On Canonical Forms and Simplification

B. F. CAVINESS*

Carnegie-Mellon University, Pittsburgh, Pennsylvania

ABSTRACT. This paper deals with the simplification problem of symbolic mathematics. The notion of canonical form is defined and presented as a well-defined alternative to the concept of simplified form. Following Richardson it is shown that canonical forms do not exist for sufficiently rich classes of mathematical expressions. However, with the aid of a number-theoretic conjecture, a large subclass of the negative classes is shown to possess a canonical form.

KEY WORDS AND PHRASES: symbolic mathematics, nonnumerical mathematics, formula manipulation, simplification, canonical form, normal form, standard form, exponential expressions

CR CATEGORIES: 5.10, 5.20

1. *Introduction*

Formula manipulation is the process of carrying out operations and transformations on mathematical expressions or formulas. In formula manipulation processes, expressions with unnecessarily complicated structures are invariably generated. For example, most differentiation algorithms, when applied to the expression $x^2 + x(e^{e^3+2}) + 1$ will produce an expression similar to

$$2x^1 + 1(e^{e^3+2}) + x(0 \cdot e^3 + 0)(e^{e^3+2}) + 0 \tag{1}$$

instead of the functionally equivalent and structurally simpler expression

$$2x + e^{e^3+2}. \tag{2}$$

Such behavior seems to be intrinsic to most formula manipulation algorithms. The process of transforming expressions like (1) into a simpler equivalent form like (2) is called *simplification*. Simplification is also taken to embrace other kinds of transformations, such as reducing rational expressions by factoring out greatest common divisors, lexicographical ordering of subexpressions appearing in sums and products, etc.

There are at least three important reasons for keeping expressions in a simplified form. First of all, simplified expressions usually require less memory. Second, the processing of simplified formulas is faster and simpler. The processing is simpler in the sense that simplified formulas usually possess nice features which make possible cleaner and more precise algorithm design. Third, functionally equivalent expressions are easier to identify when they are in simplified form. Indeed, simplification is of such a nature that almost no formula manipulation program can do without simplification capabilities.

Given the central role of simplification, it is hardly surprising to find that many

* Present address: Department of Mathematics, Duke University, Durham, N.C. This work was supported in part by an NSF graduate fellowship and by the Advanced Research Projects Agency of the Office of the Secretary of Defense (SD-146).

algorithms for performing simplification have been reported in the literature. See Sammet's bibliographies [18, 19] for a listing of these. The usual form of attack of these algorithms has been to take a set of simplifying transformations that apply in obvious local cases and to try to weld these into a stable and coherent global scheme for simplifying a class of expressions. The need for simplification and the kind of simplification transforms needed seem obvious in simple cases. However, as expressions and algorithms increase in complexity, the answers are no longer so obvious.

Fenichel [8], Moses [11], and Tobey, Bobrow, and Zilles [20] have discussed the problems of the simplification algorithms in some detail. One of the main conclusions to be drawn from their discussions is that simplification has meaning only in a local context. For instance, Fenichel points out that $\csc^2(x) - \cot(x)\csc(x)$ is easier to integrate than its structurally simpler equivalent $1/[1 + \cos(x)]$. Thus in the context of integration the former expression is simpler, whereas in other cases the latter is considered simpler.

Recently Richardson [15] provided some theoretical evidence of simplification problems. He proved that for sufficiently rich classes of expressions it is impossible to identify all expressions which are identically zero. Hence no set of local simplification transforms such as $x - x \to 0$ can be sufficient for Richardson's class of expressions.

In this paper we study simplification through the concepts of canonical and normal forms. These global concepts, as developed in Section 3, are formalized alternatives to the ill-defined notion of a simplified form and hence are appropriate for a careful study. The structures of some common classes of expressions are studied and canonical (or normal) forms are shown to exist for these classes.

Some of the results of Section 4 are similar to results obtained by others. Results of W. S. Brown [2] and Richardson [16] are discussed later. P. J. Brown [1] has written an interesting paper in which he studies the existence of canonical forms in a more general setting than we have. A paper by G. Rousseau [17] attacks some problems similar to ours in a somewhat different realm. He proves the existence of an effective procedure for deciding whether or not functions contained in a subclass of the primitive recursive functions are identically zero. (This problem is recursively undecidable for the class of all primitive recursive functions.)

This paper is itself a revision of parts of [3].

2. *Undecidability Results*

From Richardson's theorem we know that canonical forms cannot exist for certain classes of expressions. In order to limit the search for canonical forms, it is desirable to have as much information as possible about negative results. Thus in this section Richardson's theorem and proof are studied in detail. From Richardson's proof and from studies on the unsolvability of Hilbert's tenth problem, some conclusions about sharpenings of Richardson's theorem are drawn.

To be given a *class of expressions* $\mathcal{E}$ means to be given an effective set of rules for determining the well-formed expressions in the class. The expressions must be formed from a finite set of atomic symbols of which a subset must be designated as *variables*. Any member of $\mathcal{E}$ not containing a variable is called an $\mathcal{E}$-*constant* or *constant* $\mathcal{E}$*-expression.* The expressions are to be interpreted as functions over some domain $\mathfrak{D}$.

If E_1 and E_2 are members of an expression class $\mathcal{E}$, E_1 is said to be *identical* to E_2 if E_1 and E_2 are the same string of atomic symbols. This relation is denoted by $E_1 \equiv E_2$. E_1 and E_2 are *functionally equivalent* or simply *equivalent* if for all assignments of values in $\mathfrak{D}$ to their variables for which they are defined, they are equal. This relation is denoted by $E_1 = E_2$.

In all the classes $\mathcal{E}$ of this section and Section 4 all the expressions are to be interpreted as single-valued elementary functions of one or more variables over the domain $\mathfrak{D}$ of $\mathcal{E}$-constants. Richardson's theorem provides us with a basis for our undecidability results.

THEOREM. *Let* $\mathcal{R}$ *consist of the class of expressions generated by*

(*i*) *the rational numbers and the two real numbers* π *and* $\log_e 2$,

(*ii*) *the variable* x,

(*iii*) *the operations of addition, multiplication, and composition, and*

(*iv*) *the sine, exponential, and absolute value functions.*

If $E \in \mathcal{R}$, *the predicate "*$E = 0$*" is recursively undecidable.*

This decision problem will be referred to as Richardson's decision problem. (Informal descriptions such as the above will be used in the text to describe expression classes. BNF (Backus-Naur form) definitions for some classes can be found in the Appendix.)

In order to derive some further results that follow from the proof of this theorem, the proof is included here. For the proof a variation of the class $\mathcal{R}$ is needed. Let $\mathcal{R}_1$ be the class of expressions generated by

(i) the rational numbers and the real numbers π and $\log_e 2$,

(ii) the variables $x_1, x_2, \cdots, x_n$,

(iii) the operations of addition, multiplication, and composition, and

(iv) the sine and exponential functions.

$\mathcal{R}_1$ differs from $\mathcal{R}$ by containing an arbitrary number of variables and by not containing the absolute value function.

Richardson shows that for $G(x_1)$ in $\mathcal{R}_1$ ($G(x)$ is a member of $\mathcal{R}$ since G is an expression of only one variable), the predicate "there exists a real number a such that $G(a) < 0$" is recursively undecidable. This decision problem will be referred to as the decision problem for $\mathcal{R}_1$. Now suppose that Richardson's decision problem is decidable and $G(x_1)$ is in $\mathcal{R}_1$. Consider $F(x) = |G(x)| - G(x)$. $F(x)$ is in $\mathcal{R}$ and $F(x) \neq 0$ if and only if there exists a constant b in $\mathcal{R}$ such that $G(b) < 0$. Since the constants of $\mathcal{R}$ (and $\mathcal{R}_1$) are dense in the reals and all expressions represent continuous real functions, there exists a real b such that $G(b) < 0$ if and only if there exists a b in $\mathcal{R}_1$ such that $G(b) < 0$. Thus if we can decide if $F(x) = 0$, we can decide if there exists a real b such that $G(b) < 0$. Except for the proof of the undecidability of the decision problem for $\mathcal{R}_1$, the proof of Richardson's theorem is complete.

The proof of the undecidability of the decision problem for $\mathcal{R}_1$ will be presented as a series of lemmas. The starting point is a variation by Davis [5] of a result of Davis, Putnam, and Robinson [7].

THEOREM. *Let* S *be a recursively enumerable set of nonnegative integers. For some polynomial* $\bar{P}(s, x_1, \cdots, x_n, x_{n+1})$, *with integral coefficients*, $S = \{s \mid$ *there exist nonnegative integers* $a_1, \cdots, a_n$ *such that* $\bar{P}(s, a_1, \cdots, a_n, 2^{a_n}) = 0\}$.

Since there exist recursively enumerable sets which are not recursive, we have immediately:

COROLLARY. *There exists a subset of* $\mathcal{R}_1$, *say* $\mathcal{P} = \{P(x_1, \cdots, x_n)\}$, *of polynomials with integral coefficients in* $x_1, \cdots, x_n, 2^{x_n}$ *such that the predicate "there exist nonnegative integers* $a_1, \cdots, a_n$ *such that* $P(a_1, \cdots, a_n) = 0$*" is recursively undecidable.*

Now consider

LEMMA 1. *For every* F *in* $\mathcal{R}_1$ *there is a* G *in* $\mathcal{R}_1$ *such that (i)* $G(x_1, \cdots, x_n) > 1$ *for all real* $x_1, \cdots, x_n$, *and (ii)* $G(x_1, \cdots, x_n) > F(x_1 + \Delta_1, \cdots, x_n + \Delta_n)$ *for all real* x_i *and all real* Δ_i *satisfying* $|\Delta_i| < 1$, $i = 1, \cdots, n$.

G is called a *dominating function* for F.

PROOF. The proof follows easily by induction on the number of operators and functions in the expression for F.

Using Davis's theorem and Lemma 1 Richardson proves:

LEMMA 2. *For each* P *in* $\mathcal{P}$ *there exists* F *in* $\mathcal{R}_1$ *such that (i) there exists an n-tuple of nonnegative integers* $\mathbf{a} = (a_1, \cdots, a_n)$ *such that* $P(\mathbf{a}) = 0$ *if and only if (ii) there exists an n-tuple of nonnegative real numbers* $\mathbf{b} = (b_1, \cdots, b_n)$ *such that* $F(\mathbf{b}) < 0$.

PROOF. Let P be an arbitrary member of $\mathcal{P}$. Observe that $(\partial/\partial x_i)P^2$, $i = 1, \cdots, n$, is in $\mathcal{R}_1$. Let K_i be the dominating function for $(\partial/\partial x_i)P^2$. Define F by

$$F(x_1, \cdots, x_n) = (n + 1)^2[P^2(x_1, \cdots, x_n) + \sum_{i=1}^{n} (\sin^2 \pi x_i)K_i^2(x_1, \cdots, x_n)] - 1.$$

Obviously (i) implies (ii). To show that (ii) implies (i), choose a_i to be the smallest integer such that $|a_i - b_i| \le \frac{1}{2}$. We shall show that $P^2(\mathbf{a}) < 1$ which implies that $P(\mathbf{a}) = 0$ since P maps nonnegative integers into integers. $F(\mathbf{b}) < 0$ implies that

$$P^2(\mathbf{b}) + \sum_{i=1}^{n} (\sin^2 \pi b_i)K_i^2(\mathbf{b}) < 1/(n + 1)^2.$$

Hence $P^2(\mathbf{b}) < 1/(n + 1)$ and $|\sin \pi b_i| K_i(\mathbf{b}) < 1/(n + 1)$, $i = 1, \cdots, n$. By the n-dimensional mean value theorem

$$P^2(\mathbf{a}) \le P^2(\mathbf{b}) + \sum_{i=1}^{n} |a_i - b_i| \frac{\partial}{\partial x_i} P^2(c_1, \cdots, c_n),$$

where c_i is between a_i and b_i. From the definition of K_i,

$$P^2(\mathbf{a}) < P^2(\mathbf{b}) + \sum_{i=1}^{n} |a_i - b_i| K_i(\mathbf{b}).$$

Since $|a_i - b_i| \le \frac{1}{2}$, we have $|a_i - b_i| \le |\sin \pi b_i|$; hence

$$P^2(\mathbf{a}) < P^2(\mathbf{b}) + \sum_{i=1}^{n} |\sin \pi b_i| K_i(\mathbf{b}).$$

Now since each of the $n + 1$ terms on the right is less than $1/(n + 1)$, we have $P^2(\mathbf{a}) < 1$, as was to be shown.

COROLLARY. *For* F *in* $\mathcal{R}_1$ *the predicate "there exists an n-tuple* $\mathbf{b}$ *of real numbers such that* $F(\mathbf{b}) < 0$*" is recursively undecidable.*

PROOF. Consider F as defined in Lemma 2. If we could decide if there exists an n-tuple $\mathbf{b}$ of real numbers such that $F(b_1^2, \cdots, b_n^2) < 0$, then we could decide, by

Lemma 2, if there exists an n-tuple $\mathbf{a}$ of nonnegative integers such that $P(\mathbf{a}) = 0$. But from the corollary to Davis's theorem, this is not possible.

The next lemma will enable us to obtain the above corollary for expressions with only one variable.

LEMMA 3. *Let $h(x) = x \sin x$ and $g(x) = x \sin x^3$. Then for any real numbers $a_1, \cdots, a_n$ and any $0 < \epsilon < 1$ there exists $b > 0$ such that*

$$|h(b) - a_1| < \epsilon, \quad |h(g(b)) - a_2| < \epsilon, \quad \cdots, \quad |h(g(\cdots g(b) \cdots)) - a_n| < \epsilon.$$

PROOF. The proof is by induction on n. Richardson first shows that for any two real numbers a_1 and a_2 there exists $b > 0$ such that $|h(b) - a_1| < \epsilon$ and $g(b) = a_2$. Suppose the lemma is true for n. Then there exists b' such that

$$|h(b') - a_2| < \epsilon, \quad |h(g(b')) - a_3| < \epsilon, \quad |h(g(\cdots(g(b'))\cdots)) - a_{n+1}| < \epsilon.$$

By the preceding statement there exists $b > 0$ such that $|h(b) - a_1| < \epsilon$ and $g(b) = b'$. Hence the result holds for $n + 1$.

COROLLARY. *For $G(x_1)$ in $\mathcal{R}_1$ the predicate "there exists a real number a such that $G(a) < 0$" is recursively undecidable.*

(Note that $G(x)$ is in $\mathcal{R}$.)

PROOF. Let $F(x_1, \cdots, x_n)$ be in $\mathcal{R}_1$ and consider

$$G(x_1) = F(h(x_1), h(g(x_1)), \cdots, h(g(\cdots(g(x_1))\cdots))).$$

Then there exists such an a if and only if there exist real numbers $b_1, \cdots, b_n$ such that $F(b_1, \cdots, b_n) < 0$.

This corollary proves the undecidability of the decision problem for $\mathcal{R}_1$ and hence completes the proof of Richardson's theorem.

Now let us consider some implications of the undecidability of Hilbert's tenth problem. In particular if Hilbert's tenth problem is undecidable then Richardson's result holds for a proper subset of $\mathcal{R}$. Hilbert's tenth problem refers to one of the problems that David Hilbert [9] listed in a famous presentation in 1900. The problem is the one of deciding if an arbitrary polynomial (arbitrary with respect to degree and number of variables) with integral coefficients has integral roots. The problem is still unresolved but the evidence to date [4–7] suggests that the problem is recursively undecidable.

Let $\mathcal{R}_2$ be the class of expressions generated by

(i) the rational numbers and the real number π,
(ii) the variable x,
(iii) the operations of addition, multiplication, and composition, and
(iv) the sine and absolute value functions.

Note that $\mathcal{R}_2$ is a proper subclass of $\mathcal{R}$ since it contains neither $\log_e 2$ nor the exponential function.

THEOREM 1. *If Hilbert's tenth problem is recursively undecidable then for $E(x)$ in $\mathcal{R}_2$ the predicate "$E(x) = 0$" is recursively undecidable.*

The proof is almost identical to the proof of Richardson's theorem. The unsolvability of Hilbert's tenth problem corresponds to the unsolvability of the exponential equations of Davis, Putnam, and Robinson. Thus by hypothesis if $P(x_1, \cdots, x_n)$ is a polynomial with integral coefficients, the predicate "there exist integers $a_1, \cdots, a_n$ such that $P(a_1, \cdots, a_n) = 0$" is recursively undecidable. The correspondent to Lemma 2 is

LEMMA 2′. *For each polynomial $P(x_1, \cdots, x_n)$ with integral coefficients there exists $F(x_1, \cdots, x_n)$ in $\mathcal{R}_3$ (where $\mathcal{R}_3$ is to $\mathcal{R}_2$ as $\mathcal{R}_1$ is to $\mathcal{R}$) such that (i) there exist integers $a_1, \cdots, a_n$ such that $P(a_1, \cdots, a_n) = 0$ if and only if (ii) there exist real numbers $b_1, \cdots, b_n$ such that $F(b_1, \cdots, b_n) < 0$.*

The proof is exactly like the proof of Lemma 2 except that

$$F = (n+1)^2\left[P^2 + \sum_{i=1}^{n} (\sin^2 \pi x_i)K_i^2\right] - 1$$

does not contain the term $2^{x_n} = \exp(x_n \log_e 2)$ as the F of Lemma 2 does. The remainder of the proof of Theorem 1 is exactly like the proof of Richardson's theorem.

3. *Canonical and Normal Forms*

In this section the definitions of canonical and normal forms are given along with sufficient conditions for the existence of a canonical form.

An *f-normal form* for a class of expressions $\mathcal{E}$ is a computable mapping f from $\mathcal{E}$ into $\mathcal{E}$ that satisfies the following two properties for all E in $\mathcal{E}$:

(i) $f(E) = E$, and
(ii) if $E = 0$, $f(E) \equiv 0$.

An *f-canonical form* is an f-normal form with the additional uniqueness property that for all E_1, E_2 in $\mathcal{E}$ such that $E_1 = E_2$, $f(E_1) \equiv f(E_2)$. If the particular f is clear from context or if the f is arbitrary, we shall frequently drop the prefix and simply use canonical (normal) form. If E is an expression such that $f(E) \equiv E$ then E is said to be *in (f-) canonical* (normal) *form*. A class of expressions is called a *canonical* (normal) *class* or is said to *possess a canonical* (normal) *form* if there exists a canonical (normal) form for it.

For a given set of expressions $\mathcal{E}$ and a canonical (normal) form f for $\mathcal{E}$, the members of the set $f(\mathcal{E})$ of canonical expressions will usually have a certain "form." For example, one canonical form for the polynomials with rational coefficients maps each polynomial into the "form" $r_0 + r_1x + \cdots + r_nx^n$, where the r_i's are rational numbers in canonical form. We call generalized expressions like $r_0 + r_1x + \cdots r_nx^n$ *patterns*. A particular expression E is said to be an instance of the pattern P if E matches P. This relation is denoted by $E == P$. Thus x and $1 + 3x^2$ are instances of the above polynomial pattern but $(2 + 5x)(x^2 + x^3)$ is not.

The pattern concept is useful in describing canonical (normal) forms. But patterns are more than descriptive devices in that the pattern associated with a canonical (normal) form embodies much vital information about the form. It may be that a careful formalization of the pattern concept may lead to further results about canonical (normal) forms. However, in this paper we concentrate on the equivalence problem and only use the pattern concept for descriptive purposes. Hence it is not formalized here. (This discussion of patterns uses the terminology and symbolism of FORMULA ALGOL [10, 13, 14].)

Frequently it is necessary to know that a total ordering can be imposed on a class of expressions. Usually this can be done in several different ways, but note that it can always be done with a lexicographical scheme.

Now sufficient conditions for the existence of a canonical form will be given. Given a class $\mathcal{E}$, closed under multiplication, a subclass $\mathcal{E}_2$ is linearly independent over a subclass $\mathcal{E}_1$, if for A_i in $\mathcal{E}_1$, X_i in $\mathcal{E}_2$, $X_i \not\equiv X_j$, $A_1X_1 + \cdots + A_nX_n = 0$ implies that $A_1 = A_2 = \cdots = A_n = 0$.

THEOREM 2. *Let $\mathcal{E}$ be a class of expressions closed under multiplication. Suppose $\mathcal{E}_1$ and $\mathcal{E}_2$ are subclasses of $\mathcal{E}$ with the following two properties: (i) $\mathcal{E}_1$ and $\mathcal{E}_2$ possess canonical forms f_1 and f_2 respectively, and (ii) $f_2(\mathcal{E}_2)$ is linearly independent over $\mathcal{E}_1$.*

Let $f_2(\mathcal{E}_2):f_1(\mathcal{E}_1)$ denote the set of all expressions $A_1X_1 + \cdots + A_nX_n$, where

(i) A_i, X_i are in $f_1(\mathcal{E}_1)$, $f_2(\mathcal{E}_2)$ respectively,

(ii) $A_i \not\equiv 0$ for $i = 1, \cdots, n$, and

(iii) $X_i \ll X_j$ if $i < j$, where $\ll$ is any total ordering on $\mathcal{E}_2$. If f is a computable mapping from $\mathcal{E}$ into $f_2(\mathcal{E}_2):f_1(\mathcal{E}_1) \cup \{0\}$ such that $f(E) = E$, then f is a canonical form for $\mathcal{E}$.

PROOF. It is only necessary to show that $E_1 = E_2$ implies that $f(E_1) \equiv f(E_2)$. Suppose $f(E_1) \equiv A_1X_1 + \cdots + A_kX_k$ and $f(E_2) \equiv B_1Y_1 + \cdots + B_mY_m$. Let $\{Z_1, \cdots, Z_n\}$ be the distinct members of $f_2(\mathcal{E}_2)$ occurring among the X_i and Y_i. Also assume the Z_i's are in ascending order. Then

$$f(E_1) - f(E_2) = C_1Z_1 + \cdots + C_nZ_n = 0,$$

where

$$C_l \equiv \begin{cases} A_i - B_j & \text{for some } i \text{ and } j \text{ if } Z_l \text{ appears in both } f(E_1) \text{ and } f(E_2), \\ A_i & \text{if } Z_l \text{ appears in } f(E_1) \text{ but not in } f(E_2), \\ -B_j & \text{otherwise.} \end{cases}$$

By linear independence $f(E_1) - f(E_2) = 0$ if and only if $C_l = 0$, $l = 1, \cdots, n$. Since $A_i, B_j \not\equiv 0$, $A_i, B_j \neq 0$. Hence $C_l \equiv A_i - B_j = 0$, which implies that $A_i \equiv B_j$ since A_i and B_j are in canonical form. Thus $n = m = k$, $X_i \equiv Y_i \equiv Z_i$, and $A_i \equiv B_i$, $i = 1, \cdots n$. Hence $f(E_1) \equiv f(E_2)$.

This theorem is almost self-evident. Its purpose is to point out the main technique used herein to obtain new canonical forms, i.e. mapping classes of expressions into subclasses which are linear manifolds whose coefficient and basis sets are already known to possess canonical forms.

4. *Canonical and Normal Forms for Exponential Expressions*

In this section canonical and normal forms for variations of the Richardson class $\mathcal{R}$ are presented. For simplicity, all results are stated and proved for one variable, although all results hold for an arbitrary number of variables. All the proofs depend heavily on number theoretic considerations. The first proof uses Lindemann's theorem (cf. [12, p. 117]).

THEOREM (Lindemann). *Suppose $a_1, \cdots, a_k$ are distinct algebraic numbers. Then the set $\{e^{a_1}, \cdots, e^{a_k}\}$ is linearly independent over the algebraic numbers.*

Now consider the class FOE of first-order exponential expressions generated by

(i) the rationals and the complex constant i,

(ii) the variable x,

(iii) the operations of addition, multiplication, and restricted composition, and

(iv) the exponential function.

Restricted composition means that the exponential function may not be nested, i.e. expressions like $\exp(\exp(x) + 1)$ are not permitted. See the Appendix for a more rigorous definition of the class FOE. The class FOE contains as a subclass the class $\mathcal{P}$ of polynomials over the field of complex rationals. $\mathcal{P}$ possesses a canonical form.

THEOREM 3. *Let $S_1, \cdots, S_k$ be distinct canonical members of $\mathcal{P}$. Then the set $\{\exp(S_1), \cdots, \exp(S_k)\}$ is linearly independent over $\mathcal{P}$.*

PROOF. Suppose $P_1(x)\exp(S_1) + \cdots + P_k(x)\exp(S_k) = 0$ where P_i, $i = 1, \cdots, k$, is in $\mathcal{P}$. Since a polynomial has only finitely many roots, there are only finitely many rationals r such that for $i \neq j$, $S_i(r) = S_j(r)$. Thus there are infinitely many rationals r such that $S_1(r), \cdots, S_k(r)$ are distinct numbers. Hence by Lindemann's theorem, for each such r, $P_i(r) = 0$, $i = 1, \cdots, k$. Hence $P_i = 0$ and the linear independence is established.

COROLLARY 3.1. *There exists a canonical form f for the first-order exponentials that maps each FOE into an instance of the pattern $P_1 \exp(S_1) + \cdots + P_k \exp(S_k)$, where the P_i are nonzero canonical members of $\mathcal{P}$ and the S_i are canonical members of $\mathcal{P}$ with the property that $S_i \ll S_j$ if $i < j$.*

PROOF. Each FOE can be straightforwardly mapped into such an equivalent form by application of the transformations $\exp(E_1)\exp(E_2) \rightarrow \exp(E_1 + E_2)$ $\exp(0) \rightarrow 1$. The fact that such a mapping is canonical follows from Theorems 2 and 3.

This corollary obviously will still hold if the class FOE is expanded to include trigonometric functions that can be expressed in terms of exponentials. If the division operator is introduced a normal form exists that maps each expression into a quotient of canonical expressions of the form $P_1 \exp(R_1) + \cdots + P_k \exp(R_k)$ where the P_i are polynomials and the R_i are rational function expressions. In the FOE expressions composition is limited. This limitation may be removed by using a conjectured generalization of Lindemann's theorem.

Consider the class of exponential expressions generated by

(i) the rationals and i,
(ii) the variable x,
(iii) the operations of addition, multiplication, and composition, and
(iv) the exponential function.

The *order* of an exponential expression is the maximum number of nestings of the exp function. For example, all polynomials are of order 0, all FOE's are of order less than or equal to 1, and

$$\exp(\exp(\exp(x + 2) + 3i)) + \exp(x^2 + 5) + x^{10} + 1$$

is of order 3.

For exponentials of order less than or equal to 1, Corollary 3.1 gives a canonical form. Each order 1 expression is mapped into an instance of the pattern

$$P_1 \exp(S_1) + \cdots + P_k \exp(S_k),$$

where the P_i are nonzero canonical polynomials and the S_i are distinct canonical polynomials in ascending order.

Now define the mapping f on the exponential expressions as follows. If E has order less than or equal to 1, then $f(E)$ is the equivalent instance of the above pattern. If f has been defined for expressions of order less than or equal to $n - 1$ and E has order n, $f(E)$ is the equivalent instance of the pattern

$$P_1 \exp(E_1) + \cdots + P_k \exp(E_k), \tag{3}$$

where the P_i are nonzero canonical polynomials and the E_i are f-form exponentials of order at most $n - 1$ with the property that $E_i \ll E_j$ if $i < j$.

CONJECTURE. *Suppose $E_1, \cdots, E_k$ are distinct f-form exponential constants. Then the set of constants $\{exp\ (E_1), \cdots, exp\ (E_k)\}$ is linearly independent over the rationals.*

If $E_1, \cdots, E_k$ are 0 order constants then the conjecture is a special case of Lindemann's theorem. However the proof of the conjecture, if true, appears to be beyond current boundaries of number theoretic research since little seems to be known about such specific numbers as e^e. The conjecture implies that e^e is transcendental.

THEOREM 4. *If the above conjecture is true, f is a canonical form for the exponential expressions.*

PROOF. If E and E' are exponential expressions, it is only necessary to show that $f(E) \not\equiv f(E')$ implies that $E \neq E'$. It is clear from the definition of f that $f(f(E) - f(E')) \not\equiv 0$ if $f(E) \not\equiv f(E')$. So it is sufficient to show that if E is an instance of (3) and $E \not\equiv 0$, then $E \neq 0$. The proof is by induction on n, the order of E. By Theorem 3 the result holds when $n \leq 1$. Assume the result holds for all instances of (3) with order less than n. Let

$$E(x) = P_1(x) \exp (E_1(x)) + \cdots + P_k(x) \exp (E_k(x))$$

be an expression of order n. Assume $E(x) = 0$. Then for each rational r in any finite closed real interval I, $E(r) = 0$. By the conjecture this implies that either

(i) $P_i(r) = 0$ for $i = 1, \cdots, k$, or

(ii) there exist $1 \leq i < j \leq k$ such that $E_i(r) = E_j(r)$.

Since (i) or (ii) holds for every r in I, either (i) or (ii) holds for infinitely many r in I. Each exponential expression represents an entire analytic function and an analytic function is completely determined by its values at an infinite number of points on a closed interval. Thus either

(i) $P_i = 0$ for $i = 1, \cdots, k$, or

(ii) $E_i = E_j$.

But (i) does not hold by the definition of E and (ii) does not hold by the induction hypothesis. Hence $E \neq 0$.

If the division operator is allowed in the exponential expressions, the existence of a normal form may be shown with an argument similar to the above. Such a normal form g would map each well-defined expression into an equivalent instance of the pattern $[P_1 \exp (E_1) + \cdots + P_k \exp (E_k)]/[Q_1 \exp (F_1) + \cdots + Q_m \exp (F_m)]$, where each P_i, Q_i is a nonzero canonical member of $\mathcal{P}$ and each E_i, F_i is a g-form exponential with the properties that if $i < j$, $g(E_i - E_j) \not\equiv 0 \not\equiv g(F_i - F_j)$ and $E_i \ll E_j$, $F_i \ll F_j$.

This normal form is analogous to a normal form given by W. S. Brown [2] for the class $\mathcal{B}$ of expressions generated by

(i) the rationals, π, and i,

(ii) the variables $x_1, \cdots, x_n$ (denoted collectively by x),

(iii) the operations of addition, subtraction, multiplication, division, and composition, and

(iv) the exponential function.

He conjectures that if $E_1, \cdots, E_k$ are nonzero expressions in $\mathcal{B}$ such that the set $\{E_1, \cdots, E_k, i\pi\}$ is linearly independent over the rationals, then the set $\{\exp (E_1),$

$\cdots$, exp (E_k), x, $\pi\}$ is algebraically independent over the rationals. Using this conjecture he shows that there exists a normal form f for $\mathcal{B}$ that maps each expression into an equivalent expression of the form

$$\frac{g(\exp(E_1), \cdots, \exp(E_k), x, \pi, \omega_m)}{h(\exp(E_1), \cdots, \exp(E_k), x, \pi)},$$

where

(i) g and h are relatively prime polynomials over the rationals,

(ii) the degree of g in $\omega_m = \exp(i \cdot \pi/2m)$ is less than the degree of the minimal polynomial for ω_m,

(iii) $E_1, \cdots, E_k$ are distinct normalized expressions, and

(iv) the set $\{E_1, \cdots, E_k, i\pi\}$ is linearly independent over the rationals.

Richardson [16] has also proved a theorem that is somewhat similar to Theorem 4 and to Brown's theorem. He considers the class of expressions $\mathcal{S}$ generated by

(i) the rationals and π,

(ii) the variable x,

(iii) the operations of addition, subtraction, multiplication, division, and composition, and

(iv) the exponential, sine, cosine, and log $| x |$ functions.

THEOREM. *Given an expression E in $\mathcal{S}$, a finite sequence $E_1, \cdots, E_k$ of $\mathcal{S}$-expressions can be found such that if r is any rational number and I is any interval containing r on which $E(x)$ is totally defined, $E(x) = 0$ on I if and only if $E(r) = E_1(r) = \cdots = E_k(r) = 0$.*

However, no method is known for deciding, in general, whether $E(r) = 0$. Whether or not such a method exists is an open question.

5. *Conclusion*

In summary our knowledge of the boundary between decidability and undecidability is as follows. Without resorting to conjectures, the smallest class of expressions for which a negative result holds is $\mathcal{R}$. The largest class for which a positive result holds is FOE.

However, subject to a number of plausible conjectures, we can bring the boundary into much sharper focus. Consider the class $\mathcal{R}_2$ for which we have a negative result. If the absolute value function is removed from $\mathcal{R}_2$, one has a restricted case of Brown's positive result. If the sine function is removed, a class of polynomials extended by absolute value remains. In this case the immediately preceding theorem of Richardson implies the existence of a normal form.

Theorem 4 gives us our most general canonical form.

Appendix. Backus-Naur Form Definitions for Classes of Expressions

GENERAL DEFINITIONS

⟨nonzero digit⟩ ::= 1|2|3|4|5|6|7|8|9
⟨digit⟩ ::= ⟨nonzero digit⟩ | 0
⟨positive integer⟩ ::= ⟨nonzero digit⟩ | ⟨positive integer⟩⟨digit⟩
⟨integer⟩ ::= 0 | ⟨positive integer⟩ | − ⟨positive integer⟩
⟨rational⟩ ::= ⟨integer⟩ | ⟨integer⟩ / ⟨positive integer⟩
⟨variable⟩ ::= x

DEFINITION OF THE CLASS $\mathcal{R}$

⟨$\mathcal{R}$ primary⟩ ::= ⟨rational⟩ |π| *log* 2 | ⟨variable⟩ | (⟨$\mathcal{R}$⟩) | *sin* (⟨$\mathcal{R}$⟩) | *exp* (⟨$\mathcal{R}$⟩) | *abs* (⟨$\mathcal{R}$⟩)
⟨$\mathcal{R}$ term⟩ ::= ⟨$\mathcal{R}$ primary⟩ | ⟨$\mathcal{R}$ term⟩ * ⟨$\mathcal{R}$ primary⟩
⟨$\mathcal{R}$⟩ ::= ⟨$\mathcal{R}$ term⟩ | ⟨$\mathcal{R}$⟩ + ⟨$\mathcal{R}$ term⟩

Note. abs (⟨$\mathcal{R}$⟩) is also denoted | ⟨$\mathcal{R}$⟩ | where "|" is an absolute value bar.

DEFINITION OF THE FOE CLASS

⟨FOE argument primary⟩ ::= ⟨rational⟩ |i| ⟨variable⟩ | (⟨FOE argument⟩)
⟨FOE argument term⟩ ::= ⟨FOE argument primary⟩ | ⟨FOE argument term⟩ * ⟨FOE argument primary⟩
⟨FOE argument⟩ ::= ⟨FOE argument term⟩ | ⟨FOE argument⟩ + ⟨FOE argument term⟩
⟨FOE primary⟩ ::= ⟨FOE argument primary⟩ | (⟨FOE⟩) | exp (⟨FOE argument⟩)
⟨FOE term⟩ ::= ⟨FOE primary⟩ | ⟨FOE term⟩ * ⟨FOE primary⟩
⟨FOE⟩ ::= ⟨FOE term⟩ | ⟨FOE⟩ + ⟨FOE term⟩

ACKNOWLEDGMENT. I am grateful to Dr. A. J. Perlis for his guidance and encouragement during the course of this work. Also, the suggestions of the reviewers were most helpful.

REFERENCES

1. BROWN, P. J. Canonical forms and artificial languages. Mathematical Notes No. 19, Computation Center, U. of North Carolina, July 5, 1963.
2. BROWN, W. S. Rational exponential expressions and a conjecture concerning π and e. *Amer. Math. Mon. 76* (1969), 28–34.
3. CAVINESS, B. F. On canonical forms and simplification. Ph.D. Diss., Carnegie-Mellon U., Pittsburgh, Pa., Aug. 1967.
4. DAVIS, MARTIN. Diophantine equations and recursively enumerable sets. In E. R. Caioniello (Ed.), *Automata Theory*, Academic Press, New York, 1966, pp. 146–152.
5. ——. Extensions and corollaries of recent work on Hilbert's tenth problem. *Ill. J. Math. 7* (1963), 246–250.
6. —— AND PUTNAM, HILARY. Reductions of Hilbert's tenth problem. *J. Symbolic Logic 23* (1958), 183–187.
7. ——, ——, AND ROBINSON, JULIA. The decision problem for exponential diophantine equations. *Ann. Math. 74* (1961), 425–436.
8. FENICHEL, R. R. An on-line system for algebraic manipulation. Ph.D. Diss., Harvard U., Cambridge, Mass., 1966.
9. HILBERT, DAVID. Mathematische probleme. *Bull. Amer. Math. Soc. 8* (1901–1902), 437–479.
10. ITURRIAGA, R. Contributions to mechanical mathematics. Ph.D. Diss., Carnegie-Mellon U., Pittsburgh, Pa., 1967.
11. MOSES, JOEL. Symbolic integration. Ph.D. Diss., Massachusetts Inst. of Technology, Cambridge, Mass., Sept. 1967.
12. NIVEN, IVAN. *Irrational Numbers*. Wiley, New York, 1956. (Carus Mathematical Monographs, No. 11, Mathematical Ass. of Amer.)
13. PERLIS, A. J., AND ITURRIAGA, R. An extension to ALGOL for manipulating formulae. *Comm. ACM 7*, 2 (Feb 1964), 127–130.
14. ——, ——, AND STANDISH, T. A. A definition of Formula Algol. Computation Center, Carnegie-Mellon U., Pittsburgh, Pa., March 1966.
15. RICHARDSON, DANIEL. Some unsolvable problems involving elementary functions of a real variable. *J. Symbolic Logic 33* (1968), 514–520.
16. —— A solution of the identity problem for integral exponential functions. *Z. Math. Logik Grundlagen Math.* (to appear).

17. Rousseau, G. A decidable class of number theoretic equations. *J. London Math. Soc.* *41* (1966), 737–741.
18. Sammet, J. E. An annotated descriptor-based bibliography on the use of computers for non-numerical mathematics. *Comput. Rev.* *7* (1966), B1–B31.
19. ——. Modification No. 1 to an annotated descriptor-based bibliography on the use of computers for doing non-numerical mathematics. ACM SICSAM Bull., No. 5 (Dec. 1966), Appendix, pp. 1–19.
20. Tobey, R. G., Bobrow, R. J., and Zilles, S. N. Automatic simplification in FORMAC. Proc. AFIPS 1965 Fall Joint Comput. Conf., Vol. 27, Pt. 1, pp. 37–53.

RECEIVED NOVEMBER, 1968; REVISED SEPTEMBER, 1969