ELSEVIER

Information Processing Letters 61 (1997) 63-67

Information Processing Letters

Zero testing of algebraic functions

Richard Zippel [1]

Department of Computer Science, Cornell University, Ithaca, NY 14853, USA

Received 23 October 1996; revised 5 December 1996
Communicated by D. Gries

Abstract

It is well known that we can efficiently test whether a polynomial is identically zero or not by examining the values of the polynomial at well-chosen points. Both deterministic and efficient probabilistic algorithms have been devised for this purpose. It is not so well recognized that algebraic functions can be similarly tested for zeroness. The need for zero testing black boxes representing algebraic functions has recently arisen in the area of self-testing/self-correcting programs. Given a black box $\mathcal{B}_\alpha$ that represents an algebraic function α and a few additional parameters about α, we show how to test if α is equal to the zero function. © 1997 Elsevier Science B.V.

Keywords: Zero testing; Algebraic functions; Symbolic computing; Self-testing programs; Learning theory

1. Introduction

Let α be a function of n arguments, each of which comes from some field k and where the value of the function lies in an algebraic extension of k. Given a *black box* $\mathcal{B}_\alpha$ that represents α, we wish to determine if α is identically zero. That is, $\alpha(x_1, \ldots, x_n) = 0$ for all $x_i \in k$. If α is not identically zero, then there exist evaluation points for which $\alpha(w_1, \ldots, w_n) \neq 0$. Such a point is called a *witness to the non-zeroness* of α.

When additional information is known about α, *witnesses to the zeroness* of α do exist but tend to be large. For instance, if α is a univariate polynomial over the rational integers $\mathbb{Z}$, whose coefficients are bounded in absolute value by A, then the existence of an $x > 2A$ for which $\mathcal{B}_\alpha(x) = 0$ proves α is identically zero, and x is a witness to α's zeroness. For multivariate polynomials in v variables, the witnesses are larger and have additional constraints on their components.

To avoid growth in the size of the numbers used in zero testing, a sequence of test points is usually used. Test values $\vec{x}_1, \ldots, \vec{x}_N$ are chosen such that if $\mathcal{B}_\alpha(\vec{x}_1), \ldots, \mathcal{B}_\alpha(\vec{x}_N)$ are each zero, then

- α is identically zero (for deterministic algorithms), or
- α is very likely to be identically zero (for probabilistic algorithms).

If $\mathcal{B}_\alpha(\vec{x}_i)$ is different from zero for some i, then $\vec{x}_i$ is a witness to the non-zeroness of α. The essence of the problem is to determine the minimum N and a sequence of evaluation points $\vec{x}_1, \ldots, \vec{x}_N$ that yield the desired "zeroness" from the parameters of α.

We show how to reduce the zero testing of algebraic functions to zero testing of polynomials. The al-

[1] Email: rz@cs.cornell.edu. This work was supported in part by the Defense Advanced Research Projects Agency of the Department of Defense under ONR Contract N00014-96-1-0699, in part by the U.S. Army Research Office through the Mathematical Science Institute of Cornell University and in part by a grant from the United States-Israel Binational Science Foundation.

0020-0190/97/$17.00 © 1997 Elsevier Science B.V. All rights reserved.
PII S0020-0190(96)00207-4

gorithms are the same as those for polynomials. The subtlety is in determining how many test values are needed.

2. Reduction to polynomial zero testing

We recall some basic definitions from algebraic function theory. Unproven results mentioned below can be found in standard references on algebraic extensions, such as Lang [5]. An element of an extension of the field K is said to be *algebraic* over K if it is a zero of a monic polynomial

$$\begin{aligned} P(Z) &= Z^d - p_1 Z^{d-1} + p_2 Z^{d-2} - \cdots + (-1)^d p_d, \\ &= (Z - \alpha) \prod_{i=2}^{d} (Z - \alpha_i), \qquad (1) \end{aligned}$$

where the p_i are elements of K. The monic polynomial of lowest degree satisfied by α is unique. This polynomial is called the *minimal polynomial* of α, which we denote by P_α. The other zeroes of P_α are called the *conjugates* of α. For simplicity, we will let $\alpha_1 = \alpha$. The p_i are symmetric functions of the α_i and, in particular,

$$p_d = \alpha_1 \cdot \alpha_2 \cdots \alpha_d.$$

Expression p_d is called the *norm* of α. If p_d is zero and P_α is irreducible, then the degree of P_α is 1 - the element 0 has no conjugates. Therefore, α is identically zero *if and only if* p_d is identically zero.

If K is a field of rational functions over a ground field, e.g., $K = k(u_1, \ldots, u_n)$, and at least one of the p_i is not an element of k, then α is said to be an *algebraic function*. The norm of the algebraic function α is a rational function in the u_i. We have the following proposition.

Proposition 1. *Let k be a field, α be an algebraic function over $k(u_1, \ldots, u_n)$ and $p_d(u_1, \ldots, u_n)$ be the norm of α over $k(u_1, \ldots, u_n)$. Then α is zero if and only if the numerator of p_d is zero.*

Zero testing algorithms for polynomials, whether probabilistic or deterministic, compute the value of the polynomial at a carefully chosen sequence of test points. If any value differs from zero, then the polynomial is definitely not equal to zero. If all values are equal to zero, then the polynomial is either likely to be zero or definitely equal to zero, depending upon how the points where chosen.

To zero test an algebraic function α, it is enough to zero test the numerator of the norm of α (by Proposition 1). To zero test the norm of α, we do not need to compute p_d. Assume $\vec{u}^{(i)} = \langle u_1^{(i)}, \ldots, u_n^{(i)} \rangle$ is an element of k^n. For each evaluation of α there are two possible cases.

- If $\alpha(\vec{u}^{(i)})$ is different from zero, then $\vec{u}^{(i)}$ is a witness to α's non-zeroness and we are finished.
- If $\alpha(\vec{u}^{(i)})$ is equal to zero, then $p_d(\vec{u}^{(i)})$ is also equal to zero, since p_d is a multiple of α.

This technique allows us to use the zero testing techniques discussed in Chapter 12 of [9]. These techniques require bounds on the polynomial $p_d(u_1, \ldots, u_n)$ of one of two types:

- a bound on the number of non-zero terms in the polynomial, or
- a bound on the degree of the u_i's in p_d.

Some techniques require bounds of both types.

Since we are treating these polynomials as black boxes, it is most natural to assume bounds on the degrees of the u_i. Degree bounds are most naturally expressed as bounds on the total degrees of the coefficients of the powers of Z in $P_\alpha(Z, u_1, \ldots, u_n)$. (The *total degree* of a polynomial $p(u_1, \ldots, u_n)$ is the degree in t of the polynomial $p(u_1 t, \ldots, u_n t)$.)

By clearing the denominators of the rational functions in (2), we can write the minimal polynomial for α as

$$\begin{aligned} P_\alpha(Z) &= P_\alpha(Z, u_1, \ldots, u_n) \\ &= p'_0 Z^d - p'_1 Z^{d-1} + p'_2 Z^{d-2} \\ &\qquad - \cdots + (-1)^d p'_d, \end{aligned}$$

where there is no common divisor of all of the p'_j. The *height of α* ($\operatorname{ht} \alpha$) is the maximum of the total degrees of the p_j in the variables $u_1, \ldots, u_n$. The height of a constant, an element of k, is defined to be 1, not zero.

Clearly, the total degree of p_d is bounded by the height of α. Using Proposition 5, which is stated in the Appendix and which is discussed in [9], we have the probabilistic result:

Proposition 2. *Let $\mathcal{B}_\alpha$ be a black box representing an algebraic function α in n variables over a field k. Assume that the height of α is bounded by D. If*

$x_1^{(i)}, \dots, x_n^{(i)}$ are chosen from a subset of k of cardinality B, $i = 1, \dots, N$ and $\mathcal{B}_\alpha(x_1^{(i)}, \dots, x_n^{(i)}) = 0$, then the likelihood that α is not identically zero is less than D/B.

Using Proposition 6 (given in the Appendix and first presented in [4]) we have the following deterministic result.

Proposition 3. *Let $\mathcal{B}_\alpha$ be a black box representing an algebraic function α in n variables over a field k of characteristic zero. Assume that the height of α is bounded by D. Let q_i denote the ith prime number in $\mathbb{Z}$. If $\mathcal{B}_\alpha(q_1^j, \dots, q_n^j) = 0$ for $j = 1, \dots, \binom{D+n}{n}$, then α is identically zero.*

Proof. That the components of the set of potential witnesses should be powers of prime numbers follows from the proof of Proposition 6, which is given in the Appendix. The only parameter needed by Proposition 6 is the maximum number of monomials in p_d, which is bounded by $\binom{D+n}{n}$. The fact that a polynomial in n variables of total degree D is bounded by $\binom{D+n}{n}$ is well known [1,3]. □

3. Estimating the height of an algebraic function

The height of an algebraic function is a bound on the coefficients of the algebraic function's minimal polynomial. When an algebraic function is constructed from other algebraic functions using arithmetic operations and extraction of roots, we can compute the minimal polynomial of the new algebraic function from those of the "smaller" algebraic functions. The height of the new algebraic function can then be related to the heights of the smaller ones, by relating the sizes of the coefficients of the minimal polynomials.

For instance, let $P_\alpha(Z, u_1, \dots, u_n)$ and $P_\beta(Z, u_1, \dots, u_n)$ be the minimal polynomials of two algebraic functions α and β over the field $K = k(u_1, \dots, u_n)$. Denote the degree of α by m and the degree of β by n. Then the minimal polynomial of $\alpha + \beta$ divides the resultant of $P_\alpha(Z - t)$ and $P + \beta(t)$ with respect to t (see Section 9.4 of [9]):

$$Q(Z) = \mathrm{res}_t(P_\alpha(Z - t), P_\beta(t)).$$

The height of $Q(Z)$ can be bounded using the Sylvester determinant for the resultant:

$$\mathit{res}_t(F(t), G(t))$$
$$= \det \begin{pmatrix} f_0 & f_1 & f_2 & \cdots & 0 & 0 & 0 \\ 0 & f_0 & f_1 & \cdots & 0 & 0 & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & f_{m-1} & f_m & 0 \\ 0 & 0 & 0 & \cdots & f_{m-2} & f_{m-1} & f_m \\ g_0 & g_1 & g_2 & \cdots & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & 0 & 0 & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & g_{n-1} & g_n & 0 \\ 0 & 0 & 0 & \cdots & g_{n-2} & g_{n-1} & g_n \end{pmatrix}.$$

Identifying $F(t)$ with $P_\alpha(Z-t)$ and $G(t)$ with $P_\beta(t)$, the Sylvester matrix is $(n + m) \times (n + m)$. There are n rows of f_i and m rows of g_j entries. The g_i are just the coefficients of the powers of Z in P_β. The f_i are linear combinations of coefficients of P_α and thus have the same height as P_α.

The determinant is a signed sum of products. Each product contains one element from each row in the matrix. Since we are only concerned with the degrees of the coefficients of $Q(Z)$ we can ignore the summation and focus on the products. The degree of u_i in each of the first n rows is bounded by $\operatorname{ht}\alpha$ and is bounded in the last m rows by $\operatorname{ht}\beta$. So we have

$$\operatorname{ht}(\alpha + \beta) \leqslant (\operatorname{ht}\alpha)^n (\operatorname{ht}\beta)^m.$$

For other algebraic operations, we know the following multiples of minimal polynomials, where a and b are elements of K.

$\alpha + \beta$	$\mathrm{res}_t(P_\alpha(Z - t), P_\beta(t))$
$\alpha - \beta$	$\mathrm{res}_t(P_\alpha(Z + t), P_\beta(t))$
$\alpha \times \beta$	$\mathrm{res}_t(t^n \cdot P_\alpha(Z/t), P_\beta(t))$
α/β	$\mathrm{res}_t(P_\alpha(tZ), P_\beta(t))$
$\sqrt[r]{\alpha}$	$\mathrm{res}_t(Z^r - t, P_\beta(t))$
$a\alpha + b$	$a^m P_\alpha((Z - b)/a)$

Since the size of the coefficients are not increased in any of the variations of P_α used, we have:

Proposition 4. *The heights of arithmetic combinations of algebraic functions can be bounded as follows:*

$$\begin{aligned}
\operatorname{ht} \alpha + \beta &\leqslant (\operatorname{ht} \alpha)^n (\operatorname{ht} \beta)^m, \\
\operatorname{ht} \alpha - \beta &\leqslant (\operatorname{ht} \alpha)^n (\operatorname{ht} \beta)^m, \\
\operatorname{ht} \alpha \cdot \beta &\leqslant (\operatorname{ht} \alpha)^n (\operatorname{ht} \beta)^m, \\
\operatorname{ht} \alpha / \beta &\leqslant (\operatorname{ht} \alpha)^n (\operatorname{ht} \beta)^m, \\
\operatorname{ht} \sqrt[r]{\alpha} &\leqslant (\operatorname{ht} \alpha)^r, \\
\operatorname{ht}(a\alpha + b) &\leqslant (\operatorname{ht} \alpha)(\operatorname{ht} a)^m.
\end{aligned}$$

Note that height of $\sqrt[r]{\alpha}$ is somewhat smaller than the other bounds since the height of $Z^r - t$ is 1.

4. Conclusions

We have extended the techniques for zero testing of polynomials to zero testing of algebraic functions. The key to this approach lies in estimating the size of the norm of the algebraic function, which we have shown can be done from a straight line program representing the algebraic function. This technique can be used to develop self-checkers and self-testers for programs that compute functions satisfying functional equations [6].

Ronitt Rubinfeld encouraged the writing of this note and made useful suggestions in its presentation.

Appendix. Polynomial zero testing theorems

The following two propositions are the basis of most zero testing algorithms. Proposition 5, a probabilistic result, is used in most computer algebra implementations. Variations of this result first appeared in [2,7,8]. Proposition 6 yields a deterministic zero testing technique; it was first given in [4].

Proposition 5. *Let $P \in A[Z_1, \dots, Z_v]$ be a polynomial of total degree D over an integral domain A. Let $\mathcal{S}$ be a subset of A of cardinality B. Then*

$$\mathcal{P}[(P(Z_1, \dots, Z_v) = 0 \mid Z_i \in \mathcal{S}] \leqslant \frac{D}{B}.$$

The following deterministic result depends on the number of *monomials* of a polynomial. A *monomial* is a product of constants and variables. Thus the polynomial

$$(x + y)^2 = x^2 + 2xy + y^2$$

has 3 monomials. Although $(x + y)^2$ could be written as the sum of four monomials $(x^2 + y^2 + xy + xy)$, all monomials with similar degree structure are combined. The following polynomial also has three non-zero monomials:

$$x^5 + y^5 + z^5.$$

Proposition 6. *Let $P(\vec{Z})$ be a polynomial in v variables over a ring of characteristic zero and assume that P has no more than T non-zero monomials. Then there exists a set of v-tuples, $\{\vec{Z}_0, \dots, \vec{Z}_{T-1}\}$ such that either $P(\vec{Z}_i) \neq 0$ for some $\vec{Z}_i$ or P is identically zero.*

Proof. One set of v-tuples that satisfies the requirements of the proposition is

$$\begin{aligned}
\mathcal{S} = \{&(1, 1, \dots, 1), (2, 3, \dots, q_v), \\
&\dots, (2^{T-1}, 3^{T-1}, \dots, q_v^{T-1})\}.
\end{aligned}$$

Write $P(\vec{Z}) = c_1 m_1(\vec{Z}) + c_2 m_2(\vec{Z}) + \cdots + c_T m_T(\vec{Z})$, where the m_i are distinct monomials in the Z_i. Denote the value of the monomial m_i at $(2^k, 3^k, \dots, q_v^k) \in \mathcal{S}$ by M_i^k. The M_i are distinct by unique factorization of the rational integers.

Assume that $P(\vec{Z})$ vanishes at each element of $\mathcal{S}$:

$$\begin{aligned}
c_1 + \cdots + c_T &= 0, \\
c_1 M_1 + \cdots + c_T M_T &= 0, \\
&\vdots \\
c_1 M_1^{T-1} + \cdots + c_T M_T^{T-1} &= 0.
\end{aligned}$$

The only solution to this Vandermonde system of equations is $c_i = 0$. □

A thorough discussion of zero testing techniques is given in [9].

References

[1] J.F. Canny, *The Complexity of Robot Motion Planning* (MIT Press, Cambridge, MA, 1987).

[2] R.A. Demillo and R.J. Lipton, A probabilistic remark on algebraic program testing, *Inform. Process. Lett.* 7 (4) (1978) 193-195.

[3] W. Morven Gentleman, Optimal multiplication chains for computing a power of a symbolic polynomial, *Math. Comput.* 26 (120) (1972) 935-939.

[4] D.Yu. Grigor'ev and M. Karpinski, The matching problem for bipartite graphs with polynomial bounded permanents is NC, in: *Proc. 28th Symp. on Foundations of Computer Science* (ACM, 1987) 166-172.

[5] S. Lang, *Algebra* (Addison-Wesley, Reading, MA, 3rd ed., 1993).

[6] R. Rubinfeld, On the robustness of functional equations, in: *Proc. 35th IEEE Conf. on the Foundations of Computer Science* (IEEE Press, 1994) 288-299.

[7] J.T. Schwartz, Probabilistic algorithms for verification of polynomials identities, *J. ACM* 27 (1980) 701-717.

[8] R.E. Zippel, Probabilistic algorithms for sparse polynomials, in: E. Ng, ed., *EUROSAM '79*, Lecture Notes on Computer Science, Vol. 72 (Springer, Berlin, 1979) 216-226.

[9] R.E. Zippel, *Effective Polynomial Computation* (Kluwer Academic Press, Boston, MA, 1993).