# Fast Probabilistic Algorithms for Verification of Polynomial Identities

J. T. SCHWARTZ

*New York University, New York, New York*

ABSTRACT The startling success of the Rabin–Strassen–Solovay primality algorithm, together with the intriguing foundational possibility that axioms of randomness may constitute a useful fundamental source of mathematical truth independent of the standard axiomatic structure of mathematics, suggests a vigorous search for probabilistic algorithms In illustration of this observation, various fast probabilistic algorithms, with probability of correctness guaranteed a priori, are presented for testing polynomial identities and properties of systems of polynomials. Ancillary fast algorithms for calculating resultants and Sturm sequences are given. Probabilistic calculation in real arithmetic, previously considered by Davis, is justified rigorously, but only in a special case. Theorems of elementary geometry can be proved much more efficiently by the techniques presented than by any known artificial-intelligence approach

KEY WORDS AND PHRASES: polynomials, polynomial algorithms, probabilistic algorithms

CR CATEGORIES. 5.21, 5.7

## 1. *Integer Probabilistic Calculations for Multivariate Polynomials*

The startling success of the Rabin–Strassen–Solovay algorithm (see Rabin [17]), together with the intriguing foundational possibility that axioms of randomness may constitute a useful fundamental source of mathematical truth independent of, but supplementary to, the standard axiomatic structure of mathematics (see Chaitin and Schwartz [3]), suggests that probabilistic algorithms ought to be sought vigorously. As an illustration of what may be possible, this paper presents probabilistic algorithms for testing asserted multivariable polynomial identities $Q = R$, as well as other asserted or conjectured relationships between sets of polynomials, e.g., the assertion that one polynomial $Q$ belongs to the ideal generated by finitely many others.

The technique that we use is essentially elementary. Given a purported polynomial identity, we can always write it as $Q = 0$. We do not suppose that the $Q$ presented to us for testing is given in standard simplified polynomial form. For example, if we did not immediately recognize its truth, we might wish to test the identity $(x + y)(x - y) - x^2 + y^2 = 0$. Indeed, if we write $\hat{Q}$ for the standard simplified form of $Q$, what we want is precisely a test to determine whether all the coefficients of $\hat{Q}$ are zero.

We allow our polynomials to have coefficients in any field or integral domain $F$. At some points in our argument the condition that $F$ should be infinite will play an essential role. We write $\deg(Q)$ for the degree of $Q$ and $|S|$ for the cardinality of a set $S$.

Note that it will generally be trivial to develop upper bounds for $\deg(Q)$ directly from the expression structure of $Q$.



Author's address: Computer Science Department, Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY 10012.

This work was supported in part by the National Science Foundation under Grant MCS-76-00116 and in part by the U.S. Department of Energy under Contract EY-76-C-02-3077.

LEMMA 1. *Suppose that $Q$ is a polynomial in the variables $x_1, \dots, x_n$ and that $Q$ is not identically zero. Let $Q_1$ be the standard simplified form of $Q$. Let $d_1$ be the degree of $Q_1$ in $x_1$ and $Q_2$ the coefficient of $x_1^{d_1}$ in $Q_1$. Then, inductively, let $d_j$ be the degree of $Q_j$ in $x_j$ and $Q_{j+1}$ the coefficient of $x_j^{d_j}$ in $Q_j$. This defines $d_j$ and $Q_j$ for $j = 1, \dots, n$. For $1 \le j \le n$, let $I_j$ be any set of elements in the domain or field $F$ of coefficients of $Q$. Then in the set $I_1 \times \cdots \times I_n$, $Q$ has at most*

$$|I_1 \times \cdots \times I_n| \left( \frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|} \right) \tag{1}$$

*zeros.*

PROOF. The case $n = 1$ is obvious, since a nonzero polynomial of degree $d$ can have at most $d$ zeros, and we proceed by induction on $n$, supposing the asserted result to be true for $Q_2$, which is a polynomial in $n - 1$ variables. If $(z_2, \dots, z_n)$ is a zero of $Q_2$, then $Q_1(x_1, z_2, \dots, z_n)$ might be zero for all $x_1$. Otherwise $Q_1(x_1, z_2, \dots, z_n)$ has at most $d_1$ zeros in $I_1$. Thus the total number of zeros of $Q_1$ in $I_1 \times \cdots \times I_n$ is bounded by

$$|I_1| \cdot |I_2 \times \cdots \times I_n| \left( \frac{d_2}{|I_2|} + \cdots + \frac{d_n}{|I_n|} \right) + d_1 \cdot |I_2 \times \cdots \times I_n|$$

$$= |I_1 \times \cdots \times I_n| \left( \frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|} \right). \qquad \text{Q.E.D.}$$

COROLLARY 1. *Let $I = I_1 = \cdots = I_n$, and let $|I| \ge c \deg(Q)$. Then if $Q$ is not identical to zero, the number of elements of $I \times \cdots \times I$ which are zeros of $Q$ is at most $c^{-1}|I|^n$.*

PROOF. In this case $\sum d_i/|I| \le \deg(Q)/|I| \le c^{-1}$. Q.E.D.

We can therefore test a purported identity $Q \equiv 0$ by the following probabilistic procedure. Choose $I$ such that $|I| \ge C \deg(Q)$ with $C$ significantly greater than 1, e.g., $C = 2$. Let $N$ be such that $C^{-N}$ is small enough, e.g., $< 2^{-400}$, and then select $N$ elements $y = (y_1, \dots, y_n)$ from $I \times \cdots \times I$ at random. If any one of these $y$ is not a zero of $Q$, then $Q$ is not identically equal to zero. If all are zeros of $Q$, then $Q$ is very probably equal to zero identically. For a rigorous discussion of the term "very probably" which appears here, see Chaitin and Schwartz [3].

Polynomials with integer coefficients will interest us particularly. In dealing with such polynomials, we will want to avoid having to deal with very large integers. To avoid this, we can adapt the standard technique of carrying out all calculations in modular arithmetic. This suggests the following definition.

*Definition* 1. Let $Q = Q(x_1, \dots, x_n)$ be an $n$-parameter integer-coefficient polynomial. Then

(a) A *modular zero* of $Q$ is an $(n + 1)$-tuple $(i_1, \dots, i_n, p)$ of integers, the last integer $p$ being prime, such that $Q(i_1, \dots, i_n) \equiv 0 \pmod{p}$.

(b) We write $\operatorname{maxv}(Q, k)$ for the maximum absolute value which $Q$ can assume on the rectangle $|x_j| \le k, j = 1, \dots, n$.

Note that it will generally be easy to develop an upper bound for $\operatorname{maxv}(Q, k)$ directly from the expression structure of $Q$.

LEMMA 2. *Let the hypotheses of Lemma* 1 *be satisfied. Suppose in addition that the coefficients of $Q$ are integers, that $I = I_1 = I_2 = \cdots = I_n = \{i \mid -k \le i \le k\}$, and that $L = \operatorname{maxv}(Q, k)$. Let $J$ be any finite set of primes, and suppose that the product of any $m + 1$ of the primes in $J$ exceeds $L$. Then in the set $I_1 \times \cdots \times I_n \times J$, $Q$ has at most*

$$|I_1 \times \cdots \times I_n \times J| \left( \frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|} + \frac{m}{|J|} \right) \tag{2}$$

*modular zeros.*

PROOF. Let $(i_1, \ldots, i_n) \in I_1 \times \cdots \times I_n$. If $Q(i_1, \ldots, i_n) = 0$, then $(i_1, \ldots, i_n, p)$ is a modular zero of $Q$ for every $p \in J$. Otherwise $|Q(i_1, \ldots, i_n)| \leq L$, but is nonzero. In this case it is impossible for $Q(i_1, \ldots, i_n)$ to have more than $m$ prime factors in $J$. Thus by Lemma 1 the total number of modular zeros of $Q$ in $I_1 \times \cdots \times I_n \times J$ is bounded by

$$|J| \cdot |I_1 \times \cdots \times I_n| \left(\frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|}\right) + m|I_1 \times \cdots \times I_n|$$

$$= |I_1 \times \cdots \times I_n \times J| \left(\frac{d_1}{|I_1|} + \cdots + \frac{d_n}{|I_n|} + \frac{m}{|J|}\right). \qquad \text{Q.E.D.}$$

COROLLARY 2. *Let $2k + 1 \geq c \cdot deg(Q)$, and suppose that the product of the $c^{-1}|J| + 1$ smallest primes in $J$ exceeds $maxv(Q, k)$. Then if $Q$ is not identically equal to zero, the number of elements of $I_1 \times \cdots \times I_n \times J$ which are modular zeros of $Q$ is at most $2c^{-1}|I|^n|J|$.*

Corollary 2 allows us to carry out the probabilistic tests for $Q = 0$ in modular arithmetic. The computations necessary for each test can be carried out at almost full arithmetic speed on a $b$-bit computer by programming in the following style. Keep a table of all the primes in $J$, and for each such prime record the value of $2^b \bmod p$. Then use the ordinary arithmetic operations as long as no overflow occurs, but whenever a quantity overflowing single precision is encountered, reduce modulo $p$. The set $J$ and the quantity $k$ of Corollary 2 can be chosen to minimize the number of computations needed to verify a given identity to within some prescribed probability, e.g., $10^{-100}$.

As an example, consider the problem of verifying Vandermonde's identity,

$$\begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i<j} (x_i - x_j), \tag{3}$$

for some fixed but substantial value of $n$, say $n = 100$. The polynomials appearing in this case are of total degree roughly 5000. (Thus simplification by direct expansion is hopeless, since roughly $2^{5000}$ terms would appear on the right.) Suppose that we choose the $x_j$ at random in the range $|x_j| \leq 250{,}000$, and let $J$ be the set of primes extending from the $M$th to the $2M$th prime, where $(M \log M)^{M/100} \geq \text{maxv}(Q, 250{,}000)$, $Q$ being the difference between the left and right sides of (3). Then by Corollary 2 a fractional part at most equal to $2 \times 10^{-2}$ of the elements of $I_1 \times \cdots \times I_n \times J$ are modular zeros of $Q$ if $Q$ is not identically equal to zero. Thus, to guarantee the desired probabilistic accuracy $10^{-100}$, 60 random tests will be sufficient. Using Hadamard's determinant inequality (see Dunford and Schwartz [7, p. 1018]) to bound the left side of the equation, an upper bound of $10^{100} \cdot (2.5 \times 10^5)^{5000} \leq 10^{27{,}100}$ can easily be set for $Q$. Thus the value $M = 1/2 \times 10^6$ is sufficient, and we make our selection of a prime $p$ at random from among all primes from $P_{500{,}000}$ to $P_{1{,}000{,}000}$. The determinant in (3) can be calculated modulo $p$ by Strassen's method; at any rate, $10^8$ is a rough upper bound on the number of arithmetic operations required. (For efficiency, these operations should be compiled and executed rather than interpreted.) On a reasonably fast computer these computations should take about 3 minutes.

The polynomial identity verification technique that we have outlined extends immediately to rational functions. Suppose that we are given a function $R$ expressed in terms of the three operations of multiplication, subtraction, and division, but not reduced to the standard quotient-of-polynomials form $R = Q_1/Q_2$. The degree of the numerator and denominator of this standard-form representation can be bounded easily by examination of the structure of $R$, and upper bounds for $Q_1$, $Q_2$ in any numerical range $|x_i| \leq k$ can easily be set. Hence we can proceed as in the polynomial case. Divisions modulo $p$ will of course pose no problem. Denominators equal to zero should be noted, and any test in which such a denominator has occurred should be bypassed. The probability that a denominator not equal to zero ever appears as zero in a modular test can be kept low by choosing the $k$ and $J$ of Lemma 2 appropriately, so that expressions $R$ not involving excessively many divisions can be handled without difficulty. Any denominator which

appears as zero in too many tests is very probably equal to zero and calls the definition of the rational function $R$ into question.

Other properties of polynomials and rational functions can be tested by much the same technique. To test for constancy, linearity, etc., we can form differences of $Q$ and test to see if they are identically zero. To test a pair $Q_1$, $Q_2$ of polynomials for the relationship $Q_1 \mid Q_2$ of divisibility we can proceed as follows. Substitute random values for the parameters $x_2, \ldots, x_n$ of $Q_1$, $Q_2$; calculate modulo a random prime, and simplify both polynomials in the remaining parameter $x_1$ to $Q_1^* = C_{d_1}x_1^{q_1} + \cdots + C_0$ and $Q_2^* = \tilde{C}_{d_2}x_1^{q_2} + \cdots + \tilde{C}_0$. Divide $Q_2^*$ by $Q_1^*$. If $Q_1^* \mid Q_2^*$, this must give a zero remainder. If the remainder calculated in this way is zero for enough random choices, we will have verified that the remainder of $Q_1 \mid Q_2$, calculated by regarding $Q_1$ and $Q_2$ as polynomials in $x_1$ with coefficients in the field of rational functions of $x_2, \ldots, x_n$, is zero. But then we can write

$$R_1(x_2 \cdots x_n)Q_2(x_1 \cdots x_n) = A_1(x_1, \ldots, x_n)Q_1(x_1, \ldots, x_n) \tag{4}$$

for some polynomials $A_1$ and $R_1$. Proceeding in the same way for each of the other variables, we see that there exist polynomials $A_j(x_1, \ldots, x_n)$, $R_j(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$ such that $R_jQ_2 = A_jQ_1$ for all $j$. But then $A_1R_j = A_jR_1$ for all $j$. Any common prime factor of $R_1$ and $R_2$ must clearly be independent of both $x_1$ and $x_2$, and from the preceding equation, any other factor of $R_1$ must divide $A_1$. Thus we can write $A_1 = \tilde{A}_1F_1$, $R_1 = \tilde{R}_1F_1$, where $\tilde{R}_1$ is independent of both $x_1$ and $x_2$. It follows that $\tilde{R}_1Q_2 = \tilde{A}_1Q_1$. Replacing $A_1$, $R_1$ by $\tilde{A}_1$, $\tilde{R}_1$ and repeating this argument, we eventually find that $Q_1 \mid Q_2$.

The problem of determining whether $Q_1 \mid Q_2^k$ for some integer $k$ generalizes the polynomial divisibility problem in a significant way, since this is equivalent to the condition that the algebraic manifold $V(Q_1)$ of zeros of $Q_1$ is a subset of the manifold $V(Q_2)$ of zeros of $Q_2$. Moreover, $Q_1 \mid Q_2^k$ if and only if every prime factor of $Q_1$ is a prime factor of $Q_2$. To test this condition, we can use the following sequence of purely rational calculations. Put $A_1 = Q_1$, $B_1 = Q_2$, regarding these as polynomials in $x_1$ with coefficients in the field of rational functions of $x_2, \ldots, x_n$. Then successively define

$$B_{j+1} = \mathrm{GCD}(A_j, B_j), \qquad A_{j+1} = A_j/B_{j+1}. \tag{5}$$

Since the degrees of the polynomials $A_j$ and $B_j$ are falling, this sequence must eventually stabilize with some $A_\infty$ and $B_\infty$. If $A_\infty$ is not of degree zero in $x_1$, then it is relatively prime to every prime factor of $B_1 = Q_2$. Thus the zeros of $A_\infty$ (in the field of algebraic functions of $x_1, \ldots, x_n$) are distinct from the zeros of $Q_2$. Returning to the space of complex variables, this means that $Q_1$ has zeros which are not zeros of $Q_2$, so that $Q_1 \mid Q_2^k$ is false. On the other hand, if $A_\infty$ is of degree zero in $x_1$, then we can write $Q_1 = A_\infty B_2 \cdots B_\infty$, and clearly each $B_j$ (if regarded as a polynomial in $x_1$ with coefficients which are rational functions of $x_2, \ldots, x_n$) is a factor of $Q_2$. Thus $Q_1 \mid Q_2^k$ if $Q_1$ and $Q_2$ are regarded as polynomials in $x_1$. It follows that in the domain of polynomials in all $n$ variables we have $Q_1 \mid Q_0Q_2^k$ for some $Q_0$ which is independent of $x_1$. Thus $Q_1/\mathrm{GCD}(Q_1, Q_2^k)$ is independent of $x_1$ for sufficiently large $k$. Proceeding in the same way for all the other variables, we can make probabilistic tests which verify that $Q_1/\mathrm{GCD}(Q_1, Q_2^k)$ is independent of $x_j$ for each $j$ and all sufficiently large $k$. But then clearly $Q_1 \mid Q_2^k$ for $k$ sufficiently large.

The sequence of GCD calculations and divisions just described can be performed probabilistically by evaluating $Q_1$ and $Q_2$ for randomly chosen $x_2, \ldots, x_n$ modulo random primes $p$ and simplifying to write the results as polynomials of standard form in $x_1$. Standard algorithms for polynomials in one variable can be used. Any computation leading to a polynomial of lower degree than those of the $Q_2$ calculated for other values of $x_2, \ldots, x_n$ can be dropped, since its leading coefficient has vanished "accidentally." The probability of this ever happening can be kept small by choosing places of evaluation and primes from a sufficiently large range.

The general subject to which the preceding considerations belong, namely, the effective calculation of relationships between polynomials and between the sets of zeros of polynomials, has a very long history, which comes to a peak in Tarski [19]; see also Hermann

[11] and Seidenberg [18]. The classical approach to these questions is via the so-called *elimination theory*. See van der Waerden [20] for an account of this theory and for various algebraic results which we shall use. The probabilistic technique suggested in the preceding pages serves to extend the practical reach of these classical methods a bit beyond what would otherwise be their limits. We shall now illustrate this point with a series of examples.

## 2. *Application of Elimination Theory*

Given a set of $m$ polynomials $Q_1, \ldots, Q_m$, we can form the algebraic manifold $V(Q_1, \ldots, Q_m)$ of their common zeros. The problem of determining the dimension of this manifold is an obvious generalization of the problem of testing a single identity $Q \equiv 0$. A systematic elimination-theoretic procedure for determining this dimension is described in van der Waerden [21]. This procedure is based on the calculation of polynomial resultants.

Let $Q$ and $\tilde{Q}$ be polynomials in a single variable $x$, having nominal degrees $d$, $\tilde{d}$, respectively. The *resultant* $R(Q, \tilde{Q})$ is the determinant of the linear transformation $T: f + x^{\tilde{d}}\tilde{f} \to \tilde{Q}f + Q\tilde{f}$ where $f, \tilde{f}$ are arbitrary polynomials of degree $d$, $\tilde{d}$, respectively, and where we regard $T$ as a transformation in the $(d + \tilde{d})$-dimensional linear space of polynomials of degree $d + \tilde{d} - 1$. A fundamental property of this determinant is that it vanishes if and only if $Q$, $\tilde{Q}$ either have a factor in common or both have leading zeros. Let $Q(x) = C_d x^d + \cdots C_0$ and $\tilde{Q}(x) = \tilde{C}_{\tilde{d}} x^{\tilde{d}} + \cdots + \tilde{C}_0$. Then $R(Q, \tilde{Q})$ is the $(d + \tilde{d}) \cdot (d + \tilde{d})$-dimensional determinant,

$$\begin{vmatrix} C_d & \cdots & C_1 & C_0 & 0 & 0 & \cdots & 0 \\ 0 & C_d & \cdots & C_1 & C_0 & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & C_d & \cdots & C_1 & C_0 \\ \tilde{C}_{\tilde{d}} & \cdots & \tilde{C}_0 & 0 & 0 & & \cdots & 0 \\ 0 & \tilde{C}_{\tilde{d}} & \cdots & \tilde{C}_0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & \vdots \\ 0 & \cdots & 0 & 0 & \tilde{C}_{\tilde{d}} & \cdots & & \tilde{C}_0 \end{vmatrix} \tag{6}$$

where $d$ rows contain coefficients $C_j$ and $d$ rows contain coefficients $\tilde{C}_j$. It is clear from (6) that

$$R(\tilde{Q}, Q) = (-1)^{\deg(Q)\deg(\tilde{Q})} R(Q, \tilde{Q}). \tag{7}$$

Suppose that $\deg(\tilde{Q}) \geq \deg(Q)$ and that $k \leq \deg(\tilde{Q}) - \deg(Q)$. Then by subtracting an appropriate upper row from each lower row in (6) we can see that $R(Q, \tilde{Q}) = R(Q, \tilde{Q} - x^k Q)$. Performing an appropriate expansion by minors, it follows that

$$R(Q, \tilde{Q}) = (L(Q))^{\deg(\tilde{Q}) - \deg(Q)} R(Q, \tilde{Q} // Q), \tag{8}$$

where $L(Q)$ denotes the leading coefficient of $Q$ and $\tilde{Q} // Q$ denotes the remainder after division of $\tilde{Q}$ by $Q$. By (7) and (8) we have

$$R(Q, \tilde{Q}) = (L(\tilde{Q}))^{\deg(Q) - \deg(\tilde{Q})} (-1)^{\deg(Q)} R(Q // \tilde{Q}, Q) \tag{9}$$

if $\deg(Q) \geq \deg(\tilde{Q})$. For the special case $\deg(Q) = 0$ we have

$$R(Q, \tilde{Q}) = (L(Q))^{\deg(\tilde{Q})} \quad \text{if} \quad \deg(Q) = 0. \tag{10}$$

Collins [4] uses relationships (8) and (9) repeatedly to calculate the resultant of a pair of polynomials, in this way obtaining an $n^2 \log n$ algorithm for resultant calculation, where $n = \deg(Q) + \deg(\tilde{Q})$. In view of the central role which the resultant plays in classical elimination theory, a more efficient technique for computing it is desirable, and we now show that the fast polynomial GCD algorithm of Moenck [14] (see also Aho et al. [1]) can be adapted to give an $n \log^2 n$ algorithm for resultant calculation. To this end, we make the following definition.

*Definition* 2. Let a pair of polynomials $w = [Q, \tilde{Q}]$ of degree $d$, $\tilde{d}$ with coefficients in a field or domain $F$ be given, and let $d = \max(d, \tilde{d})$. Write $Q // \tilde{Q}$ for the remainder of $Q$

upon division by $\tilde{Q}$. Then the *RQ-sequence* RQ($w$) is the sequence $t_i$, $i = d, d-1, \ldots, 0$, of triples

$$t_i = [[Q_i, \tilde{Q}_i], a_i, M_i], \tag{11}$$

defined as follows:

(1) $Q_i$, $\tilde{Q}_i$ are polynomials, $a_i$ is a quantity of $F$, $M_i$ is a $2 \times 2$ matrix of polynomials.
(2) $t_d = [[Q, \tilde{Q}], 1, I]$, where $I$ is the $2 \times 2$ identity matrix.
(3) $\max(\deg(Q_i), \deg(\tilde{Q}_i)) \geq i \geq \min(\deg(Q_i), \deg(\tilde{Q}_i))$ for $i > 0$.
(4a) $t_{i-1} = t_i$ if $\min(\deg(Q_i), \deg(\tilde{Q}_i)) < i$;
(4b) otherwise, if $\deg(Q_i) = i$, then (dropping remainders in all polynomial divisions) we have

$$t_{i-1} = [[Q_i, \tilde{Q}_i//Q_i], a_i(L(Q_i))^{\deg(\tilde{Q}_i)-\deg(Q_i)}, MM_i], \tag{12}$$

where

$$M = \begin{bmatrix} 1 & 0 \\ -\tilde{Q}_i/Q_i & 1 \end{bmatrix};$$

(4c) otherwise $\deg(\tilde{Q}_i) = i$, and then

$$t_{i-1} = [[Q_i//\tilde{Q}_i, \tilde{Q}_i], a_i(-1)^{\deg(\tilde{Q}_i)}L(\tilde{Q}_i)^{\deg(Q_i)-\deg(\tilde{Q}_i)}, MM_i], \tag{13}$$

where

$$M = \begin{bmatrix} 1 & -Q_i/\tilde{Q}_i \\ 0 & 1 \end{bmatrix}.$$

LEMMA 3. *Let $w = [Q, \tilde{Q}]$, $t_i$, etc., be as in the preceding definition. Then the sequence RQ($w$) has the following properties:*

(*i*) $[Q_i, \tilde{Q}_i] = M_i[Q, \tilde{Q}]$.
(*ii*) $deg(M_i) \leq d - max(deg(Q_i), deg(\tilde{Q}_i)) \leq d - i$.
(*iii*) $R(Q, \tilde{Q}) = a_iR(Q_i, \tilde{Q}_i)$.

PROOF. All this is clear for $i = d$. A step from $t_i$ to $t_{i-1}$ via (4a) of the preceding definition clearly preserves the validity of (i)–(iii). Now suppose that rule (4b) applies to the step from $t_i$ to $t_{i-1}$. Property (i) is clearly preserved. Moreover,

$$\begin{aligned} \deg(M_{i-1}) &\leq \deg(\tilde{Q}_i) - \deg(Q_i) + \deg(M_i) \\ &\leq \deg(\tilde{Q}_i) - \deg(Q_i) + d - \deg(\tilde{Q}_i) \\ &= d - \deg(Q_i) = d - \max(\deg(Q_{i-1}), \deg(\tilde{Q}_{i-1})). \end{aligned}$$

Concerning (iii), it follows by (8) and (12) that

$$\begin{aligned} R(Q, \tilde{Q}) &= a_iR(Q_i, \tilde{Q}_i) = a_i(L(Q_i))^{\deg(\tilde{Q}_i)-\deg(Q_i)}R(Q_i, \tilde{Q}_i//Q_i) \\ &= a_{i-1}R(Q_{i-1}, \tilde{Q}_{i-1}). \end{aligned}$$

The case in which rule (4c) applies to the step from $t_i$ to $t_{i-1}$ can be handled in much the same way. Q.E.D.

LEMMA 4. *Let $w = [Q, \tilde{Q}]$, $w^* = [Q^*, \tilde{Q}^*]$ be two pairs of polynomials. Suppose that $max(deg(Q), deg(\tilde{Q}), deg(Q^*), deg(\tilde{Q}^*)) = d$, and suppose that the terms of order not less than $d - 2i$ in $Q$, $\tilde{Q}$ agree with the corresponding terms in $Q^*$, $\tilde{Q}^*$. Then the first $i + 1$ terms of the sequence $RQ(w) = [t_d, t_{d-1}, \ldots]$ have precisely the same components $a_i$, $M_i$ as the corresponding terms $a_i^*$, $M_i^*$ of the sequence $RQ(w^*) = [t_d^*, t_{d-1}^*, \ldots]$.*

PROOF. This is clear for $i = 0$, and we use the same notation as in the preceding definition and lemma and proceed by induction. For $j = d - i$ we have $[Q_{j+1}, \tilde{Q}_{j+1}] = M_{j+1}w$, and similarly for $[Q_{j+1}^*, \tilde{Q}_{j+1}^*]$, so that $Q_{j+1}$, $\tilde{Q}_{j+1}$ agree with $Q_{j+1}^*$, $\tilde{Q}_{j+1}^*$ modulo terms of order $d - 2i + \deg(M_{j+1})$ at most. By Lemma 3(ii) it follows that $\deg(M_{j+1}) \leq d - j - 1 = i - 1$, so that $Q_{j+1}$, $\tilde{Q}_{j+1}$ agree with $Q_{j+1}^*$, $\tilde{Q}_{j+1}^*$ modulo terms of

order $d - i - 1 = j - 1$ at most. Thus if (4a) of the preceding definition applies to the step from $[Q_{j+1}, \tilde{Q}_{j+1}]$ to $[Q_j, \tilde{Q}_j]$, it also applies to the corresponding step from $[Q^*_{j+1}, \tilde{Q}^*_{j+1}]$, and in this case clearly $[a_i, M_i] = [a^*_i, M^*_i]$. Similarly, if (4b) applies to $[Q_{j+1}, \tilde{Q}_{j+1}]$, it also applies to $[Q^*_{j+1}, \tilde{Q}^*_{j+1}]$, and we have

$$\deg(Q_{i+1}) = i + 1,$$

$$a_j = a_{j+1}(L(Q_{j+1}))^{\deg(\tilde{Q}_{j+1}) - \deg(Q_{j+1})},$$

$$M_j = MM_{j+1} \qquad \text{where} \quad M = \begin{bmatrix} 1 & 0 \\ -\tilde{Q}_{j+1}/Q_{j+1} & 1 \end{bmatrix},$$

and similarly for $a^*_j, M^*_j$, so that $a_j = a^*_j$, $M_j = M^*_j$. The case in which (4c) of the preceding definition applies is handled in exactly the same way. Q.E.D.

Lemmas 3 and 4 justify the following resultant calculation algorithm.

(1) Calculate $a_{d-1}$ and $M_{d-1}$, which depend only on the two leading coefficients of $Q, \tilde{Q}$.

(2) Next, assuming recursively that a procedure for calculating $a_{d-i}(Q, \tilde{Q})$ and $M_{d-i}(Q, \tilde{Q})$ is available, calculate $a_{d-2i}$ and $M_{d-2i}$ (both are functions of $Q$ and $\tilde{Q}$) as follows:

(2a) Calculate $a_{d-i}$ and $M_{d-i}$.

(2b) Drop all but the first $d - 3i$ terms from $Q, \tilde{Q}$ to obtain polynomials, $Q^*, \tilde{Q}^*$, and then calculate $[Q^*_{d-i}, \tilde{Q}^*_{d-i}] = M_{d-i}[Q, \tilde{Q}]$ By Lemma 3(i) and (ii), $Q_{d-i}, \tilde{Q}_{d-i}$ agree with $Q^*_{d-i}, \tilde{Q}^*_{d-i}$ to within terms of order $d - 2i$.

(2c) Starting from the polynomials $Q^*_{d-i}, \tilde{Q}^*_{d-i}$, apply steps 2a and 2b recursively to calculate $a^*_{d-i} = a_{d-i}(Q^*_{d-i}, \tilde{Q}^*_{d-i})$ and $M^*_{d-i} = M_{d-i}(Q^*_{d-i}, \tilde{Q}^*_{d-i})$. By Lemma 4, these are the same as $a_{d-i}(Q_{d-i}, \tilde{Q}_{d-i})$ and $M_{d-i}(Q_{d-i}, \tilde{Q}_{d-i})$.

(2d) We can now put

$$M_{d-2i}(Q, \tilde{Q}) = M_{d-i}(Q_{d-i}, \tilde{Q}_{d-i})M_{d-i}(Q, \tilde{Q}) \tag{14}$$

and

$$a_{d-2i}(Q, \tilde{Q}) = a_{d-2i}(Q_{d-i}, \tilde{Q}_{d-i})a_{d-i}(Q, \tilde{Q}). \tag{15}$$

(2e) Repeated use of the relations (14) and (15) will give $M_{d-2^i}(Q, \tilde{Q})$ and $a_{d-2^i}(Q, \tilde{Q})$. If $d$ is not a power of 2, we multiply both $Q$ and $\tilde{Q}$ by a power $x^k$ of $x$ to make $\max(\deg(Q), \deg(\tilde{Q}))$ a power $2^r$ of 2. Then we calculate $[Q_0, \tilde{Q}_0] = M_0(Q, \tilde{Q})[Q, \tilde{Q}]$ It is then clear that $R(Q, \tilde{Q}) = a_{d-2^r}(L(x^{-k}Q_0))^{\deg(\tilde{Q}_0) - \deg(Q_0)}$ if $\deg(\tilde{Q}_0) \geq \deg(Q_0)$, etc.

Multiplication and division of polynomials of order $m$ can be accomplished in time $Km \log m$, where $K$ is a constant of proportionality. In the process that we have just described, polynomials of order at most $3 \cdot 2^i$ are multiplied and divided at the $i$th step. Thus the total time $T(m)$ required to calculate the resultant of two polynomials of degree $m$ satisfies $T(2m) \leq 2T(m) + Km \log m$ and has the estimate $T(m) \leq Km \log^2 m$.

Tarski [19] notes that by making use of Sturm's formula for the zeros of a real polynomial, the results of elimination theory can be carried over to the study of the sets of zeros of real algebraic polynomials. To do this efficiently, we need a fast algorithm for calculating the sequence of coefficients which occur in Sturm's formula. For the convenience of the reader, we restate this beautiful formula (see Bieberbach and Bauer [2, pp. 173 ff.]).

THEOREM 1 (STURM). *Let $R$ be a polynomial with real coefficients and suppose that $R$ has no multiple zeros, so that $R$ and $R' = dR/dx$ have no common factor. Put $R_1 = R_0$, $R_2 = R'$, and then form the sequence of quotients $Q_j$ and remainders $R_j$ defined by $Q_{j+1}/R_j$ with remainder $-R_{j+2}$, i.e.,*

$$R_j = R_{j+1} * Q_{j+1} - R_{j+2},$$

*where $\deg(R_{j+2}) < \deg(R_{j+1})$, until a nonzero constant $R_k$ is reached. Then the number of zeros of $R$ in an interval $[a, b]$ (whose endpoints are not zeros) is the difference $S(a) - S(b)$, where $S(x)$ is the number of changes of sign in the sequence $R_1(x), \ldots, R_{k-1}(x), R_k$.*

COROLLARY. *Let the hypotheses of the preceding theorem be satisfied, and let $ST(R)$ be the sequence $[r_1, \ldots, r_k]$ of leading coefficients of the polynomials $R_1, \ldots, R_k$. (We will*

*sometimes call this sequence the* Sturmian coefficient sequence *of R.) Then the number of real zeros of R is the number of sign changes in* $[r_1, \ldots, r_k]$ *minus the number of sign changes in* $[(-1)^{deg(R_1)}r_1, \ldots, (-1)^{deg(R_k)}r_k]$.

PROOF. This follows from Sturm's theorem if we let $b \to \infty$ and $a \to -\infty$ in that theorem. Q.E.D.

A fast algorithm for calculating ST($Q$) for any real polynomial $Q$ without multiple zeros can be developed in close analogy with the resultant algorithm that has been presented. We simply build up a sequence

$$t_i^* = [[Q_i, \tilde{Q}_i], n_i, M_i] \tag{16}$$

for $i = d, d-1, \ldots, 0$, where $d = \deg(Q')$ and

(1*) $Q_i$, $\tilde{Q}_i$ are polynomials, $n_i$ is an integer, and $M_i$ is a $2 \times 2$ matrix of polynomials.
(2*) $t_d^* = [[Q, Q'], 0, I]$, where $I$ is the $2 \times 2$ identity matrix.
(3*) $\max(\deg(Q_i), \deg(\tilde{Q}_i)) \geq i \geq \min(\deg(Q_i), \deg(\tilde{Q}_i))$.
(4a*) $t_{i-1}^* = t_i^*$ if $\min(\deg(Q_i), \deg(\tilde{Q}_i)) < i$;
(4b*) otherwise, if $\deg(Q_i) = i$, then

$$t_{i-1}^* = [[Q_i, -\tilde{Q}_i//Q_i], n_i + \delta, MM_i], \tag{17}$$

where

$$M = \begin{bmatrix} 1 & 0 \\ \tilde{Q}_i/Q_i & 1 \end{bmatrix}$$

and

$$\delta = \tfrac{1}{2}\left((1 - \operatorname{sign}(L(Q_i)/L(\tilde{Q}_i))) + (1 - (-1)^{\deg(Q_i)-\deg(\tilde{Q}_i)} \operatorname{sign}(L(Q_i)/L(\tilde{Q}_i)))\right);$$

(4c*) otherwise $\deg(\tilde{Q}_i) = i$, and then

$$t_{i-1}^* = [[-Q_i//\tilde{Q}_i, \tilde{Q}_i], n_i + \delta, MM_i], \tag{18}$$

where

$$M = \begin{bmatrix} 1 & -Q_i/\tilde{Q}_i \\ 0 & 1 \end{bmatrix},$$

and where $\delta$ is as above.

Lemmas 3 and 4 obviously carry over to the sequence $t_i^*$. If $d = \deg(Q')$ is not a power of 2, we multiply $Q$ by a quantity $x^k + C$ to make it a power of $Q$ and then calculate $t_0^*$ and, in particular, $n_0$ and $[Q_0, \tilde{Q}_0] = M_0[Q, Q']$. Assuming that $C$ is positive it is clear from Sturm's theorem that the number of real zeros of $Q$ is $n_0$ if $k$ is even and $n_0 - 1$ if $k$ is odd. As previously, the time $T(m)$ required for this calculation has the estimate $T(m) \leq Km \log^2 m$.

We now return to considering the problem of determining the dimension of the manifold $V(Q_1, \ldots, Q_m)$ of common zeros of a set of polynomials with constant coefficients. The classical technique for handling this problem and for testing the condition $V(Q) \supseteq V(Q_1, \ldots, Q_m)$ is based on Kronecker's method of elimination, (see van der Waerden [21, Ch. 9]). For the reader's convenience, we now summarize the main points of this technique.

(a) Let the degrees of the polynomials $Q_1, \ldots, Q_m$ be $d_1, \ldots, d_m$; suppose for the moment that only one variable $x$ is involved, and that the leading coefficient of $Q_1$ is nonzero. Then we can introduce a formal auxiliary variable $u$ and form the resultant

$$R(Q_1, Q_2 + Q_3 u + \cdots + Q_m u^{m-2}). \tag{19}$$

If regarded as an element in the field $F$ of rational functions of $u$, this expression vanishes (which is to say, vanishes identically in $u$) if and only if $Q_1$ and $Q_2 + Q_3 u + \cdots + Q_m u^{m-2}$

(regarded as polynomials with elements in this field) have a common factor. But this is the case if and only if $Q_1, \ldots, Q_n$ have a common factor, i.e., a common root in the algebraic closure ACF of the field generated by their coefficients. Thus, if we decompose (19) into separate powers of $u$, we will get a collection of expressions $\rho_j^{(m)}(Q_1, \ldots, Q_m)$, each a polynomial in the coefficients of $Q_1, \ldots, Q_m$, such that

$$\rho_j^{(m)}(Q_1, \ldots, Q_m) = 0 \qquad \text{for all } j \tag{20}$$

if and only if $Q_1, \ldots, Q_m$ have a common root in ACF. The collection of expressions $\rho_j^{(m)}(Q_1, \ldots, Q_m)$ is called the *resultant system* of $Q_1, \ldots, Q_m$.

(b) Next let $Q_1, \ldots, Q_m$ be polynomials in $n$ variables $x_1, \ldots, x_n$. We can regard $Q_1, \ldots, Q_m$ as polynomials in $x_1$ with coefficients in the ring $R(x_2, \ldots, x_n)$ of polynomials in the remaining coefficients and form the resultant system (20) of these polynomials. If we assume that the $x_1$ term of highest degree in $Q_1$ has a constant coefficient, then $x_2, \ldots, x_n$ satisfy the equations of the resultant system (20) if and only if the equations

$$Q_j(z, x_2, \ldots, x_n), \qquad j = 1, \ldots, m, \tag{21}$$

have a solution $z$ (in the algebraic closure ACF of the field generated by all the coefficients of $Q_1, \ldots, Q_m$). We can now pass iteratively from the system (21) to its resultant system (20), then to the resultant system of all the $\rho_j^{(m)}$, etc. At each stage, one of the original variables $x_j, \ldots, x_n$ is eliminated. Eventually we will either come to a set of polynomials $\{g(x_k, \ldots, x_n)\}$ whose resultant system is identically zero, or all variables will be eliminated and we will be left with a nonzero constant. In the latter case, the manifold $V(Q_1, \ldots, Q_m)$ is empty; in the former case, the dimension of this manifold is $n - m$.

(c) In a space of $n > m$ variables, the dimension of the manifold $V(Q_1, \ldots, Q_m)$ cannot be less than $n - m$ without the manifold being empty. (See van der Waerden [21, Sec. 29, 34]). Thus, if in forming successive resultant systems from $Q_1, \ldots, Q_m$ more than $m$ variables are ever eliminated, we can be sure that the process of elimination will eventually produce a nonzero constant. This remark is useful for a number of purposes. In particular, $Q$ vanishes on $V(Q_1, \ldots, Q_m)$ if and only if the system

$$Q_j = 0, \qquad j = 1, \ldots, m, \qquad uQ - 1 = 0 \tag{22}$$

of equations has no common solution, where $u$ is an auxiliary variable. Thus if $m < n$, the condition $V(Q) \supseteq V(Q_1, \ldots, Q_m)$ is equivalent to $\dim(V(Q_1, \ldots, Q_m, uQ - 1)) < n - m$.

(d) Each time we eliminate a variable $x_j$ we require a polynomial whose $x_j$ term of highest degree has a constant coefficient. To ensure that such polynomials occur, we can pass from the set of polynomials $Q_j(X)$, where $X = (x_1, \ldots, x_n)$, to the set $Q_j((I - S)X)$, where $S$ is a subdiagonal matrix with indeterminate coefficients. Unless the $k$th resultant system of this set of polynomials vanishes identically in $X$ and $S$, $V(Q_1, \ldots, Q_m)$ has dimension less than $n - k$. For purposes of probabilistic testing, it is most convenient to form

$$P_1(X, S, u_1) = R_1(Q_1((I + S)X), Q_2((I + S)X) + Q_3((I + S)X)u + \cdots), \tag{23}$$

where $u_1$ is an indeterminate, and then successively

$$P_{i+1}(X, S, u_1, \ldots, u_{2^i}) = R_{i+1}(P_i(X, S, u_1, \ldots, u_{2^{i-1}}), P_i(X, S, u_{2^{i-1}+1}, \ldots, u_{2^i})), \tag{24}$$

where $R_i$ designates the resolvent formed with respect to the variable $x_i$. The first polynomial $P_k$ which vanishes identically determines the dimension $n - k$ of $V(Q_1, \ldots, Q_m)$. To test the condition $P_i \equiv 0$, the probabilistic techniques described previously can be used. If $d$ and $D$ are the smallest and the largest degree, respectively, of any polynomial $Q_j$, then $P_1$ will be of degree $d_1 = 2dD$ in the variables $x_2, \ldots, x_n$, and then successively $P_j$ will be of degree $d_j = 2d_{j-1}^2$ in $x_{j+1}, \ldots, x_n$. Since this sequence increases quite rapidly, and since calculation of the resultant of two polynomials of degree $d_j$ requires time $Kd_j \log^2 d_1$, calculation of values of $P_j$ will become impractical after approximately $d_{j-1} = 10^5$. If, for example, we begin with a system of polynomials $Q_1, \ldots, Q_m$ of degree 4 in $n$ variables, the test $\dim(V(Q_1, \ldots, Q_m)) < n - 3$ will generally

be feasible (even though the degree of $P_3$ might be as high as $8 \times 10^6$), but it will be infeasible to test the condition $\dim(V(Q_1, \ldots, Q_m)) < n - 4$ by the techniques that we have described. By the remark made in connection with (22), this means that these techniques suffice to test the condition $V(Q) \supseteq V(Q_1, Q_2)$ for polynomials of fairly small degree, but not to test the condition $V(Q) \supseteq V(Q_1, Q_2, Q_3)$.

Tarski [19] gave an effective technique based on Sturm's theorem for testing compatibility of sets of polynomial equalities and inequalities in the real domain. We now describe the way in which probabilistic testing can be used to extend the reach of his methods somewhat. We consider the problem of determining whether a set of polynomial equalities and inequalities in $n$ real variables $X = (x_1, \ldots, x_n)$ of the form

$$f_i(X) = 0, \qquad g_i(X) \geq 0, \qquad h_i(X) > 0, \tag{25}$$

is satisfiable. Since $g_i \geq 0$ can be written as $g_i - y^2 = 0$, and $h_i > 0$ can be written as $y^2 h_i = 1$, it is sufficient for theoretical purposes to consider systems consisting of equalities only. (However, for practical purposes we will often wish to avoid introducing additional variables like $y$ if we can.) Since $f_1 = f_2 = \cdots = f_m = 0$ if and only if $f_1^2 + \cdots + f_m^2 = 0$, it is sufficient to consider the existence of a solution of a single real polynomial equation $f(X) = 0$. To handle this question, we adapt the technique introduced by Seidenberg [18]. Suppose that $f(X) = 0$. Then for any $Y = (y_1, \ldots, y_n)$, $f = 0$ has a real solution $Z$ nearest to $Y$, and if $X \neq Y$, then every one of the variational equations $(x_i - y_i)f_{x_i} - (x_j - y_j)f_{x_i} = 0$ will also be satisfied by $Z$. This leads us to consider the system

$$f = 0, \qquad (x_i - y_i)f_{x_i} - (x_1 - y_1)f_{x_i} = 0, \qquad i = 2, \ldots, n, \tag{26}$$

of $n$ polynomial equations in the variables $x_1, \ldots, x_n$.

Multiple factors in $f$ can be detected and eliminated by forming $\mathrm{GCD}(f_1, f_{x_i})$ for various $i$ and then dividing by any common divisors of degree greater than zero which appear. Thus we can suppose that no $f_{x_j}$ is identically zero on the set $V(f)$. Hence $V(f)$ has nonsingular points in the neighborhood of which it is a smooth surface of dimension $n - 1$ with a well-defined tangent hyperplane. Considered in the complex domain, the system (26) defines an algebraic correspondence $A$ between points $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$. A generic point $\tilde{X}$ of $V(f)$ is nonsingular, and for each such $\tilde{X}$ the set of corresponding $Y$ is one dimensional. It follows by the principle of enumeration of variables (see [21, Sec. 139]) that the algebraic correspondence $A$ is $n$-dimensional, and hence that for generic $Y$ the set of complex solutions $X$ of the system (26) is zero-dimensional, which is to say finite. Moreover, if $f$ is of degree $d$, then so is every one of the equations of (26), and it follows by Bezout's theorem (see [21, Sec. 41]) that for each $Y = (y_1, \ldots, y_n)$ for which (26) has finitely many solutions the number of these solutions is bounded by $d^n$.

Write the system (26) in the form $F(X, Y) = 0$, where $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n)$ as above, and where $F$ is a vector-valued polynomial whose individual components are the various polynomials appearing in (26). Then consider the system

$$F((I + S)X, (I + S)Y) = 0, \tag{27}$$

where $S$ is subdiagonal. We can pass from this system to its resultant system formed with respect to the variable $x_1$, and then to successive resultants with respect to the variables $x_2, \ldots, x_{n-1}$, thus obtaining a set of polynomials in the remaining variable $x_n$. Finally, we can form the GCD of all these polynomials, thus obtaining a real polynomial $\Phi(x_n, S, Y)$ in $x_n$, with coefficients which are polynomial in the components of $S$ and $Y$. By collecting the coefficients $C$ of the terms $x_j^{d_j} C(x_{j+1}, \ldots, x_n, S, Y)$ of highest $x_j$-degree which appear during the process of resultant formation which leads to $\Phi(x_n, S, Y)$, and by adjoining to these any one of the nonvanishing coefficients of $\Phi$, we obtain a set of $n$ polynomials $q_j(S, Y)$. These have the property that if $q_j(S, Y) \neq 0$ for all $j$ and $\Phi(x_n, S, Y) = 0$, then there exist (possibly complex) $x_1, \ldots, x_{n-1}$ such that $X = (x_1, \ldots, x_{n-1}, x_n)$ satisfies the system (27), and such that (27) has at most $d^n$ solutions. Moreover, the polynomial $q_j$ is of

degree at most $2^{-1}(2d)^{2^{j-1}}$, so that the product $q(S, Y)$ of all the polynomials $q_j$ is of degree at most $4^{-1}(2d)^{2^n}$. For each $(S, Y)$ such that $q(S, Y) \neq 0$ let $X^{(j)}$, $j = 1, \ldots, \nu \leq d^n$, be all the solutions of the system of equations

$$F(X, Y) = 0. \tag{28}$$

Then the solutions $x_n$ of (27) are $(I + S)^{-1}X^{(j)}$. If any of the vectors $X^{(j)}$ is real, then the system (28), hence the system (26), and hence the equation $f = 0$, has a real solution. Suppose on the other hand that none of the vectors $X^{(j)}$ is real. Write $\mathrm{Im}(z)$ for the imaginary part of the complex number $z$, and let the vector $e_n$ be such that the inner product $(e_n, X)$ is the $n$th component $x_n$ of the vector $X$. Then each polynomial $\mathrm{Im}(e_n, (I + S)^{-1}X^{(j)})$ is of degree $n - 1$ in $S$ and is not identically zero for real $S$. Multiply $q(S, Y)$ by the product of all these polynomials to obtain a polynomial $\tilde{q}(S, Y)$ of degree at most $D = 2^{-2}(2d)^{2^n} + (n - 1)d^n$ with the property that if $\tilde{q}(S, Y) \neq 0$, then $\Phi(x_n, S, Y)$ has no real zero unless $f(X) = 0$ has a real solution. Hence if we assume that $f(X) = 0$ has no real solution and choose the components of $S$ and $Y$ at random from the range $-CD \leq i \leq CD$, it follows from Corollary 1 that the number of pairs $(S, Y)$ for which $\Phi(x_n, S, Y)$ has real solution amounts to at most $(2C)^{-1}$ of the total of all $(S, Y)$ which can be formed with components satisfying $-CD \leq i \leq CD$. Hence if we form $N$ different pairs $(S, Y)$ at random (but with components subject to this condition), compute $\Phi(x_n, S, Y)$ for each of them, and find in each case that $\Phi(x_n, S, Y)$ has a real root $x_n$, then it follows with probability $(2C)^{-N}$ that $f(X) = 0$ has a real solution. We can use Sturm's theorem to test $\Phi$ for the existence of a real solution $x_n$; the number of such solutions can be calculated rapidly by the method defined by formulas (16)–(18).

We can estimate in much the same way as previously that the technique just outlined will be practical in the three-variable case for a system $S$ of polynomials $f$ of small degree but will probably not suffice to do much for the four-variable case. In particular, we cannot expect to handle more than one inequality $g > 0$ or $g \geq 0$ by replacing it by an equality $u^2g = 1$ or $g - u^2 = 0$. If the system of equations and inequalities we need to process contains just one inequality $g > 0$ or $g \geq 0$, we can handle it without introducing any additional variables by testing the equation $g = \epsilon$ or $g = -\epsilon$, where $\epsilon$ is a formal infinitesimal constant, for compatibility with the other equations of $S$. If $S$ contains two inequalities, we can handle one of them by this technique and the other by replacing it by an equality involving an additional variable. Thus the approach we have outlined will allow a two-variable system $S$ involving two nonlinear inequalities, and a three-variable system $S$ involving just one such inequality, to be tested for compatibility without undue expenditure of time.

### 3. *Verification of Theorems of Elementary Plane Geometry*

Following Tarski [19] (and of course Descartes), P.J. Davis [6] notes the fact that the theorems of elementary plane geometry can be expressed as algebraic identities. Generally speaking, these are identities which involve expressions of the field generated from the rational functions of $n$ variables by repeated square root and rational operations; normally, no nonrational operations other than square roots will occur. It is worth displaying the identities to which a few common geometric theorems reduce, in order to make the depth of these identities and the technique for reduction of geometric theorems to identities explicit. It is convenient to use a complex notation, writing a point as $z = x + iy$. Then a line is represented (nonuniquely) as a pair $(u, w)$ with $u \neq 0$, and the point $z$ lies on the line if $u(\overline{z - w}) = \bar{u}(z - w)$. (Here $\bar{z}$ denotes the complex conjugate of $z$, i.e., $x - iy$.) Every primitive geometric notion has of course a straightforward algebraic expression, and for explicitness we catalog a few of them here.

(a) $(u, w)$ and $(u_1, w_1)$ are parallel iff $u\bar{u}_1 = u_1\bar{u}$.
(b) $(u, w)$ and $(u_1, w_1)$ are perpendicular iff $u\bar{u}_1 = -u_1\bar{u}$.
(c) The line through $z$ and $z_1$ is $(z - z_1, z_1)$.
(d) The square of the distance from $z$ to $z_1$ is $(z - z_1)(\overline{z - z_1})$.

(e) The intersection of $(u, w)$ and $(u_1, w_1)$ is

$$((w_1\bar{u}_1 - \bar{w}_1u_1)u - (w\bar{u} - \bar{w}u)u_1)(u\bar{u}_1 - \bar{u}u_1).^{-1}$$

(f) The double angle between $(u, w)$ and $(u_1, w_1)$ is $\theta = u\bar{u}_1/(\bar{u}u_1)$.
(g) The sum of two angles $\theta_1, \theta_2$ is $\theta_1\theta_2$.
(h) The difference of two angles $\theta_1, \theta_2$ is $\theta_1/\theta_2$.
(i) The line parallel to $(u, w)$ through $z$ is $(u, z)$.
(j) The line perpendicular to $(u, w)$ through $z$ is $(iu, z)$.
(k) The right angle is $i$.
(l) The straight angle is $-1$.

A circle is represented by a pair $(R, z)$ with $R > 0$. The most familiar circle-related constructions and their algebraic expressions are

(m) The tangent to $(R, z)$ through one of its points $w$ is $(i(z - w), w)$.
(n) The points of intersection of the circle $(R, z)$ and the line $(u, w)$ are

$$z + (2\bar{u})^{-1}((w - z)\bar{u} - u\overline{(w - z)} \pm (((w - z)\bar{u} - u\overline{(w - z)})^2 + 4R^2u\bar{u})^{1/2}).$$

(o) The chord of intersection of the circles $(R_1, z_1)$ and $(R_2, z_2)$ is

$$(i(z_2 - z_1), z_1 + (2\overline{(z_2 - z_1)})^{-1}(R_1^2 - R_2^2 + (z_2 - z_1)\overline{(z_2 - z_1)})).$$

A few useful but somewhat more compound constructions have the following expressions:

(p) Any point on the line $(u, w)$ has the form $u(v + \bar{v}) + w$.
(q) Any point on the circle $(R, z)$ has the form $Rv/\bar{v} + z$.
(r) The line equidistant between $z_1$ and $z_2$ has the form $(i(z_2 - z_1), \frac{1}{2}(z_1 + z_2))$.
(s) The bisector of the angle between $(u_1, w)$ and $(u_2, w)$ is $((u_1u_2)^{1/2}, w)$.

Algebraic constants $\alpha$ other than $\pm 1, \pm i$ appear in certain geometric constructions and are therefore useful; for example, rotation by 60 degrees (respectively, 45 degrees) is multiplication by the root $\alpha$ of $\alpha^2 - \alpha + 1 = 0$ (respectively, $\alpha^2 + i = 0$). If the irreducible equation satisfied by such an $\alpha$ is of degree $k$, then a rational expression $R$ involving $\alpha$ can be written as $R = R_0 + R_1\alpha + \cdots + R_{k-1}\alpha^{k-1}$, and then the identity $R \equiv 0$ simply abbreviates $R_0 \equiv \cdots \equiv R_k \equiv 0$. Of course, plane areas also have rational expressions; e.g.,

(t) The area of the triangle with corners $z_1, z_2, z_3$ is

$$\text{area} = \frac{i}{4}\det\begin{bmatrix} z_1 & \bar{z}_1 & 1 \\ z_2 & \bar{z}_2 & 1 \\ z_3 & \bar{z}_3 & 1 \end{bmatrix}.$$

The familiar elementary relationships cataloged above allow a wide variety of elementary geometric statements to be compiled automatically into algebraic identities, or if necessary into implications $(Q_1 = 0 \;\&\; Q_2 = 0 \;\&\; \cdots \;\&\; Q_n = 0) \to (Q = 0)$ between algebraic identities, and thus to be verified automatically. As we have seen, verification of an implication of this kind by the technique outlined in the preceding pages will be easy when $n \leq 2$ but will start to become infeasible when $n = 3$. Thus, in attempting to verify a geometric theorem it is important to formulate it in a manner which holds the number of premises $Q_i = 0$ which appear in its compiled form to a minimum. Any one of the points appearing in a geometric theorem can be identified with the origin; this simplifies the expression of the theorem as a rational function.

To illustrate all this, we consider a few familiar theorems of elementary plane geometry and the manner in which a geometric theorem verifier based on the rational relationships listed above would handle them. As a first example we take the *pons asinorum*: "Base angles of an isosceles triangle are equal." For easy verification this should be put: "If $w_1$ and $w_2$ are both points of the circle $(R, z)$ with $z$ the origin, then the angles $zw_1w_2$ and $zw_2w_1$ are equal." This latter statement compiles into the identity

$$\frac{(Ru/\bar{u})\overline{(Ru_1/\bar{u}_1 - Ru/\bar{u})}}{(Ru_1/\bar{u}_1 - Ru/\bar{u})\overline{(Ru_1/\bar{u}_1)}} = \frac{(Ru_1/\bar{u}_1)\overline{(Ru/\bar{u} - Ru_1/\bar{u}_1)}}{(Ru/\bar{u} - Ru_1/\bar{u}_1)\overline{(Ru/\bar{u})}}, \tag{29}$$

which is trivially verified, even by simplification. Next consider "the sum of the angles of a triangle is a straight angle," which we can put as "if $w_1$, $w_2$ and the origin $z$ are three points, then the sum of the doubled angles $w_2w_1z$, $w_1zw_2$, $zw_2w_1$ is twice a straight angle." This last statement compiles into the obvious identity

$$\frac{(w_1/\bar{w}_1)(\overline{w_2 - w_1})}{(w_2 - w_1)(\bar{w}_2/w_1)(w_1/\bar{w}_1)(\overline{w_2 - w_1})/(w_2 - w_1)(w_2/\bar{w}_2)} = 1. \tag{30}$$

As a third example, consider that "the angle between two chords of a circle is measured by half the difference of the subtended angles." For our purposes this is most appropriately put as follows: "Let $p_1$, $p_2$, $p_3$, $p_4$ be four points on the circle $(R, z)$ with $z$ the origin. Then twice the doubled angle between the line through $p_1$, $p_2$ and the line through $p_3$, $p_4$ is equal to the difference between the angles $p_3zp_1$ and $p_2zp_4$." This compiles into the easily verified identity

$$\frac{p_1\bar{p}_3/\bar{p}_1p_3}{p_4\bar{p}_2/\bar{p}_4p_2} = \frac{(p_1/\bar{p}_1 - p_2/\bar{p}_2)(\bar{p}_3/p_3 - \bar{p}_4/p_4)}{(\bar{p}_1/p_1 - \bar{p}_2/p_2)(p_3/\bar{p}_3 - p_4/\bar{p}_4)}. \tag{31}$$

A fourth example is: "If the diagonals of a parallelogram are orthogonal, then the parallelogram is a rhombus." This can be stated as the following implication:

$$(z_1 + z_2)(\overline{z_2 - z_1}) = -(\overline{z_1 + z_2})(z_2 - z_1) \qquad \text{implies} \qquad z_1\bar{z}_1 = z_2\bar{z}_2, \tag{32}$$

which follows easily either by simplification or by the general techniques described in the preceding pages. As final example we consider the theorem of N. Buonaparte mentioned in Davis [6]: "If equilateral triangles are erected on the sides of any triangle $T$, the three centroids of these triangles themselves form an equilateral triangle." Here it is convenient to make use of the root $e^{-\pi i/3}$ of the irreducible equation $\alpha^2 - \alpha + 1 = 0$, in terms of which the centroid of the equilateral triangle erected on the segment from $z_1$ to $z_2$ is $\frac{1}{3}((2 - \alpha)z_1 + (1 + \alpha)z_2)$. Thus Buonaparte's theorem compiles into the identity

$$\begin{aligned}((2 - \alpha)z_1 + (2\alpha - 1)z_2 - (1 + \alpha)z_3)&\overline{((2 - \alpha)z_1 + (2\alpha - 1)z_2 - (1 + \alpha)z_3)} \\ = ((2 - \alpha)z_2 + (2\alpha - 1)z_3 - (1 + \alpha)z_1)&\overline{((2 - \alpha)z_2 + (2\alpha - 1)z_3 - (1 + \alpha)z_1)},\end{aligned} \tag{33}$$

which is easily verified by writing it as $a\alpha + b = 0$ and verifying $a = 0$ and $b = 0$ separately. It is amusing to note that since $\alpha$ and $\bar{\alpha}$ are algebraically indistinguishable, the equilateral triangles in this theorem can either all be erected on the outside, or all erected on the inside, of $T$.

## 4. *Probabilistic Computations in Real Arithmetic*

Rather than using integer or modular arithmetic to test polynomial identities in the manner just outlined, it is possible to make use of real arithmetic, provided that computations can be carried out with a sufficient, and guaranteed, precision. (For this, arithmetic procedures, or hardware, which guarantee computational significance, or at least randomness of error, may be appropriate.) Probabilistic use of real arithmetic seems considerably harder to justify than probabilistic use of integer or modular arithmetic, but at least in the one-variable case we are able to give formal justification by use of theorems of Tschebycheff, Kakeya [12], and Okada [15].

THEOREM 2 (KAKEYA–OKADA). *Let $Q$ be a polynomial in one variable $x$ with integer coefficients, and suppose that $|Q(x)| < 1$ for all $x$ in an open interval $I$ of length at least 4. Then $Q$ is identically equal to zero.*[1]

PROOF. We reproduce Okada's reasoning for the convenience of the reader. We can assume without loss of generality that $I$ is $-2 < x < 2$. Consider any irreducible monic

[1] Thanks are extended to Peter Lax for putting the author on the track of this and the following theorem. The suggestion that real arithmetic be used is found in Davis [6], but no formal probabilistic argument is advanced in support of this suggestion.

polynomial $\phi$ with integer coefficients, all of whose roots $x_1, \ldots, x_n$ lie in $I$. $|\prod_{i=1}^{n} Q(x_i)| < 1$, but this product is symmetric in the roots $x_i$, hence expressible in terms of the elementary symmetric functions of those roots, which is to say the coefficients of $\phi$, hence an integer, and hence zero. Thus $Q(x_i) = 0$ for at least one root of $\phi$. Since $\phi$ is irreducible, it follows that $Q(x_i) = 0$ for every root of $\phi$. Since any monic polynomial factors into monic irreducibles, this holds even if we drop the assumption that $\phi$ is irreducible. Now let $\phi(x) = \sin(n \arccos(x/2))/\sin(\arccos(x/2))$. Then $\phi(2\cos x) = \sin nx/\sin x$, from which it is easily seen that $\phi$ is monic and that the roots of $\phi$ are $2\cos(k\pi/n)$, $k = 1, \ldots, n-1$. Hence $Q$ vanishes at all these points, and therefore identically. Q.E.D.

COROLLARY 3 (FEKETE–SZEGÖ). *Let $Q$ be a polynomial in one variable $x$ with integer coefficients, and suppose that $|Q(x)| < 1$ for all $x$ in a point set $I$ of the complex plane. Suppose that infinitely many irreducible monic polynomials $\phi$ with integer coefficients have all their roots in $I$. Then $Q$ is identically equal to zero.*

PROOF. This follows immediately by the argument of Okada given just above. Q.E.D.

To exploit this corollary, we want to find sets $I$ in which infinitely many irreducible monic polynomials have all their roots. For this purpose we can use a theorem of Fekete and Szegö [9], phrased by them in terms of the notion of *transfinite diameter* of a point set, as introduced by Fekete [8]. This notion has the following definition:

*Definition* 3. Let $I$ be a subset of the complex plane. For each $n$, let $M_n(I)$ be the maximum of

$$\prod_{1 \le i < j \le n} |z_i - z_j|, \tag{34}$$

taken over $z_1, \ldots, z_n$ varying independently in $I$. Then the sequence $(M_n(I))^{2/n(n-1)}$ is monotone decreasing, and its limit $M(I)$ is called the *transfinite diameter* of $I$.

It is clear from this definition that $M(I) \le M(J)$ if $I \subseteq J$, and that $M(cI) = cM(I)$ for each positive constant $c$ (here $cI$ designates the set $\{cx : x \in I\}$).

THEOREM 3 (FEKETE–SZEGÖ [9]). *Let $I$ be a closed bounded subset of the real axis whose transfinite diameter exceeds 1, and let $S$ be a set of points in the complex plane whose interior includes $I$. Then there exist infinitely many monic irreducible polynomials with integer coefficients whose zeros lie in $S$.*

THEOREM 4 (FEKETE [8]). *Let $I$ be a closed bounded subset of the real axis whose transfinite diameter is less than 1. Then there exist only finitely many monic irreducible polynomials with integer coefficients whose zeros lie in $I$.*

THEOREM 5 (KAKEYA; SEE OKADA [15]). *For any $\alpha < 2$, there exists a polynomial $Q$ with integer coefficients such that $|Q(x)| < 1$ everywhere in $-\alpha \le x \le \alpha$.*

Since the monic polynomials $\sin(n \arccos(x/2))/\sin(x/2)$ have all their zeros in $-2 \le x \le 2$, it follows from Theorem 4 that the transfinite diameter of this set is at least 1. By Theorem 3 and Corollary 3, $M(\{x : -a \le x \le a\}) < 1$ for $a < 2$. Thus $M(\{x : -2 \le x \le 2\}) = 1$, and hence $M(\{x : -a \le x \le a\}) = a/2$. From this we can easily derive the following lemma.

LEMMA 5. *Let $I$ be the union of finitely many disjoint intervals of the real axis, and suppose that the measure of $I$ (i.e., the total length of all these intervals) exceeds 4. Then the transfinite diameter $M(I)$ exceeds 1.*

PROOF. Put

$$f(x) = \int_{-\infty}^{x} \mu_I(y)\, dy, \tag{35}$$

where $\mu_I$ is the characteristic function of $I$. Then $f(\infty)$ is the measure of $I$ and hence exceeds 4. For each $0 \leq y \leq f(\infty)$, let $g(y)$ be the leftmost point in $I$ such that $y = f(x)$. Then $g$ maps $0 \leq y \leq f(\infty)$ into $I$, and clearly $|g(y_1) - g(y_2)| \geq |y_1 - y_2|$, since $\int_{y_1}^{y_2} \mu_I(y)\,dy \leq y_2 - y_1$. It follows from this and from Definition 3 that $M(I) \geq M(\{y: 0 \leq y \leq f(\infty)\})$, so that $M(I) \geq f(\infty)/4 > 1$. Q.E.D.

COROLLARY 4. *Let $Q$ be a polynomial in one variable $x$ with integer coefficients, and suppose that $|Q(x)| < 1$ for all $x$ in a portion $I$ of the real axis having measure greater than 4. Then $Q$ vanishes identically.*

PROOF. Consider the set $S = \{x: Q(x) < 1\}$. This set is open, and its intersection $S \cap R$ with the real axis $R$ is a finite union of subintervals with measure greater than 4. Hence $S \cap R$ contains a finite union $I$ of closed subintervals with total measure greater than 4. By Lemma 5, $M(I) > 1$, and hence our assertion follows by Theorem 3 and Corollary 3. Q.E.D.

Corollary 4 clearly justifies real arithmetic probabilistic testing of polynomial identities in one variable. Purported identities of this kind can be tested by choosing a real number at random in an interval of length $L > 4$; the probability that $P$ should have a value less than 1 without being identically zero is then no more than $4/L$.

It would of course be desirable to extend the preceding discussion to polynomials and polynomial identities in more than one variable, but the present author has thus far been unable to do so.

## 5. *Functions Other Than Polynomials*

The identity-testing technique that we have outlined rests on a very crude counting principle and hence can be applied to any class of functions whose nonzero members can only have some suitably limited number of zeros in a region known in advance. We shall see that this includes a class of functions formed using polynomial functions and exponentiation. It must be noted, however, that the family of identities which such functions satisfy is less rich than the class of polynomial identities. The following result (see Polya and Szego [16, p. 46] gives an easy but basic fact concerning the class of functions we wish to consider.

LEMMA 6. *For $j = 1, \ldots, m$, let $P_j$ and $Q_j$ be polynomials in the variable $x$ of degree $d_j$ and $\delta_j$, respectively. Let $\delta = max_{1 \leq j \leq m} \delta_j$. The function*

$$E(x) = \sum_{j=1}^{m} P_j(x) e^{Q_j(x)} \tag{36}$$

has at most $\sum_{i=1}^{m} (c_j + 1)$ real roots, where $c_n$ is defined inductively as follows:

$$c_1 = d_1; \qquad c_{i+1} = d_{i+1} + \delta \sum_{j=1}^{i} (c_j + 1) \qquad \text{for} \quad 1 < i \leq m. \tag{37}$$

PROOF. By Rolle's theorem, a function can have at most one more root than its derivative. Thus $E(x)$ can have at most $c_1 + 1$ more roots than

$$\left(\frac{d}{dx}\right)^{d_1+1} e^{-Q_1(x)} E(x) = \left(\frac{d}{dx}\right)^{d_1+1} \sum_{j=2}^{m} P_j(x) e^{(Q_j(x) - Q_1(x))}. \tag{38}$$

After differentiation, the exponentials appearing on the right-hand side of (38) will have polynomial coefficients of degree $d_j + \delta(d_1 + 1)$ at most. Hence we can repeat our argument and conclude that $E(x)$ has at most $(c_1 + 1) + (c_2 + 1)$ more roots than an expression of the form

$$\sum_{j=3}^{m} \hat{P}_j(x) e^{(Q_j(x) - Q_2(x))}, \tag{39}$$

where $\hat{P}_j$ is of degree at most $d_j + \delta(c_1 + 1) + \delta(c_2 + 1)$. Arguing inductively in this way, we prove our assertion. Q.E.D.

COROLLARY 5. *For $j = 1, \ldots, m$, let $P_j$ and $Q_j$ be polynomials in the variables $x_1, \ldots, x_n$ of total degree $d_j$ and $\delta_j$, respectively. Let $\delta = max_{1 \le j \le m} \delta_j$ and $d = max_{1 \le j \le m} d_j$. Let $I$ be any finite set of real points. Then if the function*

$$E(x_1, \ldots, x_n) = \sum_{j=1}^{m} P_j(x_1, \ldots, x_n) e^{Q_j(x_1, \ldots, x_n)} \tag{40}$$

*has more than $|I \times \cdots \times I|(n/|I|)(\delta^{-1}((\delta + 1)^m - 1)(d + 1)$ zeros in the $n$-fold Cartesian product set $I \times \cdots \times I$, it is identically zero.*

PROOF. For $n = 1$ our assertion follows at once from Lemma 6, and we proceed by induction on $n$. Suppose that $E$ is not identically zero. Then there exist $\hat{x}_1, \ldots, \hat{x}_{n-1}$ for which $E(\hat{x}_1, \ldots, \hat{x}_{n-1}, x_n)$ is not identically zero in $x_n$. Put $K = \delta^{-1}((\delta + 1)^m - 1)(d + 1)$. By Lemma 6, $E(\hat{x}_1, \ldots, \hat{x}_{n-1}, x_n)$ has at most $K$ zeros. If $\hat{x}_n$ is one of these zeros, then $E(x_1, \ldots, x_{n-1}, \hat{x}_n)$ can be zero for all $(x_1, \ldots, x_{n-1}) \in I_1 \times \cdots \times I_{n-1}$, where $I_j = I$. If $x_n$ is not one of these zeros, then by the inductive hypothesis, $E(x_1, \ldots, x_{n-1}, \hat{x}_n)$ has at most

$$\frac{(n-1)}{|I|} K \tag{41}$$

zeros in the $(n-1)$-fold Cartesian product $I \times \cdots \times I$. Thus the total number of zeros of $E$ in the $n$-fold Cartesian product $I \times \cdots \times I$ is at most

$$|I_1 \times \cdots \times I_{n-1}| \cdot K + |I| \frac{(n-1)}{|I|} K |I_1 \times \cdots \times I_{n-1}| = |I_1 \times \cdots \times I_n| \frac{n}{|I|} K, \tag{42}$$

where to avoid ambiguity we have written $I$ as $I_j$. Q.E.D.

It is clear that Corollary 5 justifies much the same sort of probabilistic test as is discussed in the first section of the present paper. Moreover, if in addition to the hypotheses of Corollary 5 we asume that for $1 \le j \le m$, $P_j$ and $Q_j$ have integer coefficients, and that $k_j$ is an integer, then identities of the form

$$\sum_{j=1}^{m} P_j(x_1, \ldots, x_n) k_j^{Q_j(x_1, \ldots, x_n)} = 0 \tag{43}$$

can clearly be tested probabilistically, either by calculations carried out in rational arithmetic or by modular calculations using primes chosen at random from a sufficiently large set.

## REFERENCES

(Note References [10, 13] are not cited in the text.)

1. AHO, A., HOPCROFT, J., AND ULLMAN, J *The Design and Analysis of Computer Algorithms* Addison-Wesley, Reading, Mass., 1974.
2. BIEBERBACH, L., AND BAUER, G *Vorlesungen uber Algebra.* B G Teubner Publishing Co., Berlin, 1928.
3. CHAITIN, G., AND SCHWARTZ, J.T. A note on Monte Carlo primality tests and algorithmic information theory *Commun Pure Appl Math.* (1978)
4. COLLINS, G.E The calculation of multivariate polynomial resultants. *J. ACM 18*, 4 (Oct 1971), 515–532
5. COLLINS, G.E Computer algebra of polynomials and rational functions *Amer. Math Monthly 80* (1973), 725–753
6. DAVIS, P.J. Proof, completeness, transcendentals, and sampling. *J. ACM 24*, 2 (April 1977), 298–310
7. DUNFORD, N., AND SCHWARTZ, J T *Linear Operators, Part II.* Wiley-Interscience, New York and London, 1963.
8. FEKETE, M. Uber die Verteilung der Wurzeln bei Gewissen Algebraischen Gleichungen mit Ganzzahligen Koeffizienten *Math. Z. 17* (1927), 228–249.
9. FEKETE, M., AND SZEGO, G. On algebraic equations with integer coefficients whose roots belong to a given point set *Math. Z. 63* (1955), 158–172
10. HEINDEL, L.E. Integer arithmetic algorithms for polynomial real zero determination. *J. ACM 18*, 4 (Oct. 1971), 533–548

11. HERMANN, G. Die Frage der Endlich Vielen Schritte in der Theorie der Polynomidealen. *Math. Ann. 95* (1926), 736–788
12. KAKEYA, S On approximate polynomials *Tohoku Math J. 6* (1914), 182–186.
13 MARTIN, W A. Determining the equivalence of algebraic expressions by hash coding. *J. ACM 18*, 4 (Oct. 1971), 549–558.
14 MOENCK, R Fast computation of GDC's Proc. 5th Ann ACM Symp on Theory of Computing, 1973, Austin, Texas, pp 142–151
15 OKADA, Y On approximate polynomials with integer coefficients only *Tohoku Math. J. 23* (1924), 26–35.
16 POLYA, G , AND SZEGO, G *Problems and Theorems in Analysis*, vol 2 Springer-Verlag, New York, 1976.
17 RABIN, M. Probabilistic algorithms In *Algorithms and Complexity. New Directions and Recent Results* J.F. Traub, Ed , Academic Press, New York, 1976, pp. 21–39
18. SEIDENBERG, A. A new decision method for elementary algebra. *Ann. Math. 60* (1954), 365–374.
19 TARSKI, A *A Decision Method for Elementary Algebra and Geometry*, 2nd ed. University of California Press, Berkeley, Calif., 1951.
20 VAN DER WAERDEN, B.L. *Modern Algebra*, vols. I, II. Frederick Ungar Publishing Co., New York, 1949, 1950.
21. VAN DER WAERDEN, B L. *Einfuhrung in die Algebraische Geometrie*, 2nd ed. Springer Verlag, New York, 1973

RECEIVED JUNE 1978, REVISED JANUARY 1980, ACCEPTED JANUARY 1980