JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 78B, No. 1, January–March 1974

Integer Arithmetic Determination of Polynomial Real Roots

George W. Reitwiesner

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(May 3, 1973)

The real roots of a polynomial with rational coefficients may be evaluated to absolute precision by integer arithmetic. Based upon the theorems of Sturm and Budan, two algorithms for this evaluation are described, and some comparative observations are offered.

Key words: Budan theorem; exact computation; integer arithmetic; modular arithmetic; polynomial; polynomial real roots; roots; Sturm theorem.

1. Introduction

Given some $P_0(x)$, we consider the sequence $P_0(x)$, $P_1(x)$, . . . $P_t(x)$ of polynomials

$$P_i(x) = \sum p_m^{(i)} x^{n_i - m}$$

formed by an algorithm (detailed below) under which the degrees $n_0, n_1, \ldots n_t$ of the $P_i(x)$ decrease monotonically. We denote degree drop by $d_i = n_i - n_{i-1} \geqq 1$; we distinguish the leading and maximum coefficient magnitudes of the $P_i(x)$ by $c_i = |p_0^{(i)}|$ and $g_i \geqq |p_m^{(i)}|$; we denote the norms of the $P_i(x)$ by $e_i = (\Sigma (p_m^{(i)})^2)^{1/2}$; and we distinguish the degree of the initial $P_0(x)$ by $N = n_0$. We observe $t \leqq N$, and we define $M = N - 1$.

We consider two algorithms. In the Sturm case: $P_1(x)$ is the derivative of $P_0(x)$, and each other $P_i(x)$ is the negative of the remainder polynomial upon dividing $P_{i-2}(x)$ by $P_{i-1}(x)$; and $d_i \geqq 1$ yields $t \leqq N$. In the Budan (or Fourier-Budan) case: every $P_i(x)$ for $i \geqq 1$ is the derivative of $P_{i-1}(x)$; and all $d_i = 1$ yields $t = N$. We discuss these cases, first together, and then separately.

We seek the real roots of $P_0(x)$ by determining the $p_m^{(i)}$ for $i \geqq 1$ and then employing a procedure which requires determining, for selected values of x, the sign(s) of either $P_0(x)$ or all $P_i(x)$. Hence, as convenient, we may replace any $P_i(x)$ by any associate polynomial formed by multiplying $P_i(x)$ by some positive scaling factor f_i. Arbitrarily, we regard $p_0^{(0)} > 0$; and (optionally) we ignore zero roots of $P_0(x)$ by imposing $p_N^{(0)} \neq 0$ (adjusting N if necessary). Trivially, we demand $N > 0$.

By B we denote some bound such that all real roots of $P_0(x)$ lie in the range $-B < x \leqq B$ (e.g., $e_0 < B$); and, by analyzing the signs of the $P_i(x)$ at interval endpoints, we develop successively smaller intervals $x' < x \leqq x''$ within $-B < x \leqq B$ to bound each root in an interval of desired small length.

We consider only rational $p_m^{(0)}$ (e.g., terminating digital expressions), and we restrict all f_i to be rational, whence all $p_m^{(i)}$ are rational.

For exactness in computation, through suitable f_i we constrain all $p_m^{(i)}$ to be integers; and we consider only integer values for B and all x' and x''; hence only integer values are assumed by the $P_i(x)$ at interval endpoints, and the maximum error within which roots ultimately are determinable is 1. Root determination to subinteger precision is tractable, under this integer convention, by suitable initial upscaling of the $p_m^{(i)}$ and corresponding terminal downscaling of the (integer) roots thus determined. Accordingly, hereinafter the minimum value of $x''-x'$ is 1.

Toward precluding unnecessarily large magnitudes among the integer values of the $p_m^{(i)}$ and $P_i(x)$, we remove all common prime factors from the $p_m^{(i)}$ of each $P_i(x)$: initially from $P_0(x)$, and from each other $P_i(x)$ as the algorithm is executed.

The restriction that all values of $p_m^{(i)}$ and B and x' and x'' (and $P_i(x)$) be integers affords opportunity to isolate the roots of $P_0(x)$ into intervals which are bounded exactly—without error accural from numerical rounding or truncation. We are not concerned here with perturbations in root values resulting from change(s) in the integer value(s) of any individual $p_m^{(0)}$.

By $V(x)$ we denote the number of sign changes (ignoring any $P_i(x)=0$) in the sequence $P_0(x)$, $P_1(x)$, . . . $P_t(x)$; and by $R(x', x'')$ we denote the number of real roots of $P_0(x)$ in the interval $x'<x\leqq x''$. Also, we define $\bar{R}(x', x'')=V(x')-V(x'')$. The distinct considerations which apply in establishing $R(x', x'')\leqq\bar{R}(x', x'')$ are discussed separately for the Sturm and Budan cases below.

In both cases, establishing B as any (e.g., the smallest) integer power of 2 which maximizes $\bar{R}(-B,+B)\leqq\bar{R}(-\infty, +\infty)$, and employing $V(x)$ at interval endpoints, the real roots of $P_0(x)$ may be separated into intervals of lengths diminishing to 1—and thus evaluated to within an error of at most 1—by repeated interval halving: first of the initial interval $-B<x\leqq B$, and then of its repeatedly halved subintervals $x'<x\leqq x''$ for which $\bar{R}(x', x'')\neq 0$.

2. The Sturm Case

The Sturm algorithm is expressible as $P_i(x)=[Q_i(x)P_{i-1}(x)-\theta_i P_{i-2}(x)]/\phi_i$ for $i=2, 3, \ldots t$, terminating when $P_{t+1}(x)=0$, where θ_i and ϕ_i are positive scaling factors and the $Q_i(x)$ are discarded.

Obviously $d_1=1$, but $d_i\geqq 1$ applies for $i\geqq 2$; and $t\leqq N$. The constrain that all $p_m^{(i)}$ be integers commends the establishment of $\theta_i=(c_{i-1})^{d_{i-2}+1}$, and $\phi_i>0$ may be chosen arbitrarily so long as the integer quality of the $p_m^{(i)}$ is maintained. Under Euclid's algorithm (for polynomials), the final $P_t(x)$ is (within scaling factors) the greatest-degree polynomial divisor of every $P_i(x)$, and each of its roots is a root of every $P_i(x)$; and, by a property of the derivative, each single or multiple root of $P_0(x)$ is, to multiplicity one less, a root of each $P_1(x)$, $P_2(x)$, . . . $P_t(x)$.

In the Sturm case, every single or multiple root of $P_0(x)$ counting exactly once, $R(x', x'')=\bar{R}(x', x'')=V(x')-V(x'')$ is the number of distinct real roots of $P_0(x)$ in the interval $x'<x\leqq x''$, provided that neither x' nor x'' is a root of $P_t(x)$ (for then would follow all $P_i(x)=0$); however this constraint upon x' and x'' vanishes when every $P_i(x)$ is replaced by its quotient upon division by $(p_0^{(t)}/c_t)P_t(x)$, for then $P_0(x)$ contains no multiple roots, and $P_t(x)=\pm 1$ (and N is correspondingly reduced by n_t).

For the choice all $\phi_i=1$, the $p_m^{(i)}$ may assume unreasonable magnitudes when not all $c_i=1$. The ϕ_i may be chosen [1][1] such that the magnitude of each $p_m^{(i)}$ is equal to that of a particular subdeterminant, of order $2(N-n_i)-1$, of the Sylvester matrix for $P_0(x)$ and $P_1(x)$. This choice is $\phi_i=s_1 s_2 \ldots s_{i-2}c_{i-2}$, where $h_k=(d_1)(1-d_2)(1-d_3) \ldots (1-d_{k-2})(1-d_{k-1})(d_k)$ and $s_k=(c_k)^{h_k}$; and $\phi_2=1$ is understood; and when all $d_i=1$, there applies simply $\phi_i=(c_{i-2})^2$ for $i>2$. In each of these determinants: only coefficients of $P_1(x)$ occur in $N-n_i$ columns, and only coefficients of $P_0(x)$ occur in $M-n_i$ columns; hence by Hadamard's theorem, each subdeterminant magnitude is bounded by $e_1^{(N-n_i)}e_0^{(M-n_i)}\leqq e_1^N e_0^M$.

[1] Figures in brackets indicate the literature references at the end of this paper.

In implementing the Sturm case, with due sign consideration each $p_m^{(i)}$ may be computed as ± its counterpart subdeterminant of that Sylvester matrix, and the bound $e_1^N e_0^M$ is excessive at least to the extent that common integer factors occur among the $p_m^{(i)}$ of the $P_i(x)$. Since only $p_0^{(0)}$ and $p_0^{(1)}$ occur in one row of each Sylvester matrix subdeterminant concerned, their greatest common factor $[c_0, c_1]$ is a common factor of all $p_m^{(i)}$ for $i \geqq 2$, and additional common factors may appear in the several $P_i(x)$ as the algorithm is executed. However, in the absence of foreknowledge of such additional factors, the a priori minimum bound of the $p_m^{(i)}$ magnitudes for $i \geqq 2$ is given by $e_1^{(N-n_i)} e_0^{(M-n_i)}/[c_0, c_1] \leqq e_1^N e_0^M/[c_0, c_1]$.

We denote $G = e_1^N e_0^M/[c_0, c_1]$.

Indeed, in the Sturm case, the $p_m^{(i)}$ may be computed [2, 3] as ± determinants of elements $p_m^{(i-1)}$ and $p_m^{(i-2)}$; and when they are so computed, the magnitudes of intermediately formed products of $p_m^{(i-1)}$ and $p_m^{(i-2)}$ may exceed G, particularly for the larger values of i. However, the bound G does apply for the $p_m^{(i)}$ magnitudes throughout $2 \leqq i \leqq t$, and the generation of the Sturm polynomial coefficients may be conducted to digital precision which need but modestly exceed two times (for sign) the bound G: e.g., modulo some prime which exceeds $2G$; or, to preclude engaging cumbersomely large integers, by a modular arithmetic in which each quantity is represented by its residues, modulo a set of distinct primes whose product exceeds $2G$.

3. The Budan Case

The Budan algorithm [5] is $P_i(x) = d(P_{i-1}(x))/dx$ for $i = 1, 2, \ldots t = N$.

All $d_i = 1$; and, indeed, $P_t(x)$ need not be computed, for it is a constant $P_t(x) = (N!)\ p_0^{(0)}$ of sign identical to that of $p_0^{(0)}$. Clearly, all $p_m^{(i)}$ magnitudes for $i < t$ are bounded by $|p_m^{(i)}| \leqq (M!) g_0 < (M!)\ e_0$.

In the Budan case, every m-fold root of $P_0(x)$ being counted m times, $\bar{R}(x', x'') = V(x') - V(x'')$ is an upper bound on the number of real roots of $P_0(x)$ in the interval $x' < x \leqq x''$, and $R(x', x'')$ can differ from $\bar{R}(x', x'')$ only by an even integer. Therefore $R(x', x'')$ is known precisely only when $R(x', x'') = \bar{R}(x', x'') \leqq 1$; otherwise $R(x', x'') \leqq \bar{R}(x', x'')$ applies.

The potential even integer excess of $\bar{R}(x', x'')$ over $\bar{R}(x', x'')$ accrues from potential complex-conjugate pairs of roots of $P_0(x)$; and the engagement of $\bar{R}(x', x'')$ in isolating the real roots of $P_0(x)$ introduces potential ambiguity, when $\bar{R}(x', x'') \geqq 2$, in distinguishing the occurrence of complex roots of $P_0(x)$ from two cases of the occurrence of real roots in $x' < x \leqq x''$: the case of m-fold real roots, for $m \geqq 2$, which are not expressible as integers under whatever upscaling is employed; and the case of distinct (single or multiple) real roots which lie in the same interval $x' < x \leqq x''$ and differ in value by less than the resolution employed (utlimately $x'' - x' = 1$).

In particular cases, however, such ambiguity may be removable, at least partially, by two devices.

Under Descartes' rule, $P_0(x)$ can have no more positive real roots than the number of sign changes in the sequence $p_0^{(0)}, p_1^{(0)}, \ldots p_N^{(0)}$ and no more negative real roots than in that sequence with every alternate $p_m^{(0)}$ negated.

Also, denoting by $V_m(x)$ the number of sign changes in the sequence $P_t(x), P_{t-1}(x), \ldots P_m(x)$, and defining $\bar{R}_m(x', x'') = V_m(x') - V_m(x'')$, and constraining $m \leqq t-2$: if $P_k(x') > 0$ and $P_k(x'') > 0$ for all $k = t, t-1, \ldots m$, except only $0 > P_{m+1}(x')$, then $\bar{R}_m(x', x'') = 2$, but no real root of $P_m(x)$ can exist in $x' < x \leqq x''$ when the respective magnitudes of $P_m(x')$; and $P_m(x'')$ exceed $x'' - x'$ times those of their tangent slopes $P_{m+1}(x')$ and $P_{m+1}(x'')$ and a corresponding argument applies for <vice>. [And $x'' - x' = 1$ in the ultimate resolution.] The occurrence of every such condition, for a distinct interval $x' < x \leqq x''$, reveals the existence of one pair of complex-conjugate roots of $P_m(x)$, and therefore of $P_0(x)$, for the real roots of every $P_i(x)$ separate those of $P_{i-1}(x)$.

4. Summary

Comparison and/or contrast between the Sturm and Budan algorithms for polynomial real root evaluation is difficult to express, for performance under either is conditioned by the particular set of $p_m^{(0)}$ which comprise $P_0(x)$.

For equal expenditure of digit capacity, in a computer, to accommodate the $p_m^{(i)}$ in either case, and for large N and large (multi-decimal-digit) $p_m^{(0)}$ magnitudes, the bounds $e_1^N e_0^M/[c_0, c_1]$ and $(M!)e_0$ suggest the achievement of higher resolution of real roots under the Budan case, but at risk of uncertainty in the solution whenever $\bar{R}(x', x'') > 1$ occurs for some $x' < x \leqq x''$ at the termination $(x'' - x' = 1)$ of interval halving.

Under the Sturm case, the precise value of $R(x', x'')$ is known for every interval $x' < x \leqq x''$, but to potentially lower resolution because of the evidently higher a priori bound on the magnitudes of the $p_m^{(i)}$.

In the appendix is displayed a table, summarizing admittedly limited experience for the Sturm case, showing common logarithms of: (a) the bound $e_1^N e_0^M$; (b) the maximum g_i generated in executing the Sturm algorithm for $\phi_i = s_1 s_2 \ldots s_{i-2} c_{i-2}$ but otherwise without common factor removal (without reducing the $p_m^{(i)}$ magnitudes by $[c_0, c_1]$); and (c) the maximum g_i after common factor removal among the coefficients of each $P_i(x)$ [and after division of each $P_i(x)$ by $(p_0^{(t)}/c_t)P_t(x)$]. The first 14 of the 16 entries are for the Nth degree polynomials whose roots are $-1, -2, \ldots -N$ for $N \leqq 14$; the 15th entry is for the 10th degree polynomial with the six real roots $-1/10$, $-1/11$, 0, 8101/8111, 1, 2, and the two doubled imaginary roots $\pm i$; and the last entry [4] is for the 8th degree polynomial $x^8 - 134x^7 + 6496x^6 - 147854x^5 + 1709659x^4 - 10035116x^3 + 28014804x^2 - 29758896x + 6531840$ whose six real roots are 58.1801 . . ., 32.1652 . . ., 17.6740 . . ., 13.0545 . . ., 1.7103 . . ., 0.2915 . . . . Also shown in the table is the smallest integer j which satisfies $e_0 < B = 2^j$.

For the first 14 entries, the sharpness of the reduction from (a) to (b) and (c) probably is due to the algebraic regularity with which the $p_m^{(0)}$ are expressible—as sums of products of integers (root negatives). For these 14 entries the maximum g_i occurs among the lower values of i, and, through symmetry in this "canonical" case of uniformly spaced roots, each $P_N(x)$ has the final (common factor removed) form $2x + (N+1)$ for even N and $x + (N+1)/2$ for odd N.

For the last two entries, the reduction from (a) to (b) and (c) is less pronounced, probably because of less algebraic regularity among the $p_m^{(0)}$.

However, despite the magnitude of the reduction from (a) to (b) and (c) for the last two entries—no further data [2] are available at this writing—there exists considerable contrast between the magnitudes of (c) (for the Sturm case) and the corresponding common logarithms of the bound $(M!)g_0$ (which would apply for the Budan case): 49.73 versus 11.52 for the 15th entry and 34.93 versus 11.18 for the 16th entry.

This contrast suggests serious consideration of the Budan algorithm, as well as the (infallible) Sturm algorithm, as a mechanism for determining, to absolute precision by integer arithmetic, the real roots of polynomials of large degree with large rational coefficient magnitudes.

5. Appendix

N	(a)	(b)	(c)	j
1	0.0	0.0	0.0	1
2	1.81	.48	.48	2
3	5.98	1.08	1.08	4
4	12.13	1.70	1.70	7
5	24.19	4.92	2.65	9
6	38.93	9.08	3.71	12
7	57.81	14.79	4.42	15
8	76.26	17.38	5.07	18
9	104.65	27.11	6.07	21
10	141.60	42.53	7.47	25
11	179.22	55.65	8.50	28
12	218.35	67.24	10.35	32
13	269.97	88.21	11.11	36
14	311.37	107.80	12.66	40
10	128.51	72.88	49.73	24
8	113.79	61.65	34.93	26

6. References

[1] Collins, George E., Subresultants and reduced polynomial remainder sequences, Journal of Association for Computing Machinery **14,** No. 1, 128–142 (Jan. 1967).

[2] Heindel, Lee E., Integer arithmetic algorithms for polynomial real zero determination, Journal of Association for Computing Machinery **18,** No. 4, 533–548 (Oct. 1971).

[3] Householder, Alston S., Principles of Numerical Analysis (McGraw Hill; 1953), p. 98.

[4] Newman, Morris, An identity for the coefficients of certain modular forms, Journal of London Mathematical Society **30,** 488–493 (1955).

[5] Patrick, Merrell L., A highly parallel algorithm for approximating all zeros of a polynomial with only real zeros, Communications of Association for Computing Machinery **15,** No. 11, 952–955 (Nov. 1972).

(Paper 78B1–397)