ON THE PROBLEM OF RECOGNIZING ZERO

S. C. Johnson
Bell Telephone Laboratories, Incorporated
Murray Hill, New Jersey

Abstract

The problem of recognizing when a complicated mathematical expression equals zero has great importance in symbolic mathematics. This paper gives two algorithms which can be applied to many such problems, and discusses two concrete examples.

The algorithms are based on the recognition that many interesting functions (such as exponentiation) are eigenvectors of well studied transformations (such as differentiation).

1. Introduction

The problem of dealing with general mathematical expressions by computer has been intensively studied. Brown,[1] Moses,[2] and Risch[3] all define environments in which some success can be obtained in doing arithmetic operations and integration within certain classes of functions. On the other hand, Richardson[4] and Caviness[5] have shown that the problem of recognizing when a mathematical expression is identically zero is undecidable for certain other classes of functions.

The aim of this paper is to state and prove two algorithms which can be applied to many such problems, and to discuss several concrete examples. The algorithms are concerned with deciding when complex mathematical expressions are identically zero. This problem is important in symbolic mathematics for several reasons:

(1) Formal division by an expression equal to zero can lead to incorrect results.

(2) Subexpressions equal to zero tend to proliferate exponentially if not found and removed.

(3) The general problem of simplification is closely connected with the problem of recognizing zero.

The algorithms will be stated in a general mathematical context. This leads to some difficulties of exposition, as the language of vector spaces is not well adapted to dealing with questions of effective computability and algorithm definition. Whenever there was a conflict between mathematical rigor and clarity of exposition, an attempt was made to yield to clarity.

2. Theory

This section is devoted to some vector space theory which will be applied to the remaining sections. The reader may find it profitable to read this section in parallel with the next two sections.

We shall assume that K is a field whose structure is known completely for our purposes. In particular, we shall assume that we can recognize zero in K.

We shall also assume a commutative ring R which contains K, and a mapping $\varphi : R \to R$.

Definition: An element $u \in R$, $u \neq 0$, is an eigenvector of φ if there is an element $a \in K$ with

$$\varphi(u) = au.$$

a is called the eigenvalue of u.

We shall denote by E the set of eigenvectors of φ.

At this point, we need to make a practical convention; when we write $u \in E$, we shall mean that we know not only u but also its eigenvalue. This has considerable practical importance, since the eigenvalue is in K, which we assume is well known.

Throughout the following, we will assume that φ satisfies these three axioms:

Axiom 1: $\varphi(u+v) = \varphi(u) + \varphi(v)$, all $u,v \in R$

Axiom 2: $\varphi(K) \subset K$, and $\varphi(1) = 0$

Axiom 3: If $u \in E$, then u is invertible and $u^{-1} \in E$. If $u,v \in E$, then $vu \in E$.

Recall that Axiom 3 implies, not merely that we know that u^{-1} and uv are eigenvectors, but also that we can construct their eigenvalues.

We now draw some simple consequences from the axioms, which can be quickly proved by the interested reader.

Axiom 1 implies that $\varphi(0) = 0$. Moreover, Axiom 2 implies that every nonzero element of K is an eigenvector. By Axiom 3, we thus deduce that

$$KE \subset E \cup \{0\},$$

and thus

$$\varphi(E) \subset E \cup \{0\}.$$

Thus, if u is an eigenvector, $\varphi(u)$ is either 0 or another eigenvector, whose eigenvalue can be computed.

Moreover, if $\varphi(u) = 0$ then the eigenvalue associated with u must be 0. Thus we can decide, for any eigenvector, whether $\varphi(u) = 0$ just by examining the eigenvalue.

The set of all u in R with $\varphi(u) = 0$, the kernel of φ (denoted $\ker(\varphi)$), is of central importance in this work. Notice that every nonzero element of $\ker(\varphi)$ is an eigenvector with eigenvalue = 0. There is no necessary

relationship, however, between $\ker(\varphi)$ and K except that they both contain 1.

We now describe the first zero recognition algorithm:

Algorithm 1

Suppose we have some algorithm for deciding, given $u \in \ker(\varphi)$, if $u = 0$. Then, given a sum $S = \sum_{i=1}^{n} u_i$, with $u_i \in E$, $i = 1,\ldots,n$, we may decide if $S = 0$ as follows:

Step 1: If $n = 1$, then $S \neq 0$. Return.

Step 2: If $n > 1$, then compute

$$T = \varphi(S/u_n)$$

and test it for zero. (See details below.)

Step 3: If $T \neq 0$ then $S \neq 0$. Return.

Step 4: If $T = 0$, then $S/u_n \in \ker(\varphi)$.

By assumption, we can test if $S/u_n = 0$.

Step 5: If $S/u_n \neq 0$, then $S \neq 0$. Return.

Step 6: If $S/u_n = 0$, then $S = 0$. Return.

It remains to explain step 2. We have:

$$S/u_n = \sum_{i=1}^{n} u_i/u_n$$

$$= 1 + \sum_{i=1}^{n-1} u_i/u_n$$

By Axiom 3, we may find the eigenvalues $b_1,\ldots,b_{n-1}$ for u_i/u_n. If any of the b_i are 0, delete the corresponding terms of the sum. If all the b_i are zero, then $T = \varphi(S/u_n) = 0$. Otherwise T is a sum of at most n - 1 eigenvectors with known eigenvalues, and we may apply algorithm 1 recursively to decide whether $T = 0$.

We may in fact go even farther in this direction. Suppose, as above, that we can decide when elements of $\ker(\varphi)$ are zero. Let $A_1,\ldots,A_n \in R$ have the property that $\varphi(A_i) \in E \cup \{0\}$, $i = 1,\ldots,n$. (Note that all elements of E have this property.) Then we may use the following algorithm to decide if $S = \sum_{i=1}^{n} A_i$ is zero:

Algorithm 2

Use Algorithm 1 to decide if $\varphi(S) = \sum_{i=1}^{n} \varphi(A_i)$ is zero. If $\varphi(S) \neq 0$ then $S \neq 0$. If $\varphi(S) = 0$, then S is in $\ker(\varphi)$, so we can decide if it is zero by assumption.

Clearly, this process may be extended to allow us to decide when a sum $\sum_{i=1}^{n} A_i$ is zero, provided only that each A_i can be transformed to a finite sum of eigenvectors by a finite number of applications of φ.

3. An Application

Let R be a field, and let φ be a derivation on R; that is, φ satisfies:

(1) Addition Law: $\varphi(a+b) = \varphi(a) + \varphi(b)$

(2) Multiplication Law: $\varphi(ab) = a\varphi(b) + b\varphi(a)$

The most common case of a derivation is when R is a field of infinitely differentiable functions, and φ is differentiation.

Let K be a subfield of R with $\varphi(K) \subset K$. Then we have

Theorem: The axioms of section two hold for φ.

Proof: Axiom 1 is precisely the addition law. Axiom 2 follows because $\varphi(K) \subset K$ and

$$\varphi(1\cdot 1) = 1\cdot\varphi(1) + 1\cdot\varphi(1)$$

or

$$\varphi(1) = \varphi(1) + \varphi(1)$$

so

$$\varphi(1) = 0.$$

Axiom 3 requires a bit of computation. Let u and v be eigenvectors with eigenvalues a and b. Then

$$\varphi(uv) = \varphi(u)v + u\varphi(v)$$

$$= (a+b)uv$$

$$\varphi(u^{-1}) = -u^{-2}\varphi(u) = -u^{-2}au$$

$$= (-a)u^{-1}$$

Thus uv and u^{-1} are eigenvectors, and we can compute their eigenvalues.

The eigenvectors of φ are a very interesting class of functions. They include

(1) Rational functions.

(2) ae^b, with a and b rational functions.

(3) b^α, with b a rational function and α any real number.

Algorithm 2 enables us to deal with functions A such that $\varphi(A)$ is an eigenvector; that is, indefinite integrals of eigenvectors. Thus we may include functions such as

(4) $\log b$, b a rational function.

(5) arctan x, arcsin x.

(6) $\mathrm{erf}(x) = \int_0^x e^{-x^2}\,dx.$

and many more.

The larger the class of functions examined, the larger $\ker(\varphi)$ is likely to be; this problem will be discussed in the next section.

4. Recognizing When an Element of $\ker(\varphi)$ is 0

The algorithms in Section 2 both depend strongly on being able to tell when an element of $\ker(\varphi)$ is in fact zero.

When φ is a derivation, $\ker(\varphi)$ is usually called the field of constants. When φ is ordinary differentiation, an element of $\ker(\varphi)$ must be constant on every interval on which it is defined. Thus we can frequently replace the problem of deciding when a constant function is zero by the problem of deciding when a constant expression, obtained by substitution, is zero. (As done in (4)).

For example, in the application of algorithm 1 we might find that differentiation of $e^{2x} - e^x.e^x$ yields 0. The problem is then to decide if $e^{2x} - e^x.e^x \in \ker(\varphi)$ is zero. Since all the functions are continuous and defined on the real line, the constant function is identically zero if and only if it attains the value zero at the point $x = 0$. Using the formula $e^0 = 1$, we see that the expression is in fact zero.

In general, the algebraic, or even linear, independence of numbers such as e, π, e^e, and so on, is not mathematically established at this time. Thus in many practical systems one is forced to make approximations or assumptions, and take the resultant risk (hopefully very small) of obtaining incorrect results based on incomplete mathematical knowledge. One example is the work of Brown,[1] where π and e were conjectured to be independent in a stronger sense than algebraically independent in order to obtain a simplification algorithm. Thus a failure of Brown's algorithm implies a very important mathematical theorem! An alternative approach might involve approximate evaluation of the constant function at a number of points using interval arithmetic, which would indicate immediately in most cases when the result was not identically 0. Constant functions which appeared to be 0 in all of these tests might be printed out, and then assumed to be 0 in later calculations.

5. Another Application

Let F be a field of rational functions over the integers. Let K be the field of rational functions over F in one variable m. Let R be a field of functions from the nonnegative integers to F such that R includes K. Define $\varphi : R \to R$ as

$$\varphi(u)(m) = u(m+1) - u(m),\quad u \in R,\ m \text{ any integer},$$

that is, φ is the first difference function.

We define

Definition: A function $u(m) \in R$ is factential if there is a rational function $a(m)$ with

$$u(m+1) = a(m)u(m)$$

Note that 2^m, $m!$, and $\binom{m}{n}$ are factential, but $2^m + 1$ and $(m^2)!$ are not. The name "factential" describes the fact that both factorial and exponential functions are factential.

We leave to the reader the following simple proposition.

Theorem:

(1) All rational functions are factential.

(2) Factential functions are closed under the operations of taking inverses and multiplication.

(3) The nonzero factential functions are precisely the eigenvectors of φ; if $u(m+1) = a(m)u(m)$, then the eigenvalue of u is $a(m) - 1$.

(4) φ satisfies the three axioms.

(5) $\ker(\varphi) = F \subset K$, since if $u \in \ker(\varphi)$, $u(m) = u(0) \in F$, for all m.

Because $\ker(\varphi)$ is a rational function field over the rational numbers, we may tell immediately when an element of $\ker(\varphi)$ is zero. Thus algorithm 1 can be used to allow us to tell when sums of factentials are identically zero.

Moreover, algorithm 2 allows us to deal with functions

$$A(m) = \sum_{i=0}^{m-1} u(i)$$

where u(m) is factential, since $\varphi(A) = u(m)$.

6. An Example

A short example of factential function simplification should give the flavor of the application of these algorithms.

We shall show that $\left(\sum_{i=0}^{n-1} 2^i\right) - 2^n + 1 = S(n)$ is identically 0. We use only that

(a) $2^{n+1} = 2 \cdot 2^n$ (The factential definition)

(b) $2^0 = 1$

Applying algorithm 2, we have

$$T(n) = \varphi(S(n)) = 2^n - (2-1)2^n + (1-1)$$

$$= 2^n - 2^n$$

Being particularly stupid, we treat this as a sum of two eigenvectors. Applying algorithm 1, we have

$$\varphi\left(\frac{T(n)}{2^n}\right) = \varphi(1) - \varphi\left(\frac{2^n}{2^n}\right)$$

$\frac{2^n}{2^n}$ is an eigenvector of φ, whose eigenvalue can be computed knowing only the eigenvalue of 2^n. The eigenvalue of $\frac{2^n}{2^n}$ is in fact 0. Thus $\varphi\left(\frac{T(n)}{2^n}\right) = 0$, so $\frac{T(n)}{2^n} = 1 - \frac{2^n}{2^n}$ is in $\ker(\varphi)$; and

$$\frac{T(n)}{2^n} \equiv \frac{T(0)}{2^0} = 1 - \frac{2^0}{2^0} = 1 - \frac{1}{1} = 0.$$

Thus T(n) is identically 0, so $S(n) \in \ker(\varphi)$. Thus, as before

$$S(n) \equiv S(0) \equiv 0 - 1 + 1 = 0$$

Thus S(n) is identically 0.

7. An Open Problem

Sums such as

$$\sum_{i=0}^{m-1} u(i),$$

with u(i) factential, are of some practical use; however, it would be much more interesting if m could appear inside the summation as well as being a limit.

For example, in the last section we proved

$$2^m - 1 = \sum_{i=0}^{m-1} 2^i$$

but we cannot prove

$$2^m = \sum_{i=0}^{m} \binom{m}{i}.$$

Most of the interesting binomial identities are of this second type.

This problem seems very difficult. For example, examine

$$S(m) = \sum_{i=0}^{m-1} u(m,i)$$

with u(m,i) rational in m and i. Then for which functions u is S rational? Clearly if there is a rational function v(m,i) with

$$v(m,i+1) - v(m,i) = u(m,i)$$

then

$$S(m) = \sum_{i=0}^{m-1} (v(m,i+1) - v(m,i)) = v(m,m) - v(m,0)$$

is rational.

We conjecture that S(m) is rational if and only if there is such a rational v(m,i); a general proof seems quite difficult.

Special cases of this problem include inquiring if, for any rational function u(m), the functions

$$\sum_{i=0}^{m-1} \frac{1}{i+u(m)}, \quad \sum_{i=0}^{m-1} \frac{1}{i^2+u(m)}, \quad \text{or} \quad \sum_{i=0}^{m-1} \frac{i}{i^2+u(m)}$$

are rational. A number of methods have been successful in these cases and others, however.

References

1. Brown, W. S., Rational Exponential Expressions and a Conjecture Concerning π and e, American Math. Monthly, 76, (1969), 28-34.

2. Moses, J., The Integration of a Class of Special Functions with the Risch Algorithm, SIGSAM Bulletin, 13, December 1969.

3. Risch, R. H., The Problem of Integration in Finite Terms, Trans. Am. Math. Soc., 139 (1969), pp. 167-189.

4. Richardson, D., Some Unsolvable Problems Involving Elementary Functions of a Real Variable, J. Symbolic Logic 33 (1968), pp. 514-520.

5. Caviness, B. F., On Canonical Forms and Simplification, Journal of the ACM, 17, (1970), pp. 385-396.