}[x]$. Thus our problem may be restated as: given that $|\sum_{i=0}^{m-1} c_i \theta^i/\Delta| \leq B$ for all embeddings $\mathbf{Q}(\theta) \to \mathbf{C}$, find a bound on $|c_i|$. Let M be the Vandermonde matrix

$$\begin{pmatrix} 1 & \theta & \theta^2 & \cdots & \theta^{m-1} \\ 1 & \theta_2 & \theta_2^2 & \cdots & \theta_2^{m-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & \theta_m & \theta_m^2 & \cdots & \theta_m^{m-1} \end{pmatrix},$$

so we can write $M\mathbf{c} = \mathbf{b}$ with $\mathbf{b}$ lying in a cube of side $2\Delta B$ centered on $\mathbf{0}$. In [3] Wang quotes Weinberger (presumably [4]) as having proved

$$\max |c_i| \leq \frac{\Delta B m! \|\theta\|^{m-1}}{|\det(M)|} \tag{1}$$

Received August 27, 1987; revised January 25, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12D10.

whereas [4] gives the very similar formula

$$\max|c_i| \leq \frac{\Delta B m! \|\theta\|^{m(m-1)/2}}{|\det(M)|}. \tag{2}$$

There is also another "well-known," but apparently unpublished, result which is similar to the bound quoted in [3]:

$$\max|c_i| \leq \frac{\Delta B m! \|m_\theta\|_2^{m-1}}{|\det(M)|}. \tag{3}$$

We give proofs of (2) and (3). Write $\mathbf{c} = M^{-1}\mathbf{b}$, and $M^{-1} = M^{\mathrm{adj}}/\det(M)$. To show (3), we need to use the result of Landau [2] that

$$\prod\{|\alpha_i| : |\alpha_i| > 1 \text{ and } f(\alpha_i) = 0\} \leq \|f\|_2.$$

If we expand the determinants which are the entries of M^{adj}, we find that each entry is the sum of $(m-1)!$ terms and each term is a product of the θ_i to distinct powers—this gives (2) immediately. Rewriting the terms as in $ab^2c^3 = (abc)(bc)(c)$ and using Landau's result, we find each term is at most $\|m_\theta\|_2^{m-1}$; hence (3).

Now for a counterexample to (1). Let $\theta^3 = 42$. So θ can embed in $\mathbf{C}$ as $3.476\ldots$, or $-1.738\ldots \pm 3.010\ldots i$. Let $w = 21\theta^2 + 73\theta - 127$. Under any of the three embeddings into $\mathbf{C}$, w has magnitude at most 381. The defect for $\mathbf{Q}(\theta)$ is 1, so we can take $\Delta = 1$, and $B = 381$. Formula (1) would then imply that the coordinates of w with respect to $\{1, \theta, \theta^2\}$ do not exceed

$$\frac{1 \times 381 \times 3! \times (3.476\ldots)^2}{\sqrt{27 \times 42^2}} < 126.6,$$

contradicting the unique representation given above.

This counterexample is the smallest of a family. Pick a noncube $n \in \mathbf{Z}^+$, and put $m_\theta(x) = x^3 - n$. Let $\beta \in \mathbf{R}$ be a cube root of n; so there are three maps $\mathbf{Q}(\theta) \to \mathbf{C}$ according as $\theta \to \beta$, $\omega\beta$, or $\omega^2\beta$, where $\omega \in \mathbf{C}$ satisfies $\omega^2 + \omega + 1 = 0$. Let p/q be a rational approximation to β; say $p/q = \beta + \varepsilon$. Consider $w = q\theta^2 + p\theta - \lceil \frac{1}{2} q\beta^2 \rceil$. If $\theta \to \beta$, then $w \to 2q\beta^2 + q\varepsilon\beta - \lceil \frac{1}{2} q\beta^2 \rceil \approx \frac{3}{2} q\beta^2 + q\varepsilon\beta$. If $\theta \to \omega\beta$ or $\omega^2\beta$, then $\theta^2 = \beta\bar{\theta}$ (complex conjugate), so $w \to -q\beta^2 + q\varepsilon\theta - \lceil \frac{1}{2} q\beta^2 \rceil \approx -\frac{3}{2} q\beta^2 + q\varepsilon\theta$. By Dirichlet's theorem on Diophantine approximation we can make $\varepsilon < q^{-2}$, so we may ignore ε terms and find that (1) gives the bound on the coordinates of w as

$$\frac{\frac{3}{2} q\beta^2 \times 3! \times \beta^2}{\sqrt{27}\beta^3} = \sqrt{3} q\beta.$$

Hence the formula fails if $\frac{1}{2} q\beta^2 > \sqrt{3} q\beta$, i.e., if $\beta > 2\sqrt{3}$. Note that $(2\sqrt{3})^3 \approx 41.6$, so $n = 42$ is the smallest integer for which a counterexample of this family can exist.

School of Mathematical Sciences
University of Bath
Claverton Down
Bath, Avon BA2 7AY
England
E-mail: jaa@uk.ac.bath.maths
jhd@uk.ac.bath.maths

1. R. J. BRADFORD, *On the Computation of Integral Bases and Defects of Integrity*, Ph.D. Thesis, University of Bath, May 1988.

2. M. MIGNOTTE, "An inequality about factors of polynomials," *Math. Comp.*, v. 28, 1974, pp. 1153–1157.

3. P. S. WANG, "Factoring multivariate polynomials over algebraic number fields," *Math. Comp.*, v. 30, 1976, pp. 324–336.

4. P. J. WEINBERGER & L. P. ROTHSCHILD, "Factoring polynomials over algebraic number fields," *ACM Trans. Math. Software*, v. 2(4), 1976, pp. 335–350.