Simplification of Radical Expressions

by

B. F. Caviness[1]
Computer Science Department
Illinois Institute of Technology
Chicago, Illinois

and

R. J. Fateman
Computer Science Division
Department of Electrical Engineering and Computer Sciences
University of California at Berkeley
Berkeley, California

Abstract

In this paper we discuss the problem of simplifying unnested radical expressions. We describe an algorithm implemented in MACSYMA that simplifies radical expressions and then follow this description with a formal treatment of the problem. Theoretical computing times for some of the algorithms are briefly discussed as is related work of other authors.

1. Introduction

In this paper we discuss the problem of simplifying unnested radical expressions. By radical expressions we mean, roughly speaking, sums, differences, products, and quotients of rational functions raised to rational powers. Thus we will be discussing algorithms for carrying out transformations such as

$$\frac{x-y}{\sqrt{x}+\sqrt{y}} \to \sqrt{x} - \sqrt{y} \tag{1}$$

$$\frac{(x-1)^{1/4}}{(1-x)^{1/4}} - \frac{(x-1)^{3/4}}{(1-x)^{3/4}} - \sqrt{2} \to 0 \tag{2}$$

and $1/(x+\sqrt{2}+3^{2/3}) \to$

$$[((2x^3-4x-9)\sqrt{2} - x^4 - 9x + 4)3^{2/3}$$
$$+((-9x^2-6)\sqrt{2} + 3x^3 + 18x + 27)3^{1/3}$$
$$+(-x^4+4x^2+18x-4)\sqrt{2} + x^5 - 4x^3 + 9x^2 + 4x + 18]$$
$$/[x^5-6x^4+18x^3 + 12x^2 + 108x + 73]. \tag{3}$$

We will primarily consider only expressions in which the rational exponentiation is unnested, that is, like those expressions in (1), (2) and (3) above as opposed to expressions like $[(x+1)^{1/2}+(x-1)^{1/2}]^{1/2}$ in which the square root is nested.

(1) Present address: Department of Mathematical Sciences, Rensselaer Polytechnic Institute, Troy, N.Y. 12181

As is the case with all simplification problems there are three desirable attributes for any solution. First it is desirable to have a clean theoretical solution to the problem. Second the algorithms to carry out the simplifications should be as efficient as possible, and finally the solution should have good human engineering features, i.e., the use and actions of the simplification procedures should be as natural and transparent as possible. Unfortunately these three aspects of a solution are not usually compatible with each other and compromises and choices must be made. This is certainly the case for the simplification of radical expressions. Standard techniques from the theory of algebraic field extensions can be used to get a nice theoretical solution to the problem. However the nice theoretical solution neither leads to fast algorithms nor possesses nice human engineering features.

The theoretical solution involves finding an algebraic extension field of $Q(x_1,\ldots,x_n)$, the field of rational functions in $x_1,\ldots,x_n$ with coefficients in Q the field of rational numbers, to which the given radical expressions belong. In the algebraic extension field each element can be represented uniquely and this unique representation can be considered to be the simplified form for the given expression. Thus for example

$$\frac{2^{1/4}+3^{1/2}[-(x^2+1)]^{1/3}}{(x^2+1)^{1/2}} \tag{4}$$

is a member of the field $Q(x)[\omega_6, 2^{1/4}, 3^{1/2}, (x^2+1)^{1/6}]$. Each element of this field may be uniquely represented in the form

$$\alpha_0+\alpha_1(x^2+1)^{1/6}+\ldots+\alpha_5(x^2+1)^{5/6} \tag{5}$$

where α_i is in $Q(x)[\omega_6, 2^{1/4}, 3^{1/2}]$. In particular (4) may be written in the form (5) and is thus

$$\left(\frac{1}{x^2+1}\right)(2^{1/4})(x^2+1)^{3/6}+\left(\frac{1}{x^2+1}\right)\omega_6(3^{1/2})(x^2+1)^{5/6}. \tag{6}$$

However from a human engineering point of view (4) would usually be more desirable than (6). Furthermore, to find the extension field of Q(x) to which (4) belongs requires that one verify that the polynomials y_1^4-2 and y_2^2-3 are irreducible over $Q(x)[\omega_6]$ and $Q(x)[\omega_6, 2^{1/4}]$ respectively. In general such polynomials have to be factored over algebraic extension fields. Currently no efficient algorithms are known for factoring polynomials over algebraic extension fields although recently Wang [Wan 75] and Weinberger [Wei 76] have reported some progress on finding such algorithms.

In section 2 the MACSYMA algorithm for simplifying radical expressions will be presented. In particular the compromises that were made to try to balance the clean theoretical solution with the efficiency and human engineering problems will be discussed.

In simplifying radical expressions there are other problems which must be confronted. For example what does the symbol $\sqrt{x}$ mean? The square root function is multi-valued. Which branch, if any, does the symbol $\sqrt{x}$ represent? Also, what do symbols like $\sqrt{x^2}$ mean? Is this to be taken as -x, x or $|x|$? To answer these questions precisely requires a careful discussion as is given in section 3. Roughly speaking the answers are that $\sqrt{x}$ can stand for either of the single-valued branches of the square root function without affecting the way the arithmetic and simplification is carried out. The ambiguity in the symbol $\sqrt{x^2}$ is inherent and an arbitrary choice must be made to resolve it. The choice of $|x|$ for this symbol would lead to certain difficulties that we do not consider herein. In section 3 one precise way is given that changes $\sqrt{x^2}$ into x. With suitable modifications the same ideas could be used to change it into -x. Basically what is done in section 3 is to give a set of rules that transform ambiguous expressions into non-ambiguous ones. The rules given there are not the only ones that can be given but the important point is that the ambiguities must be resolved and the rules for resolving them should be clearly stated. Section 3 also contains a description of the algorithm for finding a common algebraic extension field to which a given set of radical expressions belongs.

In section 5 a brief discussion of theoretical computing times for some of the algorithms of section 2 and 3 is presented. Section 5 follows section 4 in which some theorems that show a priori the irreducibility of polynomials like y_1^4-2 and y_2^2-3 over certain algebraic extension fields. This knowledge simplifies and speeds-up the algorithms for finding the extension fields.

In section 6 an alternative approach to finding field extensions, based on the so-called theorem on the primitive element [vdW 49], is discussed. This section also contains a review of other related research.

2. The MACSYMA Algorithm RADCAN

In this section we present an informal description of the algorithm that is used in MACSYMA for the simplification of expressions containing radicals. The algorithm which is called RADCAN, an acronym for RADical CANonical simplifier, was implemented by Fateman [Mat 75] and was initially available in 1970. In our discussion we will concentrate on RADCAN's handling of radicals although the program has the capability to handle a larger class of functions. More information about RADCAN can be found in [Fat 72].

Programs with purposes similar to those of RADCAN have been written by Fitch [Fit 71 and Fit 73] for CAMAL, by Shtokhamer [Sht 75a and Sht 75b] for REDUCE, and by Jenks [GJY 75] for SCRATCHPAD.

RADCAN attempts to convert an arbitrary expression containing radicals, exponentials and logarithms into a simpler form. The result produced by RADCAN can be in various forms depending on which options are chosen. There are three options: (i) an option to produce the result in form 1 or form 2, (ii) an option to rationalize denominators, and (iii) an option to combine products of expressions raised to the same fractional power.

With the form 1 option, all polynomials appearing under radicals are factored into irreducibles, i.e., prime integers or polynomials irreducible over the integers. With the form 2 option, the polynomials appearing under radicals are factored into square-free, pair-wise relative prime factors.

For example with the form 1 option RADCAN transforms $(x^2-1)^{1/2}$ into $(x-1)^{1/2}(x+1)^{1/2}$ but with the form 2 option $(x^2-1)^{1/2}$ is not changed. The expression $(x^4+9x^3+29x^2+39x+18)^{1/2}$ is transformed into $(x+3)(x+1)^{1/2}(x+2)^{1/2}$ with the form 1 option and is transformed into $(x+3)(x^2+2x+2)^{1/2}$ with the form 2 option. $(x^4+9x^3+29x^2+39x+18)^{1/2} + (x+2)^{1/3}$ will be transformed into $(x+3)(x+1)^{1/2}(x+2)^{3/6} + (x+2)^{2/6}$ under either the form 1 or form 2 option. The dinstinction between form 1 and form 2 is discussed further in section 3.

With the rationalization of denominator option the expression $(x-y)/(\sqrt{x}-\sqrt{y})$ will be transformed into $\sqrt{x}+\sqrt{y}$. Otherwise it is not transformed. This option will also produce the transformation (3) above.

Option (iii) is used in the final step of RADCAN to determine whether or not expressions like $\sqrt{2}\ \sqrt{3}$ should be rewritten as $\sqrt{6}$.

Except for expressions involving roots of unity, RADCAN with the form 1 and rationalization of denominators option is a canonical form [Cav 70] for the unnested radical expressions.

With the form 2 option any unnested radical expression equivalent to zero which does not involve roots of unity will be transformed to zero. The form 2 option requires less computation than the form 1 option since finding square-free, pairwise relatively prime factors for non-constant polynomials is much easier than finding irreducible factors.

Experience with MACSYMA has indicated that it is not generally desirable to automatically invoke the rationalization of denominators option because simple expressions like the left-hand side of (3) are frequently transformed into complicated expressions like the right-hand side of (3).

As will be explained later to reduce zero-equivalent expressions involving roots of unity to zero, requires in general the factorization of polynomials over algebraic number fields, a task for which no efficient algorithms are known. So one of the compromises made in RADCAN was not to handle algebraic relationships involving roots of unity in a completely general way to avoid such factorization problems. Thus RADCAN will not reduce $(-1)^{1/4} - (-1)^{3/4} - (2)^{1/2}$ to zero. Although this is an expression that is unlikely to occur in practice, roots of unity do get introduced in natural ways since, for example, RADCAN transforms $(-x+1)^{1/4}$ into $(-1)^{1/4}\,(x-1)^{1/4}$.

The RADCAN algorithm consists of three basic phases which, depending upon the expression being simplified, may have to be repeated. The first phase is a global pass through the expression collecting the set R of all subexpressions which are radicals, exponentials, or logarithms. From R is generated a basis B in terms of which the elements of R can be represented. If R consists of only radicals, B is generated by factoring the polynomials that appear under the radicals. The particular set B that is generated depends on which option, form 1 or form 2, is taken.

After B is generated, appropriate radicals of the elements of B are considered as new variables and the original expression is represented in terms of the new and original variables.

In the second phase standard rational function simplification procedures such as expansion, collection of terms over a common denominator, and removal of greatest common divisors are applied to the arguments of any imbedded non-rational functions as well as to the expression as a whole. In this phase the radicals are considered simply as new independent variables. All knowledge of algebraic dependence is submerged.

The third phase reimposes the interpretation of the variables as radicals. The transformation $(\alpha^{1/a})^b \rightarrow \alpha^q(\alpha^{1/a})^r$ is applied for each radical $\alpha^{1/a}$ with $b \geq a$ where $b = qa + r$, $0 \leq r < a$. Thus $(2^{1/6})^7$ would be changed to $2(2^{1/6})$. If this transformation is applied to any radical in the expression, the expression must be rationally simplified again. Furthermore if the expression contains nested radicals then the above transformation can change nested radicals to unnested ones. A contrived example that illustrates this possibility is $(x^2 + 3x + 3 + (x+1)^{1/2}(x+1)^{1/2})^{1/2}$. After phase 1 and phase 2 the expression would be in the form $(x^2 + 3x + y^2 + 3)^{1/2}$ where $y = (x+1)^{1/2}$. The phase 3 transformation changes y^2 to $x+1$ and then the reapplication of phases 1 and 2 simplifies the original expression to $x+2$ after which no further changes are made.

If appropriate, phase 3 also carries out options (ii) and (iii), in this order.

The three phases of simplifying an expression S may be further subdivided as follows.

I. First Phase

1. Make a list R of all distinct radicals in the expression S. Collect the distinct radicands, i.e., polynomials appearing under radicals, on a list P.

2. For each radicand P_i on P

(i) If P_i is an integer, factor it completely, placing the distinct prime factors on a list B, the basis list. Only factors of P_i not already on B are placed on B. So B always contains at most one instance of an element.

(ii) If P_i is a polynomial of positive degree, factor it into factors irreducible over the integers for the form 1 option or into square-free factors for the form 2 option. For the form 1 option place all irreducible factors not occurring on B thereon. In the case of the form 2 option let P_i^* denote a square-free factor of P_i. If P_i^* is relatively prime to each element on B, place P_i^* on B. Otherwise there exist some P_j on B with $\gcd(P_i^*, P_j) = C \neq 1$. Remove P_j from B and replace it with the two factors C and (P_j/C). If $C = P_i^*$ then repeat the process on the next square-free factor of P_i. If $C \neq P_i^*$ then replace P_i^* by P_i^*/C and repeat the immediately preceding procedure for P_i^*.

At the completion of phase 2 B will be a list of polynomials of non-negative degree which are square-free and pair-wise relatively prime. Under the form 1 option each element on B will also be irreducible.

3. As step 2 processing takes place, each radical on the list R is constantly updated to reflect the changing representation of each of the original radicals in terms of the latest basis B.

4. Associated with each element on B is a radical degree. If, for example, $x+1$ is on B and the only occurrences of $x+1$ in the radicals on R are $(x+1)^{1/3}$ and $(x+1)^{2/5}$ then the radical degree of $x+1$ is $15 = \text{lcm}(3,5)$. As B changes in step 2 the radical degrees must be revised also. In the above example $(x+1)^{1/3}$ and $(x+1)^{2/5}$ are represented in terms of a new variable $v_j = (x+1)^{1/15}$ as v_j^5 and v_j^6 respectively. In the case the base is -1 and the radical degree is m, the distinguished indeterminate $\omega_m = e^{i\pi/m}$ is introduced.

II. Second Phase

At this point the expression S is considered as a rational function in its original variables and a set of new variables obtained from the elements on B and their radical degrees. S so considered is rationally simplified.

III. Third Phase

The algebraic properties of the new variables are reintroduced. If any reductions are achieved

each of the three phases must be repeated.

A well-known general procedure [Pol 50, p.38] for rationalizing denominators is based on a straightforward application of the extended Euclidean algorithm [Knu 69, p.377, exercise 3]. We will explain the algorithm by an example. To rationalize the denominator we merely need to find its inverse. So to rationalize the denominator in (3) we find the inverse of $x+\sqrt{2}+3^{2/3}$. We consider $x+\sqrt{2}+3^{2/3}$ as an element of the field $Q(x)[\sqrt{2}, 3^{1/3}]$ which is isomorphic to the polynomial ring $Q(x)[y_1,y_2]$ modulo the ideal generated by $y_1^2-2=0$ and $y_2^3-3=0$. Now y_1^2-2 is irreducible over $Q(x)$ and y_2^3-3 is irreducible over $Q(x)[\sqrt{2}]$. Thus we consider $x+\sqrt{2}+3^{2/3}$ as the polynomial $y_2^2+(x+\sqrt{2})$ in the variable y_2 with coefficients in $Q(x)[\sqrt{2}]$. We apply the extended Euclidean algorithm to $y_2^2+(x+\sqrt{2})$ and y_2^3-3 to find polynomials $S(y_2)$ and $T(y_2)$ with coefficients in $Q(x)[\sqrt{2}]$ such that

$$S(y_2)[y_2^2+x+\sqrt{2}]+T(y_2)[y_2^3-3]=a\neq 0 \quad (7)$$

where a is also in $Q(x)[\sqrt{2}]$. We are guaranteed that a is in $Q(x)[\sqrt{2}]$ since y_2^3-3 is irreducible and hence cannot have a factor of positive degree in common with $y_2^2+x+\sqrt{2}$.

If we consider (7) modulo y_2^3-3 as we should since y_2 is just another symbol for $3^{1/3}$ and hence $y_2^3-3=0$, we have that $S(y_2)[y_2^2+x+\sqrt{2}]=a\neq 0$. Thus $\frac{1}{y_2^2+x+\sqrt{2}}=\frac{1}{a}S(y_2)$. Furthermore the S and T produced by the extended Euclidean algorithm will have degrees in y_2 at most 2 and 1 respectively. In this example $S(y_2)=-(x+\sqrt{2})^{-1}y_2^2+3(x^2+2\sqrt{2}x+2)^{-1}y_2+1$ and $a=x+\sqrt{2}+9/(x^2+2\sqrt{2}x+2)$. Thus

$$\frac{1}{x+\sqrt{2}+3^{2/3}}=-\left(\frac{x+\sqrt{2}}{D}\right)3^{2/3}+\left(\frac{3}{D}\right)3^{1/3}+\frac{x^2+2\sqrt{2}x+2}{D} \quad (8)$$

where $D=(x+\sqrt{2})^3+9=(3x^2+2)\sqrt{2}+x^3+6x+9$.

To obtain (3) we must rationalize D with respect to $\sqrt{2}$. To do this we again apply the extended Euclidean algorithm, this time, to y_1^2-2 and $D=(3x^2+2)y_1+x^3+6x+9$ considered as polynomials in $y_1=\sqrt{2}$ over $Q(x)$. We find that $1/D=[-(3x^2+2)\sqrt{2}+x^3+6x+9]/E$ where $E=x^6-6x^4+18x^3+12x^2+54x+73$.

In general we must apply the extended Euclidean algorithm at most one time for each algebraic extension.

This algorithm for rationalizing denominators has been programmed for multiple algebraic number extensions in the MACSYMA algebraic arithmetic system by Richard Zippel and Barry Trager.

Examples of the use of RADCAN may be found in [MaF 71].

3. Theoretical Issues

In this section we formally define the concept of a radical expression in both a syntactic and semantic sense, give formal procedures for simplifying and performing arithmetic on radical expressions, and discuss the relationship between the formal presentation and the previously discussed algorithm RADCAN.

Radical expressions are rational roots of polynomials, rational functions, and other radical expressions. They are built up from:

(i) the field Q of rational numbers,
(ii) the variables $x_1,x_2,\ldots,x_n$,
and (iii) the operations of addition, subtraction, multiplication, division, composition, and rational exponentiation.

We will restrict our attention to unnested radical expressions, i.e., expressions like $((x^2+2x)^{1/2}+5)^{2/3}$ will not be considered further. Shtokhamer [Sht 75b] has recently discussed one way in which these ideas can be modified and extended to cover nested radical expressions.

Given a radical expression such as

$$((x^2-1)/(x+2))^{1/2}/(x+3x+2)^{1/3} \quad (9)$$

we wish to interpret it as a single-valued branch of a meromorphic function in an algebraic extension of the field $Q(x_1,\ldots,x_n)$ of multivariate rational functions over Q. Since in general there are a number of single-valued branches that might reasonably be associated with an expression like (9) we would like to interpret (9) in as general, but yet as natural, a way as possible.

There are two different aspects to the interpretation problem that are intimately related to the way that we simplify and perform computations with radical expressions. It is important that these two different aspects be clearly distinguished.

The first aspect of the problem is to take a set of radical expressions and to find an algebraic extension field to which they belong and to find the representation of the expressions in this extension field. The finding of the extension field and the representation of the expressions within the field is the process that is frequently referred to as "simplification of radical expressions," and this is essentially the process that is carried out by RADCAN.

The desired extension field is not uniquely determined by the symbols for the radical expressions. For example $(x^3)^{1/3}$ satisfies the polynomial $y^3-x^3=0$ which has the irreducible factors y-x and y^2+xy+x^2. To do the arithmetic in $Q(x)((x^3)^{1/3})$, i.e., the field of rational functions in x with $(x^3)^{1/3}$ adjoined, we must know the irreducible polynomial of which $(x^3)^{1/3}$ is a root and then perform arithmetic in the polynomial ring Q(x)[y] modulo the ideal generated by the irreducible polynomial which $(x^3)^{1/3}$ satisfies. We have two choices for the extension field: namely $Q(x)[y]/(y-x)$ which is isomorphic to Q(x) and $Q(x)[y]/(y^2+xy+x^2)$ which is not

isomorphic to Q(x).

Either of the choices is a legitimate choice. The first choice effectively gives us the simplification $(x^3)^{1/3} \rightarrow x$ whereas the second one gives $(x^3)^{2/3} \rightarrow -x(x^3)^{1/3} - x^2$ and the symbol $(x^3)^{1/3}$ would not be rewritten or simplified at all. Of course one would normally take the first interpretation in this case, but there are other cases that are not so obvious. For example should $(x^2)^{1/2}$ be considered as x or -x, i.e., should we choose y-x or y+x as the irreducible factor of $y^2 - x^2$?

So we conclude that there are choices to be made, no one of which is more right than the other, at least from a mathematical point of view. The important point is that the inherent ambiguity of these symbols must be realized and the rules chosen for the resolution of the ambiguities must be stated clearly and careful. Of course the rules may be chosen by the system designer or they may be left to the user. Below we describe the set of rules that are used by RADCAN to resolve the ambiguities. These rules attempt to give as natural an interpretation as possible to the symbols.

The second aspect of the interpretation problem is illustrated by the following simple example. Suppose we have resolved the previously discussed ambiguities and have found that our radical expressions belong to the field $Q(x)[\sqrt{x}]$ which is isomorphic to $Q(x)[y]/(y^2-x)$. What does $\sqrt{x}$ mean? From a general point of view, it is a multivalued function so when we evaluate it at $x = 4$, either +2 or -2 is a legitimate value. If we want to interpret it as a single-valued branch which branch do we choose and what difference does it make? The answer is that it does not make any difference which branch we choose when we are doing the field operations of addition, subtraction, multiplication, and division. That is, if we take two functions from $Q(x)[\sqrt{x}]$ such as $(\frac{1}{x+1})\sqrt{x} + 1$ and $(2x^2 - 2)\sqrt{x} + x$ and perform a field operation on them such as multiplication the answer will be $(\frac{2x^3+2x^2-x-2}{x+1})\sqrt{x} + 2x^2 - x$ no matter which single-valued branch we choose for the interpretation of $\sqrt{x}$.

Once we have chosen the algebraic field extension to which the expressions belong, there is no longer any ambiguity in carrying out the field operations. The answers depend on the symbols alone and not on the interpretations. When other operations such as evaluation and substitution are performed the expressions may become ambiguous again. We will have more to say about these two operations later in this section.

The foregoing should be considered as an introduction to the rigorous discussion that follows. We first give a set of rules for resolving the inherent ambiguities discussed previously along with a procedure for finding the field extensions to which a finite set of radical expressions belongs. So we assume we are given a finite set of radical expressions. The expressions are scanned and a set of radicals R is formed where each member of R is of the form $(P_1/P_2)^r$ with P_1 and P_2 relatively prime members of $Z[x_1,\ldots,x_n]$. Z denotes the ring of integers; r is a positive member of Q and $r \neq 1$. If $P_2 = 1$ then we write $(P_1)^r$. P_1 and P_2 are assumed to be relatively prime in the strong sense that their only common divisors in Z are ± 1. Henceforth we will always use relatively prime in this strong sense. Furthermore it is assumed that P_2 is positive, that is, that its leading coefficient is a positive member of Z. Let $\mathcal{P}$ consist of all polynomials P_1, P_2 where $(P_1/P_2)^r$ appears in R.

Following Collins [Col 74] we define a basis for the set $\mathcal{P}$ of polynomials of degree ≥ 0 to be a set $\mathcal{B}$ of positive, square-free elements of $Z[x_1,\ldots,x_n]$ satisfying the following three conditions:

(i) If B_1 and B_2 are distinct members of $\mathcal{B}$, they are relatively prime.
(ii) If B is in $\mathcal{B}$ then $B \mid P$ for some P in $\mathcal{P}$.
(iii) If P is in $\mathcal{P}$, there exist B_i in $\mathcal{B}$ and positive integers e_i such that $P = \pm \Pi B_i^{e_i}$.

Note that our definition of basis differs slightly from Collins'. His definition is only for a set $\mathcal{P}$ containing primitive polynomials of positive degree in x_n. In our definition the elements of $\mathcal{P}$ are neither required to be primitive nor to be of positive degree in any variable.

Let $\mathcal{B}$ be a basis for $\mathcal{P}$. In finding an algebraic extension of $Q(x_1,\ldots,x_n)$ to which each element $(P_1/P_2)^r$ of R belongs we impose the following rules to resolve the inherent ambiguities:

(i) $(P_1/P_2)^r = P_1^r/P_2^r$.
(ii) If P_1 (or P_2) $= +\Pi B_i^{e_i}$ where each B_i is in $\mathcal{B}$ and each e_i is a positive integer, then $P_1^r = \Pi B_i^{e_i r}$. If $P_1 = -\Pi B_i^{e_i}$, then $P_1^r = (-1)^r \Pi B_i^{e_i r}$.
(iii) Suppose $r = s/t$ where s,t are positive, relatively prime members of Z. If $s = qt + v$, $0 \leq v < t$, then $B^r = B^q B^{v/t}$ for B in $\mathcal{B}$. Also $(-1)^r = (-1)^q (-1)^{v/t}$.

These assumptions imply that $\sqrt{x^2} = \sqrt{(-x)^2} = (x^3)^{1/3} = x$ and similarly resolve other inherently ambiguous expressions.

Given R and assuming (i) - (iii) above, we find an extension field to which each member $(P_1/P_2)^r \in R$ belongs by the following procedure:

(a) Using (i) above, each element of R, $(P_1/P_2)^r$, can be written as a quotient of radical polynomials of the form P_1^r/P_2^r. P_1 and P_2 are called radicands. Form the set $\mathcal{P}$ of all distinct radicands.

(b) Compute a basis $\mathcal{B}$ for the set $\mathcal{P}$.

(c) Using the properties of a basis and (ii) and (iii) above, each P_1^r and P_2^r can be uniquely expressed as a product of integer and fractional powers of members of $\mathcal{B} \cup \{-1\}$.

(d) For each B in $\mathcal{B}$ let $s_1/t_1,\ldots,s_k/t_k$ be the reduced rational powers to which it appears

after the steps (a) - (c) are carried out for each member of R. Let $t = \&cm(t_1,\ldots,t_k)$. If $k = 0$, $t = 1$. Then every element of R belongs to the algebraic extension field F obtained by adjoining all the $B^{1/t}$ to $Q(x_1,\ldots,x_n)$.

For example if $R = \{(2/3)^{1/3},(x+1)^{1/2}, (2-2x^2)^{1/2}\}$ then $P = \{2,3,x+1,2x^2-2\}$, $\mathcal{B} = \{2,3,x+1,x-1\}$ and $F = \{Q(x)((-1)^{1/2},2^{1/6},3^{1/3}, (x+1)^{1/2},(x-1)^{1/2})\}$.

To do the arithmetic in F in a canonical fashion we must know the minimal polynomial $M(y)$ satisfied by each $B^{1/t}$. Of course $M(y)$ will be a factor of y^t-B. In the example above we must know the irreducible factors of y^2+1 over $F_0 = Q(x)$, the irreducible factors of y^6-2 over $F_1 = F_0(i)$, the irreducible factors of y^3-3 over $F_2 = F_1(2^{1/6})$, the irreducible factors of $y^2 - (x+1)$ over $F_3 = F_2(3^{1/3})$, and the irreducible factors of $y^2 - (x-1)$ over $F_4 = F_3((x+1)^{1/2})$.

In general to find the required irreducible factors of the j^{th} such polynomial it is necessary to factor it over F_{j-1}. As was mentioned earlier, Wang and Weinberger have recently discussed algorithms for factoring over algebraic number fields and van der Waerden [vdW 49] presents an algorithm for factoring polynomials over an algebraic extension of the field $Q(x_1,\ldots,x_n)$. However, except for special cases, these algorithms are quite slow.

Fortunately in most cases the pure polynomials that arise can be proved irreducible a priori and in such cases no factoring has to be done at all. One case in which the pure polynomials can be reducible is when the degree t is even, B is an integer, and a root of unity has been adjoined to the field in which the coefficients of the factor must lie. For example $y^2 - 2 = [y - (\omega_8 - \omega_8^3)][y + (\omega_8 - \omega_8^3)]$ since $\omega_8 - \omega_8^3 = \sqrt{2}$ where ω_8 is the primitive eighth root of unity $e^{i\pi/4}$. In RADCAN, it was decided not to attempt such factorizations in order to make the algorithm faster. Hence, as was discussed in the previous section RADCAN does not handle expressions involving roots of unity and even roots of integers in a completely general way. The theorems on the irreducibility of the pure equations are presented in section 4.

Let us return to step (b) in the above procedure. In general, given P, there are many sets $\mathcal{B}$ that form a basis for P. For example if $P = \{24, x^4+6x^3+13x^2+12x+4, x^2+2x+1\}$ then $\{24,x^2+4x+4,x^2+2x+1\}$, $\{6,x+2,x+1\}$ and $\{2,3,x+2,x+1\}$ are all bases for P. The extension field found depends not only on the rules (i) - (iii) but the basis $\mathcal{B}$ also. In order for the irreducibility theorems to apply the elements of $\mathcal{B}$ must be square-free and pair-wise relatively prime. A basis in which each element is square-free is called a square-free basis. But even a square-free basis is not necessarily unique.

There are two natural ways to compute a square-free basis. One way is to let $\mathcal{B}$ consist of all the distinct irreducible factors of elements in P. A second way is to compute a set $\bar{\mathcal{B}}$ of all square-free factors of elements in P. For polynomials of positive degree square-free factorization is much faster than factoring the polynomials into irreducible factors. See Yun [these Proceedings, pp. 248-259] for square-free factorization algorithms.

$\bar{\mathcal{B}}$ may be refined into a square-free basis if for each pair B_1,B_2 in $\bar{\mathcal{B}}$ with $\gcd(B_1,B_2) = C \neq 1$ we replace B_1 and B_2 by the non-units among (B_1/C), (B_2/C), and C. This process must be repeated until the elements of $\bar{\mathcal{B}}$ are pair-wise relatively prime at which time we will have the desired basis $\mathcal{B}$. All of these operations can be carried out fairly efficiently with the exception of computing square-free factors of integers. The only method known for computing square-free factors of integers is to completely factor them into primes. The best of the known algorithms for factoring an integer requires time that is exponential in the length of the integer.

With the form 1 option RADCAN computes a basis in which each element is irreducible. With the form 2 option RADCAN computes a basis in which the integers are prime and the polynomials of positive degree are square-free and pair-wise relatively prime.

This ends our discussion of the first aspect of the interpretation and simplification of radical expressions. We still need to give an intrepretation for the symbols that describe the algebraic extension fields found by the above procedure.

This has been done precisely and elegantly by R. H. Risch [Ris 69a] for univariate functions. For simplicity we also shall specify interpretations only for univariate functions. Interpretations for multivariate expressions can be specified in a similar way. See, for example [Eps 75, pp.161-163] for an interpretation of multivariate exponential and logarithmic expressions.

Suppose S is a list of symbols and let E(S) be the smallest set of expressions containing the elements of S with the property that whenever a,b are in S, so are a + b, a - b, a * b and a/b. For our purposes S is always of the form $S = (1, x, \gamma_1,\ldots,\gamma_m)$ where $m \geq 0$. For each γ_i there is a P_i in E((1,x)) and an r_i in E((1)) such that γ_i is the symbol $P_i^{r_i}$. Roughly speaking, E((1)) denotes rational numbers and $P_i^{r_i}$ denotes a polynomial raised to a rational power. E(S) is a special case of Risch's elementary field descriptions and shall be called an algebraic field description. An interpretation of E(S) is a pair (Mer(A),I) where Mer(A) is a field of single-valued algebraic functions which are meromorphic on an open, connected subset A of the complex plane. I is a mapping from a subset of E(S), namely that subset of expressions with a well-defined interpretation, onto Mer(A) such that

(i) I(1) is the constant function 1;
(ii) I(x) is the identity function on A;
(iii) For each γ_i symbol P^r, let s/t = I(r) where s and t are relatively prime integers with $t > 0$. Then $I(\gamma_i)^t - I(P)^s = 0$. If $I(\gamma_i)^t - I(P)^s$ is the monic irreducible equation satisfied

by $I(\gamma_j)$ over $Q(I(x), I(\gamma_1),\ldots,I(\gamma_{j-1}))$ then E(S) is regular; otherwise E(S) is non-regular.

(iv) If a and b are in the domain of I, so are a + b, a - b, and a * b. If $I(b) \neq 0$, a/b is also in the domain of I. Furthermore, $I(a\circ b) = I(a)\circ I(b)$ when $a\circ b$ is in the domain of I and $\circ$ is one of +, -, *, or /.

A regular algebraic field description E(S) has the desirable property that all interpretations of it are differentially isomorphic (see [Ris 69a], p.176, proposition 2.3 for a proof of this fact). This is the previously alluded to mathematical result that means for computational purposes all results of performing field operations and differentiation on the elements of E(S) are independent of the interpretation, i.e., independent of the single-valued branches of the multi-valued functions chosen.

Normally it is not necessary to distinguish the interpretation of a symbol from the symbol itself and we shall not do so henceforth.

Let us now consider the problem of substitution in a radical expression, i.e., we are given a radical expression f(x) and a polynomial P(x) and we wish to substitute P(x) for x in f(x) to obtain f(P(x)). When P(x) is a constant we have the evaluation problem.

We restrict ourselves to substituting polynomials for x. If radical expressions are substituted for x we can obtain nested radical expressions. Our restriction insures that f(P(x)) will be an unnested radical expression.

It is easy to see that one can obtain completely general unnested radical expressions through the process of substituting in a multivariate radical expression. Thus the substitution process is equivalent to the simplification process itself. Thus the interpretation of the symbol f(P(x)) can be given by our previous discussion and the "value" of f(P(x)) can be computed by applying our simplification process. In general when evaluating f(P(x)) one already has an algebraic extension F of Q(x) in which f(x) lies. It is only necessary to extend F and its corresponding basis to find an algebraic extension of F in which f(P(x)) lies. It is not necessary to repeat the entire process of finding an algebraic extension of Q(x) for f(P(x)).

With this view of substitution and our previous rules for resolving ambiguities and interpreting radical expressions, we have a generalization of Fateman's positive real interpretation [Fat 72] of radical expressions. The interpretation given herein effectively chooses the positive real branch for algebraic functions when the radical expression is ambiguous as it may be initially or as it may be after substitution. But once the ambiguities are solved and the extension field found, the field operations can be carried out in a manner that is independent of the interpretation. Thus there is no conflict between the regular field extensions of Risch and the positive real interpretations of Fateman that are used in MACSYMA.

4. Irreducibility Theorems for Pure Polynomials

In this section we present the irreducibility theorems for the pure polynomials discussed earlier. The first theorem tells us that $y^m - p$, p a prime integer is irreducible over any algebraic number extension of Q(x) obtained by adjoining roots of other prime integers. It is important that roots of unity not be contained in tne extension field for then the result is false as was shown by the example in which $y^2 - 2$ factors when $e^{1\pi/4}$ is in the extension field.

Theorem 1. Let m be a positive integer, $p_1,\ldots,p_k$ distinct positive prime integers. Let $p_i^{1/m}$ denote an m^{th} root of p_i. Then the field $Q(p_1^{1/m},\ldots,p_k^{1/m})$ is of degree m^k over Q.

For a proof of this theorem see [Fat 72, pp. 135-140] or [Ric 74].

Corollary 2. Let $m_1,\ldots,m_k$ be positive integers; $p_1,\ldots,p_k$ be distinct positive prime integers; and let p_i^{1/m_i} denote an m_i^{th} root of p_i. Then $y^{m_k} - p_k$ is irreducible over $Q(p_1^{m_1},\ldots,p_{k-1}^{m_{k-1}})$.

Proof. Let $m = \ell cm(m_1,\ldots,m_k)$. By theorem 1 $y^m - p_k$ is irreducible over $G = Q(p_1^m,\ldots,p_{k-1}^m)$ which contains $F = Q(p_1^{m_1},\ldots,p_{k-1}^{m_{k-1}})$. Hence $y^m - p_k$ cannot factor over F without factoring over G. ∎

All examples known to us in which $y^m - p$ factors involve roots of unity with m even. It would be nice to know if $y^{m_k} - p_k$ factors over $Q(\omega_\ell, p_1^{1/m_1},\ldots,p_{k-1}^{1/m_{k-1}})$ where $p_1,\ldots,p_k$ are distinct primes, m_k is odd, and, ℓ, $m_1,\ldots,m_{k-1}$ are arbitrary positive integers. The next theorem provides a partial answer to this question.

Theorem 3. Let ℓ be a positive integer, m an odd positive integer, and $p_1,\ldots,p_k$ be distinct positive prime integers. Then the field $Q(\omega_\ell, p_1^{1/m},\ldots,p_k^{1/m})$ is of degree m^k over $Q(\omega_\ell)$ where ω_ℓ is a primitive ℓ^{th} root of unity.

For a proof see [Cav 68, pp.50-54]. The three results above still hold under the weaker hypotheses that the p_i are square-free and pairwise relatively prime.

If the hypotheses of theorem 3 are changed so that ℓ is odd and m is any arbitrary positive integer the result is false since $\sqrt{5} = -2\omega_5^2 - 2\omega_5 - 1$.

The final theorem tells us that in our algorithm $y^m - B(x_1,\ldots,x_n)$ is always irreducible where B is a non-constant polynomial in $Q(x_1,\ldots,x_n)$.

Theorem 4. Let m be a positive integer, $B_1,\ldots,B_k$ be non-constant, square-free, pair-wise relatively prime polynomials in $Q[x_1,\ldots,x_n]$. Then the field

$C(x_1,\ldots,x_n)(B_1^{1/m},\ldots,B_k^{1/m})$ is of degree m^k over $C(x_1,\ldots,x_n)$ where C denotes the field of complex numbers and $B_i^{1/m}$ denotes any one of the roots of $y^m - B_i = 0$.

The proof in [Cav 68, pp.54-59] can be modified in a straightforward way to give the above result. In [Fat 72, pp.135-140] a slightly weaker result is proved with C replaced by Q and with the added hypothesis that the B_i be positive or m be odd.

Theorem 4 has a natural corollary that is analogous to the corollary of theorem 1 and is proved in the same manner. Hence we will not actually state it.

5. Computing Times

In this section we present a brief discussion of the worst case computing time of some of the algorithms involved in the simplification process. The length of a non-zero integer n, denoted L(n), is $\lfloor \ell og_2|n| \rfloor + 1$. L(0) = 1. Let Z[n,d,a] denote the set of polynomials in $Z[x_1,\ldots,x_n]$ with degree in each variable $\leq$ d and the length of each integer coefficient $\leq$ a.

One of the major procedures in the simplification process is the computation of a basis $\mathcal{B}$ for P, the set of radicands. Suppose each element of P is in Z[n,d,a].

In [Eps 76] Epstein presents carefully analyzed algorithms for computing a square-free basis for polynomials with Gaussian integer coefficients. We assume straightforward changes to Epstein's algorithms and computing time analyses to the restricted case that we are considering, namely polynomials with rational integer coefficients.

We have also defined basis in a slightly different manner from Epstein - his definition ignores constants. Thus for our purposes we can compute a square-free basis by first finding the integer content and primitive parts of each of the non-constant polynomials in P. Let P_1 = the set obtained by the union of the constants in P and the integer contents of the non-constant members of P. Let P_2 be the set of primitive parts of non-constant members of P. Let $\mathcal{B}_1$ be a basis for P_1 and P_2 be a basis for $\mathcal{B}_2$. Then $\mathcal{B}_1 \cup \mathcal{B}_2$ will be our desired basis for P. Assume the elements of P_1 and P_2 are in Z[n,d,a] and that P_1 contains k_1 distinct integers while P_2 contains k_2 distinct polynomials. Then $\mathcal{B}_1$ can be computed by factoring each element into prime factors which can be done in time bounded by a function which is $O(k_1 \cdot 2^{a/2})$. The best known algorithms for factoring integers have somewhat better computing time bounds but they still require time that is an exponential function of a. Hence we will be content with the $O(2^{a/2})$ bound.

Epstein's algorithms will compute $\mathcal{B}_2$ in time bounded by a function which is $O(k_2{}^3a^2d^{3/2}(d+1)^{n+1})$. Furthermore Epstein's algorithm GPPSQF (Gaussian Polynomial Primitive Square-Free Factorization) can be trivially modified to provide the desired integer contents of the non-constant elements of P without additional work. His algorithm as currently constituted actually computes the integer contents but ignores it. Thus the entire basis computation can be done in time bounded by a function which is $O(k^{1/2a} + k^3a^2d^{3/2}(d+1)^{n+1})$ where $k = \max(k_1,k_2)$.

This computing time bound was obtained assuming that the modular greatest common divisor algorithm is used for gcd computations and that the assumptions made by Brown [Bro 71] in analyzing the modular gcd algorithm hold.

In RADCAN's phase II rational simplification is performed on rational functions in $n+\nu$ variables where ν is the number of elements in $\mathcal{B}$.

A set of integers, all bounded in magnitude by A, has at most $\ell og_2 A$ distinct prime factors. Thus $\mathcal{B}$ contains at most a + 1 integers. If each polynomial in P should factor into distinct linear factors in $\mathcal{B}$ then $\mathcal{B}$ would contain at most k_2nd non-constant polynomials.

Thus the rational functions in phase II of RADCAN have at most k_2nd + a + n +1 variables. Hence the time for the gcd calculation in this phase, assuming the modular algorithm is used, is $O((d+1)^{k_2nd+a+n+1})$ assuming each of the polynomials has degree at most d in each of the variables.

Hence one can see that the bounds for the worst case computing times for phases I and II of RADCAN grow very rapidly as a, n, d and k_2 increase.

Although these algorithms can require a lot of computing time in practice, experience with MACSYMA indicates that RADCAN is a reasonable algorithm to use for routine simplification of small expressions. In fact it was, at one time, a default preliminary step in simplifying single algebraic equations prior to their solution by the SOLVE command [Mar 71].

6. An Alternative Approach and a Review of Related Research

As is well-known each multiple algebraic extension field of Q(x) can be expressed as a single extension. This statement is known as the theorem on the primitive element [vdW 49]. From van der Waerden's discussion algorithms can be constructed to find an element β such that $Q(x)(B)$ is isomorphic to $Q(x)(\alpha_1,\ldots,\alpha_n)$ where $\alpha_1,\ldots,\alpha_n$ are algebraic over Q(x). Loos[Loo 73] also discusses constructive aspects of the theorem on the primitive element in relationship to performing arithmetic in the field of all algebraic numbers.

So since the theorem on the primitive element can be constructively implemented, why use multiple algebraic extensions when one would do. There seem to be at least two reasons for not simplifying radical expressions via the approach suggested by the theorem on the primitive element. First it seems likely, although there has been no definitive study to verify it, that multiple algebraic extensions of lower degree lead to faster algorithms than would one extension of high degree. The degree of the one extension would be the product of

the degrees of the multiple extensions.

Secondly multiple algebraic extensions seem to possess better human engineering attributes than extensions obtained through the theorem on the primitive element. For example the field $Q(\sqrt{3}, \sqrt{5})$ is contained in the field Q(a) where a satisfies the irreducible polynomial $M(a) = a^4 - 16a^2 + 4$. In $Q(a), \sqrt{3}$ is written as $1/4(a^3 - 14a)$ which from a human engineering point of view is generally less desirable than simply $\sqrt{3}$.

So for these reasons replacing multiple algebraic extensions by a single extension seems undesirable.

There have been a number of other papers written that are related to our discussion in one fashion or another. We will give a brief discussion of the related work. Much of it has already been mentioned in the preceding sections. First it should be noted that the present paper is based on the authors' Ph.D. dissertations [Cav 68] and [Fat 72].

Many papers have been written on various aspects of algebraic simplication. We will discuss only those that treat algebraic numbers and algebraic functions. For an overview of other aspects of simplification up to 1971, see the paper by Moses [Mos 71]. Further much of the material in classical modern algebra on algebraic extension fields is relevant to this work. van der Waerden [vdW 49] contains a treatment of this material with many algorithmic methods given.

The first significant paper to deal explicitly with simplification of algebraic functions was an unpublished Bell Laboratories report by S. L. Kleiman [Kle 66]. Kleiman considers some problems that are closely related to the problems considered here. He assumes that he is given a set of irreducible algebraic equations that define the algebraic dependencies among the variables involved. Thus he avoids discussing the problem of transforming a set of radical expressions into a set of pure polynomials and the factoring of such polynomials over algebraic extensions of Q. However, his paper is precisely written, contains interesting ideas, and should be more widely available and better known. For example, if the polynomials generate a prime ideal, Kleiman's results constructively refute Loos' [Loo 74] conjecture that given a set of polynomial equivalences, there does not exist a canonical form for a polynomial under these relations.

Fitch [Fit 71] discusses the general problem of algebraic simplification. From his work in general relativity in which unnested radical expressions occurred extensively he was lead to consider in some detail the problem of simplifying radical expressions. His solution has much in common with the methods described in this paper although he neither discusses interpretations of radical expressions nor deals with the problems associated with roots of unity.

The more accessible [Fit 73] covers much of the same ground as [Fit 71]. In addition it contains a simple proof, which he attributed to M. N. Huxley, of the fact that $(1 + x)^{1+x}$ is transcendental over Q(x). This result also follows from the more general structure theorem of Risch [Ris 69b].

Rubald [Rub 73] developed algorithms for polynomial arithmetic over real algebraic number fields Q(a) where the extension is simple. His algorithms do not require an irreducible defining polynomial for a. He also presents an algorithm for determining if $\alpha < \beta$ where α and β are real algebraic numbers. Such a determination is dependent on the particular root of the defining equation joined to Q and could not be realized by the methods discussed here.

Recently Shtokhamer has written on matters related to the work of Kleiman [Sht 75a] and on the simplification of nested radicals [Sht 75b]. In [Sht 75a] he claims to have developed algorithms for finding unique representatives of equivalence classes of $R[x_1,\ldots,x_n]$ modulo an ideal where R is a Noetherian domain. In [Sht 75b] he generalizes the methods given in the authors' dissertations to apply to nested radical expressions. His algorithms are programmed in REDUCE.

M. Lauer [Lau 76] brings together the algorithms of Shtokhamer [Sht 75a] and an earlier algorithm of Buchberger [Buc 70] to solve the problem of finding canonical representatives for the equivalence classes of $S[x_1,\ldots,x_n]$ modulo an ideal when S is either a field or a principal ideal domain.

The recent paper by Wang [Wan 75] reports on the progress of a program to factor polynomials over algebraic number fields. While efficiencies may be realized in special cases, the general computational intractability has not been resolved.

Although the irreducibility theorems of section 4 may have been known to some members of the mathematical community for many years, the first published results appeared in 1940 [Bes 40] when Besicovitch proved Theorem 1. In 1972 [Fat 72] Fateman gave an independent proof of theorem 1. In 1968 Caviness [Cav 68] presented theorems 3 and 4, and in 1974 Richards [Ric 74] published theorem 1 and theorem 3 for even ℓ.

Acknowledgments

The authors wish to thank their colleagues at Berkeley, MIT, the University of Wisconsin, and Bell Telephone Laboratories for stimulating discussions. This work was supported in part by Project MAC, an MIT interdepartmental laboratory sponsored by the Advanced Research Projects Agency (ARPA), Department of Defense, under Office of Naval Research Contract N00014-70-A-0362-0001. One author (RJF) was supported, while a graduate student, by ARPA under Air Force contract F19628-68-0101 with Harvard University, by the National Science Foundation under their Graduate Traineeship program and by Bell Telephone Laboratories under a contract with Harvard University. The other author (BFC) was supported, while a graduate student, by the National Science Foundation, in the form of a graduate fellowship. Professors Alan Perlis of Yale University and

Henry Leonard of Northern Illinois University made valued contributions to this work. The comments of John Fitch, Peter Weinberger, and the referees about an earlier version of the paper were also helpful.

References

[Bes 40] A. S. Besicovitch, On the Linear Independence of Fractional Powers of Integers, J. London Math. Soc. 15 (1940), 3-6.

[Bro 71] W. S. Brown, On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors, J. ACM 18, 4 (Oct. 1971), 478-504.

[Buc 70] B. Buchberger, Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungssystems, Aequationes Mathematicae 4 (1970).

[Cav 68] B. F. Caviness, On Canonical Forms and Simplification, Ph.D. Dissertation, Carnegie-Mellon University (May, 1968), 80 pages. Available from Xerox University Microfilms, Ann Arbor, Michigan.

[Cav 70] _____, On Canonical Forms and Simplification, J. ACM 17 2 (April 1970), 385-396.

[Col 74] G. E. Collins, Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition - Preliminary Report, SIGSAM Bulletin 8, 3 (August 1974), 80-90.

[Eps 75] H. I. Epstein, Algorithms for Elementary Transcendental Function Arithmetic, Ph.D. Dissertation, University of Wisconsin, (May 1975), 408 pages. Available from Xerox University Microfilms, Ann Arbor, Michigan.

[Eps 76] _____, Using Basis Computation to Determine Pseudo-Multiplicative Independence, these Proceedings.

[Fat 72] R. J. Fateman, Essays in Algebraic Simplification, Ph.D. Dissertation, Harvard University. Revised version reprinted as MIT Project MAC Tech. Report MAC TR-95 (April 1972), 190 pages.

[Fit 71] John P. Fitch, An Algebraic Manipulator, Ph.D. Dissertation, University of Cambridge (Oct. 1971).

[Fit 73] _____, On Algebraic Simplification, Computer J. 16 (1973), 23-27.

[GJY 75] J. H. Griesmer, R. D. Jenks, and D. Y. Y. Yun, SCRATCHPAD Users Manual, Report RA 70, IBM Research Center, Yorktown Heights, N.Y. (June 1975), 66 pages.

[Kle 66] S. L. Kleiman, Computing with Rational Expressions in Several Algebraically Dependent Variables, Bell Laboratories Tech. Report, Murray Hill, New Jersey, (1966), 40 pages. Reprinted as Computing Science Tech. Report #42 (1976).

[Knu 69] D. E. Knuth, The Art of Computer Programming, vol. 2 "Semi-numerical Algorithms," Addison-Wesley (1969).

[Lau 76] Markus Lauer, Canonical Representatives for Residue Classes of a Polynomial Ideal, these Proceedings.

[Loo 73] R. Loos, A Constructive Approach to Algebraic Numbers, preprint.

[Loo 74] _____, Toward a Formal Implementation of Computer Algebra, SIGSAM Bulletin 9, 3 (August 1975), 21-23.

[MaF 71] W. A. Martin and R. J. Fateman, The MACSYMA System, Proceedings of Second Symposium on Symbolic and Algebraic Manipulation (March 1971).

[Mat 75] Mathlab Group, MACSYMA Reference Manual, The Laboratory for Computer Science, M.I.T., Cambridge, Massachusetts, (November 1975), 199 pages.

[Mos 71] Joel Moses, Algebraic Simplification: A Guide for the Perplexed, Comm. ACM 14, 8 (August 1971), 527-537.

[Pol 50] Harry Pollard, The Theory of Algebraic Numbers, The Mathematical Association of America (1950).

[Ric 74] Ian Richards, An Application of Galois Theory to Elementary Arithmetic, Adv. in Math. 13 (1974), 268-273.

[Ris 69a] R. H. Risch, The Problem of Integration in Finite Terms, Trans. AMS, 139 (May 1969), 167-189.

[Ris 69b] _____, Further Results on Elementary Functions, IBM Tech. Report RC 2402, Yorktown Heights, N.Y. (March 1969).

[Rub 73] C. M. Rubald, Algorithms for Polynomials Over a Real Algebraic Number Field, Ph.D. Dissertation, University of Wisconsin (1973), 224 pages.

[Sht 75a] Roman Shtokhamer, Simple Ideal Theory: Some Applications to Algebraic Simplification, University of Utah Tech. Report UCP-36 (July 1975), 22 pages.

[Sht 75b] _____, Simplification of Nested Radicals, University of Utah Tech. Report UCP-37 (July 1975), 16 pages.

[vdW 49] B. L. van der Waerden, Modern Algebra, tr. F. Blum, Frederick Ungar Publ. Co. (1949).

[Wan 75] Paul Wang, Factoring Multivariate Polynomials Over Algebraic Number Fields in MACSYMA, SIGSAM Bulletin 9, 3 (August 1975), 21-23.

[Wei 76] Peter Weinberger, Factoring Polynomials Over Algebraic Number Fields, ACM Trans. on Math. Software (to appear).