MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 126, APRIL 1974, PAGES 589–597

The Minimum Root Separation of a Polynomial*

By George E. Collins and Ellis Horowitz

Abstract. The minimum root separation of a complex polynomial A is defined as the minimum of the distances between distinct roots of A. For polynomials with Gaussian integer coefficients and no multiple roots, three lower bounds are derived for the root separation. In each case, the bound is a function of the degree n of A and the sum d of the absolute values of the coefficients of A. The notion of a seminorm for a commutative ring is defined, and it is shown how any seminorm can be extended to polynomial rings and matrix rings, obtaining a very general analogue of Hadamard's determinant theorem.

1. Introduction. Let $A(x)$ be a polynomial of degree $n > 0$ with complex coefficients a_i and complex roots α_i, so that

$$A(x) = \sum_{i=0}^{n} a_i x^i = a_n \prod_{i=1}^{n} (x - \alpha_i). \tag{1}$$

We define $\mathrm{sep}(A)$, the *minimum root separation* of A, by

$$\mathrm{sep}(A) = \min_{\alpha_i \neq \alpha_k} |\alpha_i - \alpha_k|, \tag{2}$$

with the convention that $\mathrm{sep}(A) = \infty$ in case A has only one distinct root.

The computing times required by known algorithms for isolating the zeros of A depend inversely on $\mathrm{sep}(A)$. Hence, we are interested in easily computable functions $f(a_0, \cdots, a_n)$ of the coefficients such that

$$0 < f(a_0, \cdots, a_n) \leqq \mathrm{sep}(A). \tag{3}$$

Heindel [3], in analyzing the computing time of an algorithm based on Sturm's theorem for isolating the real zeros of any polynomial with integer coefficients, used a weak lower bound for $\mathrm{sep}(A)$ due to Collins. Pinkert [9], presents an analogous algorithm for isolating all zeros, real and complex, of any polynomial with Gaussian integer coefficients. His algorithm is based on Sturm's theorem and the Routh-Hurwitz theorem and uses a stronger lower bound for $\mathrm{sep}(A)$, obtained more recently by Collins. Horowitz, using another simpler approach, has recently obtained a third lower bound, intermediate in strength, but just slightly weaker than the stronger bound of Collins. In the following, these three bounds are all derived, with the hope of stimulating further research on the problem.

Received April 16, 1973.

AMS (MOS) subject classifications (1970). Primary 12D10.

Key words and phrases. Polynomial zeros, root separation, Hadamard's theorem, seminorms.

* This research was supported by National Science Foundation Grants GJ-30125X and GJ-33169, by the Wisconsin Alumni Research Foundation, and (in part) by the Advanced Research Projects Agency of the Office of the Secretary of Defense (SD-183).

If $A(x)$ has rational complex coefficients, we can easily compute another polynomial, having the same roots, with Gaussian integer coefficients. Further, if $A(x)$ has Gaussian integer coefficients, we can easily compute another polynomial $A^*(x)$ with Gaussian integer coefficients, having the same roots as $A(x)$ and having only simple roots, namely

$$A^*(x) = A(x)/\gcd(A(x), A'(x)), \tag{4}$$

where $A'(x)$ is the derivative of $A(x)$ and "gcd" denotes the greatest common divisor. Hence, in the following, A is assumed to have Gaussian integer coefficients and no multiple roots.

Also, the three lower bounds to be obtained will all be of the form

$$0 < g(n, d) \leqq \operatorname{sep}(A), \tag{5}$$

where $n = \deg(A)$, the degree of A, and $d = \nu(A)$, where ν is some "seminorm". In the next section, we introduce the notion of a seminorm for a ring and then derive some lemmas which will be used in deriving the root separation theorems.

2. Seminorms and Resultants. If $\mathfrak{R}$ is any commutative ring, a seminorm for $\mathfrak{R}$ is any function ν from $\mathfrak{R}$ into the nonnegative real numbers satisfying the following three conditions for all $a, b \in \mathfrak{R}$:

$$\nu(a) = 0 \quad \text{if and only if } a = 0, \tag{6a}$$

$$\nu(a - b) \leqq \nu(a) + \nu(b), \tag{6b}$$

$$\nu(ab) \leqq \nu(a)\nu(b). \tag{6c}$$

These conditions imply also

$$\nu(-a) = \nu(a), \tag{6d}$$

$$\nu(a + b) \leqq \nu(a) + \nu(b). \tag{6e}$$

A *norm* for $\mathfrak{R}$ is a seminorm for $\mathfrak{R}$ such that

$$\nu(ab) = \nu(a)\nu(b). \tag{7}$$

For the ring G of the Gaussian integers, a familiar norm is $\nu(a + bi) = |a + bi| = (a^2 + b^2)^{1/2}$. A seminorm for G which is not a norm is $\nu(a + bi) = |a + bi|_1 = |a| + |b|$.

Any seminorm ν on a commutative ring $\mathfrak{R}$ can be extended to a seminorm on the polynomial ring $\mathfrak{R}[x]$ by the definition

$$\nu\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \nu(a_i). \tag{8}$$

By induction on r, repeated application of (8) extends ν to a seminorm on $\mathfrak{R}[x_1, \cdots, x_r]$, which is easily seen to be independent of the order in which the indeterminates x_i are adjoined.

As a special case, (8) defines $|A|$ and $|A|_1$ for any *Gaussian polynomial* $A(x_1, \cdots, x_r) \in G[x_1, \cdots, x_r]$ as extensions of the seminorms for G defined above. For *integral polynomials* $A(x_1, \cdots, x_r)$ with rational integer coefficients, the norm $|A|_1$ has been

used extensively for the analysis of algebraic algorithms. See, for example, [1], [2], [7] and [8]. Its extension to Gaussian polynomials, however, is new.

If M is an arbitrary matrix (or vector) over $\mathfrak{R}$, we define

$$\nu(M) = \sum_i \sum_j \nu(M_{ij}), \tag{9}$$

where the summation extends over all entries of M. It is easy to verify that the conditions (6a)–(6c) hold for matrices over $\mathfrak{R}$ whenever the operations are defined. In particular, this extends ν to a seminorm for the ring of all n by n square matrices over $\mathfrak{R}$.

By combining the seminorm extensions for polynomials and matrices, we obtain the following general analogue of Hadamard's determinant theorem [6, p. 208].

THEOREM 1. *Let $\mathfrak{R}$ be a commutative ring, ν a seminorm for $\mathfrak{R}$, M an n by n matrix over $\mathfrak{R}$. Then*

$$\nu(\det(M)) \leqq \prod_{i=1}^{n} \nu(M_i) \tag{10}$$

where M_i is the ith row of M and $\det(M)$ is the determinant of M.

Proof. By induction on n, the case $n = 1$ being trivial. We denote by $M_{i,j}$ the element of M in the ith row and jth column of M, by $M_{i,j}'$ the submatrix of M obtained by deletion of the ith row and jth column. By Laplace expansion,

$$\det(M) = \sum_{j=1}^{n+1} (-1)^{j+1} M_{1j} \det(M_{1j}'). \tag{11}$$

By (6) and (11),

$$\nu(\det(M)) \leqq \sum_{j=1}^{n+1} \nu(M_{1j})\nu(\det(M_{1j}')). \tag{12}$$

The ith row of M_{1j}' is a subrow of M_{i+1}, so

$$\nu(\det(M_{1j}')) \leqq \prod_{i=2}^{n+1} \nu(M_i) \tag{13}$$

by the induction hypothesis. By (12) and (13),

$$\nu(\det(M)) \leqq \left\{\prod_{i=2}^{n+1} \nu(M_i)\right\} \sum_{j=1}^{n+1} \nu(M_{1j}). \tag{14}$$

Since $\sum_{j=1}^{n+1} \nu(M_{1j}) = \nu(M_1)$, this completes the induction. □

A corollary of Theorem 1, needed in Section 3, will now be obtained by consideration of certain submatrices of the Sylvester matrix of two polynomials, A and B, over $\mathfrak{R}$. Let $m = \deg(A)$, $n = \deg(B)$. The Sylvester matrix of A and B is the $m + n$ by $m + n$ matrix S whose successive rows are the coefficients of the polynomials $x^{n-1}A(x), \cdots, xA(x), A(x), x^{m-1}B(x), \cdots, xB(x), B(x)$. Diagrammatically, if

$$A(x) = \sum_{i=0}^{m} a_i x^i \quad \text{and} \quad B(x) = \sum_{i=0}^{n} b_i x^i,$$

then

$$S = \begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & & & \\ & a_m & a_{m-1} & & a_0 & & \\ & & \ddots & & & \ddots & \\ & & a_m & a_{m-1} & \cdots & & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & & & \\ & b_n & b_{n-1} & & b_0 & & \\ & & \ddots & & & \ddots & \\ & & b_n & b_{n-1} & \cdots & & b_0 \end{bmatrix}, \tag{15}$$

in which all missing entries are zero. By definition, the resultant of A and B, res(A, B), is the determinant of S.

THEOREM 2. *Let A and B be polynomials over a commutative ring $\mathfrak{R}$ with seminorm ν. Let $m = \deg(A) > 0$, $n = \deg(B) > 0$, $c = \operatorname{res}(A, B)$. Then*

$$\nu(c) \leqq \nu(A)^n \nu(B)^m. \tag{16}$$

Also, there exist polynomials U and V over $\mathfrak{R}$ such that $AU + BV = c$, $\deg(U) < n$, $\deg(V) < m$,

$$\nu(U) \leqq m\nu(A)^{n-1}\nu(B)^m, \tag{17}$$

and

$$\nu(V) \leqq m\nu(A)^n \nu(B)^{m-1}. \tag{18}$$

Proof. If S_i is the ith row of S then $\nu(S_i) = \nu(A)$ for $1 \leqq i \leqq n$ and $\nu(S_i) = \nu(B)$ for $n + 1 \leqq i \leqq m + n$, and (16) follows from Theorem 1. Now consider the matrix S^* which is obtained by adding to the last column of S x^{m+n-i} times the ith column of S, for $1 \leqq i < m + n$. $\det(S^*) = \det(S) = c$ and the last column of S^* contains the entries $x^{n-1}A(x)$, $\cdots$, $xA(x)$, $A(x)$, $x^{m-1}B(x)$, $\cdots$, $xB(x)$, $B(x)$. Applying the Laplace determinant expansion theorem to the last column of S^*, we obtain $AU + BV = c$ with $\deg(U) \leqq n - 1$ and $\deg(V) \leqq m - 1$, where the coefficients of U and V are the cofactors of the last column of S^*. Each coefficient of U is the determinant of a matrix obtained from S by deleting one row of coefficients of A and the last column, and so Theorem 1 yields (17), and, similarly, (18) holds. □

3. Root Separation Bounds. For each of the first two root separation bounds, we will use the following well-known upper bound on the roots of a polynomial.

THEOREM 3. *Let A be any nonzero Gaussian polynomial, and let α be a root of A. Then*

$$|\alpha| < |A|/|a_n| \tag{19}$$

where $a_n = \operatorname{ldcf}(A)$.

Proof. $|A| \geqq |a_n|$, so (19) holds for $|\alpha| < 1$. Let $A(x) = \sum_{i=0}^{n} a_i x^i$ and assume $|\alpha| \geqq 1$. Then $a_n\alpha^n = -\sum_{i=0}^{n-1} a_i\alpha^i$, so

$$|a_n| \cdot |\alpha|^n \leqq \sum_{i=0}^{n-i} |a_i| \cdot |\alpha|^i. \tag{20}$$

Dividing (20) by $|\alpha|^{n-1}$,

$$|a_n| \cdot |\alpha| \leqq \sum_{i=0}^{n-1} |a_i| \cdot |\alpha|^{i-n+1} \leqq \sum_{i=0}^{n-1} |a_i| < |A|, \tag{21}$$

from which (19) is immediate. □

THEOREM 4 (COLLINS, 1970). *Let A be a Gaussian polynomial of degree $n \geqq 2$ with only simple roots, and $d = |A|$. Then*

$$\operatorname{sep}(A) > (2d)^{-n(n-1)/2}. \tag{22}$$

Proof. Let $\alpha_1, \cdots, \alpha_n$ be the zeros of A and $\lambda = \operatorname{sep}(A)$. We may choose notation so that $\lambda = |\alpha_1 - \alpha_2|$. Let D be the discriminant of A, so that

$$D = a_n^{2n-2} \prod_{j<k} (\alpha_j - \alpha_k)^2, \tag{23}$$

and [10, Section 28], D is a Gaussian integer. Since the α_j are distinct, $D \neq 0$ and hence $|D| \geqq 1$. Combining this with (23), we have

$$1 \leqq |a_n|^{2n-2} \prod_{j<k} |\alpha_j - \alpha_k|^2. \tag{24}$$

Dividing by λ^2,

$$\lambda^{-2} \leqq |a_n|^{2n-2} \prod_{j<k;\,(j,k)\neq(1,2)} |\alpha_j - \alpha_k|^2. \tag{25}$$

There are $(n^2 - n - 2)/2$ factors $|\alpha_j - \alpha_k|^2$ in (25) and $|\alpha_j - \alpha_k| \leqq |\alpha_j| + |\alpha_k| < 2d/|a_n|$ by Theorem 3. Hence,

$$\lambda^{-2} \leqq (2d)^{n^2-n-2}/|a_n|^{n^2-3n}. \tag{26}$$

Now, $n^2 - 3n + 2 \geqq 0$ and $|a_n| \geqq 1$ so

$$\lambda^{-2} \leqq (2d)^{n^2-n-2} |a_n|^2 < (2d)^{n^2-n}, \tag{27}$$

from which (22) is immediate. □

THEOREM 5 (HOROWITZ, 1973). *Let A be a Gaussian polynomial of degree $n \geqq 2$ with only simple roots, and $d = |A|$. Then*

$$\operatorname{sep}(A) \geqq (nd)^{-4n+5}. \tag{28}$$

Proof. Let $\alpha_1, \cdots, \alpha_n$ be the zeros of A and $\lambda = \operatorname{sep}(A)$. We may suppose that $\lambda = |\alpha_1 - \alpha_2|$. By Theorem 2, there exist Gaussian polynomials U and V such that

$$AU + A'V = c, \tag{29}$$

$\deg(U) \leqq n - 2$ and $\deg(V) \leqq n - 1$, where $c = \operatorname{res}(A, A')$. Since $A(x) = a_n \prod_{i=1}^{n} (x - \alpha_i)$, we have

$$A'(x) = a_n \sum_{j=1}^{n} \prod_{1 \leqq i \leqq n;\, i \neq j} (x - \alpha_i). \tag{30}$$

Evaluating (30) at $x = \alpha_1$, we obtain

$$A'(\alpha_1) = a_n \prod_{i=2}^{n} (\alpha_1 - \alpha_i). \tag{31}$$

Hence, evaluating (29) at $x = \alpha_1$ and using (31),

$$\left\{a_n \prod_{i=2}^{n} (\alpha_1 - \alpha_i)\right\} V(\alpha_1) = c. \tag{32}$$

By [10, Section 28], $c = a_n D$, where D is the discriminant of A, a nonzero Gaussian integer. Hence, $V(\alpha_1) \neq 0$ and, by (32),

$$\text{sep}(A) = D/V(\alpha_1) \prod_{i=3}^{n} (\alpha_1 - \alpha_i). \tag{33}$$

$|A'| \leqq n|A|$ so

$$|V| \leqq n^n d^{2n-2} \tag{34}$$

by Theorem 2. Since $\deg(V) \leqq n - 1$ and $|\alpha_1| < d$,

$$|V(\alpha_1)| \leqq |V| \cdot d^{n-1} \leqq n^n d^{3n-3}. \tag{35}$$

From (33) and (35), using $|D| \geqq 1$ and $|\alpha_1 - \alpha_i| < 2d$,

$$\text{sep}(A) \geqq 2^{-n+2} n^{-n} d^{-4n+5}. \tag{36}$$

The proof is completed by observing that $n \geqq 2$. □

In order to obtain the third root separation bound, we construct a Gaussian polynomial B^* whose roots are all the differences $\alpha_i - \alpha_j$ with $i \neq j$. The idea of constructing B^* as a resultant was suggested by some current research of R. Loos [5]. After obtaining upper bounds for the coefficients of B^*, we will apply the following well-known theorem to obtain a lower bound for the roots of B^*, and hence for sep(A).

THEOREM 6. *Let $A(x) = \sum_{i=0}^{n} a_i x^i$ be a complex polynomial of degree $n > 0$, with $a_0 \neq 0$. If α is any root of A, then*

$$|\alpha| > \tfrac{1}{2} \min_{1 \leqq i \leqq n;\, a_i \neq 0} |a_0/a_i|^{1/i}. \tag{37}$$

Proof. Let $A^*(x) = x^n A(x^{-1}) = \sum_{i=0}^{n} a_{n-i} x^i$. A^* is a polynomial of degree n whose roots are the reciprocals of the roots of A, for

$$A^*(x) = a_n x^n \prod_{i=1}^{n} (x^{-1} - \alpha_i) = a_n \prod_{i=1}^{n} (1 - \alpha_i x)$$

$$= \left\{a_n \prod_{i=1}^{n} (-\alpha_i)\right\}\left\{\prod_{i=1}^{n} (x - \alpha_i^{-1})\right\} = a_n(a_0/a_n) \prod_{i=1}^{n} (x - \alpha_i^{-1}) = a_0 \prod_{i=1}^{n} (x - \alpha_i^{-1}).$$

Hence, $A^*(\alpha^{-1}) = 0$ and, from [4, Exercise 4.6.2.20], we have

$$|\alpha^{-1}| < 2 \max_{1 \leqq i \leqq n} |a_i/a_0|^{1/i}, \tag{38}$$

from which (37) is immediate. □

THEOREM 7 (COLLINS, 1973). *Let A be a Gaussian polynomial of degree $n \geqq 2$ with only simple roots and $d = |A|$. Then*

$$\text{sep}(A) > \tfrac{1}{2}(e^{1/2} n^{3/2} d)^{-n}, \tag{39}$$

where e is the base of the natural logarithm.

Proof. Let $B(x)$ be the resultant of $A(y)$ and $A(x + y)$. If the coefficients and roots of A are given by (1), then,

$$A(x + y) = a_n \prod_{j=1}^{n} (y - (\alpha_j - x)). \tag{40}$$

Expressing the resultant $B(x)$ as a symmetric function of the roots of $A(y)$ and $A(x + y)$ by the theorem of van der Waerden [10, Section 28],

$$B(x) = a_n^{2n} \prod_{1 \leq i, j \leq n} (x - (\alpha_i - \alpha_j)). \tag{41}$$

Since $\alpha_i = \alpha_j$ if and only if $i = j$, $B(x) = x^n \bar{B}(x)$, where

$$\bar{B}(x) = a_n^{2n} \prod_{i \neq j} (x - (\alpha_i - \alpha_j)), \tag{42}$$

is a polynomial of degree $n(n - 1)$ with $\bar{B}(0) \neq 0$. Also, (42) can be written in the form

$$\bar{B}(x) = a_n^{2n} \prod_{i<j} (x^2 - (\alpha_i - \alpha_j)^2), \tag{43}$$

so that, if $\bar{B}(x) = \sum_{i=0}^{n(n-1)} b_i x^i$, then $b_i = 0$ for i odd.

Expanding $A(x + y)$ in a Taylor series,

$$A(x + y) = \sum_{i=0}^{n} \{A^{(i)}(y)/i!\} x^i, \tag{44}$$

where $A^{(i)}$ is the ith derivative of A. Let

$$A^*(x, y) = \{A(x + y) - A(y)\}/x = \sum_{i=1}^{n} \{A^{(i)}(y)/i!\} x^{i-1}. \tag{45}$$

Let M be the Sylvester matrix of $A(y)$ and $A(x + y)$. If we subtract the ith row of M from the $(n + i)$th row and then divide the latter by x, for $1 \leq i \leq n$, we obtain a matrix $\bar{M}$ such that $\det(M) = x^n \det(\bar{M})$. The first column of $\bar{M}$ contains a_n in the first row and zeros elsewhere. Hence, $\det(\bar{M}) = a_n \det(M^*)$, where M^* results from $\bar{M}$ upon deletion of its first row and column. But M^* is the Sylvester matrix of $A(y)$ and $A^*(x, y)$, so

$$\bar{B}(x) = a_n B^*(x) \tag{46}$$

where $B^*(x)$ is the resultant of $A(y)$ and $A^*(x, y)$.

We now proceed to obtain bounds for the coefficients of B^*. Let

$$A_k^*(x, y) = \sum_{i=1}^{k+1} \{A^i(y)/i!\} x^{i-1}, \tag{47}$$

so that $A_k{}^*$ is the result of deleting from A^* all terms of degree $k + 1$ or greater in x. Since A^* and $A_k{}^*$ are both of degree $n - 1$ in y, $B^*(x) \equiv B_k{}^*(x)$ (modulo x^{k+1}) for $k \geq 0$. Hence, the coefficients of x^k in $B^*(x)$ and $B_k{}^*(x)$ are identical, and, if $B^*(x) = \sum_{i=0}^{n(n-1)} b_i{}^* x^i$, then

$$|b_k^*| \leq |B_k^*|. \tag{48}$$

Now, $|A^{(i)}(y)/i!| \leq \binom{n}{i} d$, so, by (47),

$$|A_k^*(x, y)| \leq \sum_{i=1}^{k+1} \binom{n}{i} d \leq e n^{k+1} d. \tag{49}$$

By Theorem 2 and (49),

$$|B_k^*| \leqq e^n n^{(k+1)n} d^{2n-1}. \tag{50}$$

By (48) and (50), together with $|b_0^*| \geqq 1$,

$$|b_0^*/b_{2k}^*|^{1/2k} \geqq e^{-n/2} n^{-3n/2} d^{-n+1/2} \tag{51}$$

for $k \geqq 1$. Since $b_i^* = 0$ for i odd, by Theorem 6,

$$|\alpha_i - \alpha_j| > \tfrac{1}{2}(e^{1/2} n^{3/2} d)^{-n}, \tag{52}$$

completing the proof. □

The computing time of Pinkert's algorithm in [9] for isolating the zeros of a Gaussian polynomial A is dominated (in the sense of [2]) by a polynomial function of $n = \deg(A)$, $\log d$ where $d = |A|$, and $\log \lambda^{-1}$ where $\lambda = \operatorname{sep}(A)$. Specifically, $n^7(\log d\lambda^{-1})(\log nd\lambda^{-1})^2$ is derived by Pinkert as a dominating function. If "$\sim$" denotes codominance of functions as in [2] and if $C_1(n, d)$, $H(n, d)$ and $C_2(n, d)$ are the bounds on $\operatorname{sep}(A)$ given by Theorems 4, 5 and 7, then we have

$$\log C_1(n, d)^{-1} \sim n^2 \log d, \tag{53}$$

whereas

$$\log H(n, d)^{-1} \sim \log C_2(n, d)^{-1} \sim n \log nd. \tag{54}$$

Thus, although $C_2(n, d)$ is generally a much sharper bound than $H(n, d)$, the use of either yields $n^{10}(\log nd)^3$ as a dominating function for the computing time of Pinkert's algorithm.

When $n = 2$, $\operatorname{sep}(A)$ can be given explicitly. If $A(x) = ax^2 + bx + c$ has two distinct roots, then

$$\operatorname{sep}(A) = |b^2 - 4ac|^{1/2}/|a|. \tag{55}$$

Also, by Theorem 4, $\operatorname{sep}(A) > 1/2d$. Let $a = k$, $b = 2k - 1$ and $c = k - 1$ with $k \geqq 1$. Then $d = |A| = 4k - 2$ and $\operatorname{sep}(A) = 1/k < 4/(4k - 2) = 4/d$.

Define

$$L(n, d) = \min\{\operatorname{sep}(A) : \deg(A) = n \;\&\; |A| \leqq d\}. \tag{56}$$

Then, we have just shown,

$$L(2, d) \sim d^{-1}. \tag{57}$$

It does not seem unreasonable to ask for an explicit relation such as (57) for $L(3, d)$, but we have thus far not succeeded with this apparently simple problem. We know only, by Theorem 7 and some obvious examples, that

$$d^{-3} \leq L(3, d) \leq d^{-1}, \tag{58}$$

where "$\leq$" is the dominance relation.

Computer Sciences Department
University of Wisconsin
Madison, Wisconsin 53706

Computer Science Program
University of Southern California
Los Angeles, California 90007

1. G. E. COLLINS, "Computing time analyses for some arithmetic and algebraic algorithms," *Proc. 1968 Summer Institute on Symbolic Mathematical Computation*, IBM Corp., Cambridge, Mass., 1961, pp. 197–231.

2. G. E. COLLINS, "The calculation of multivariate polynomial resultants," *J. Assoc. Comput. Mach.*, v. 18, 1971, pp. 515–532. MR **45** #7970.

3. L. E. HEINDEL, "Integer arithmetic algorithms for polynomial real zero determination," *J. Assoc. Comput. Mach.*, v. 18, 1971, pp. 533–548. MR **45** #9480.

4. D. E. KNUTH, *The Art of Computer Programming*. Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969. MR **44** #3531.

5. R. G. K. LOOS, "A constructive approach to algebraic numbers," *Math. of Comp.* (submitted.)

6. H. MINC & M. MARCUS, *Introduction to Linear Algebra*, Macmillan, New York, 1965. MR **32** #5660.

7. M. T. MCCLELLAN, "The exact solution of systems of linear equations with polynomial coefficients," *J. Assoc. Comput. Mach.*, v. 20, 1973, pp. 563–588.

8. D. R. MUSSER, *Algorithms for Polynomial Factorization*, Univ. of Wisconsin Comp. Sci. Dept. Technical Report No. 134 (Ph.D Thesis), Sept. 1971, 174 pp.

9. J. R. PINKERT, *Algebraic Algorithms for Computing the Complex Zeros of Gaussian Polynomials*, Univ. of Wisconsin Comp. Sci. Dept. Ph.D. Thesis, May 1973, Technical Report No. 188, July 1973.

10. B. L. VAN DER WAERDEN, *Moderne Algebra*. Vol. I, Springer, Berlin, 1930; English transl., Ungar, New York, 1949. MR **10**, 587.