4. G. H. Hardy and E. M. Wright, The Theory of Numbers, 4th ed., Oxford, 1960.
5. A. E. Ingham, On the difference between consecutive primes, Quart. J. Math. Oxford, Ser. (2) 8 (1937) 255–266.
6. L. Kuipers, Prime-representing functions, Indag. Math., 12 (1950) 57–58.
7. W. H. Mills, A prime-representing function, Bull. Amer. Math. Soc., 53 (1947) 604.
8. I. Niven, Functions which represent prime numbers, Proc. Amer. Math. Soc., 2 (1951) 753–755.
9. O. Ore, On the selection of subsequences, Proc. Amer. Math. Soc., 3 (1952) 706–712.
10. W. Sierpinski, Sur une formule donnant tous les nombres premiers, C. R. Acad. Sci. Paris, 235 (1952) 1078–1079.
11. B. R. Srinivasan, Formulae for the nth prime, J. Indian Math. Soc., (N.S.) 25 (1961) 33–39; 26 (1962) 248.
12. ——— An arithmetical function and an associated formula for the nth prime, I, II. Norske Vid. Selsk. Forh. Trondheim, 35 (1962) 68–71, 72–75.
13. C. P. Willans, On formulae for the nth prime number, Math. Gaz., 48 (1964) 413–415.
14. E. M. Wright, A prime-representing function, this MONTHLY, 58 (1951) 616–618.
15. ——— A class of representing functions, J. London Math. Soc., 29 (1954) 63–71.

RATIONAL EXPONENTIAL EXPRESSIONS AND A CONJECTURE CONCERNING π AND e

W. S. BROWN, Bell Telephone Laboratories, Murray Hill, New Jersey

Abstract. One of the most controversial and least well defined of mathematical problems is the problem of simplification. The recent upsurge of interest in mechanized mathematics has lent new urgency to this problem, but so far very little has been accomplished. This paper attempts to shed light on the situation by introducing the class of rational exponential expressions, defining simplification within this class, and showing constructively how to achieve it. It is shown that the only simplified rational exponential expression equivalent to 0 is 0 itself, provided that an easily stated conjecture is true. However the conjecture, if true, will surely be difficult to prove, since it asserts as a special case that π and e are algebraically independent, and no one has yet been able to prove even the much weaker conjecture that $\pi+e$ is irrational.

1. Introduction. Basically simplification means the application of mathematical identities to transform a given expression into an equivalent expression satisfying some desired criteria.

If the class of admissible expressions is too broad, many dilemmas, of which the following is typical, arise. A basic identity for simplification of expressions involving the logarithm function is

$$\log z_1z_2 = \log z_1 + \log z_2 \tag{1}$$

which holds everywhere on the Riemann surface whose points have the form

$$z = re^{i\theta},\ r > 0,\ -\infty < \theta < \infty. \tag{2}$$

On this surface one must abandon the identity

$$e^{2i\pi} = 1 \tag{3}$$

which is fundamental for simplification of expressions involving the exponential function. This identity can be saved if we define the logarithm function over a cut plane (for example, by restricting θ in (2) to the interval $-\pi < \theta \leqq \pi$), but then (1) is lost.

Surprisingly, it is not even necessary to introduce complex numbers or multi-valued functions in order to get into insurmountable difficulty. Consider the class of expressions generated from the integers, the real constants π and log 2, and the real indeterminate x by application of the rational operations, the sine function, the exponential function, the absolute value function, and substitution. Richardson [1] has shown that there is no algorithm to test whether or not a given expression in this class is identically zero. Caviness [2] has shown that the same result applies to the smaller class of expressions generated as above, but with log 2 and the exponential function omitted, provided that one assumes the unsolvability of Hilbert's tenth problem [3]. The two proofs are essentially the same except that Caviness begins with this assumption, while Richardson begins with a theorem of Davis, Putnam, and Robinson [4].

This paper attempts to shed light on the simplification problem by introducing the class of rational exponential (REX) expressions, defining simplification within this class, and showing constructively how to achieve it.

The definition is such that distinct simplified expressions may be equivalent. However, it is shown that the only simplified REX expression equivalent to 0 is 0 itself, provided that an easily stated conjecture is true. Unfortunately, the conjecture, if true, will surely be difficult to prove, since it asserts as a special case that π and e are algebraically independent, and no one has yet been able to prove even the much weaker conjecture that $\pi+e$ is irrational [5].

Section 2 defines the class of REX expressions, and defines simplification for expressions in this class. The fundamental conjecture is discussed in Section 3, the zero-equivalence theorem for simplified expressions in Section 4, and the simplification algorithm in Section 5.

2. Definitions. The *rational exponential* (*REX*) *expressions* are those which are obtained by addition, subtraction, multiplication, division, and substitution starting with the (rational) integers, the constants π and i, some indeterminates $z_1, \cdots, z_N$ (denoted collectively by z), and the exponential function. The *rational exponential functions* are those which can be represented by REX expressions.

Note that all roots of unity are REX. It is convenient to introduce the abbreviations

$$\omega_m = \exp(i\pi/2m) \qquad m \geqq 1. \tag{4}$$

In particular $\omega_1 = \exp(i\pi/2) = i$.

A REX expression is *equivalent to* 0 if it is identically 0 when viewed as an analytic function of z. A REX expression is *equivalent to* U (that is, *undefined*) if it involves division by a subexpression equivalent to 0. For example, the expression $2(z_1-z_1)$ is equivalent to 0, while the expression $3+1/2(z_1-z_1)$ is equivalent to U. The symbol U is considered to be a REX expression, but the construction of more complicated expressions involving it is forbidden. Two REX expressions are *equivalent* if both are equivalent to U or if their difference is equivalent to 0.

Any REX expression can be transformed by a straightforward process [6] into an equivalent weakly simplified REX expression. A REX expression is said to be *weakly simplified* if it is 0 or U or if it has the form

$$\frac{f(\exp p_1, \cdots, \exp p_n, z, \pi, \omega_m)}{g(\exp p_1, \cdots, \exp p_n, z, \pi)}, \tag{5}$$

where

(a) f and g are relatively prime nonzero polynomials;
(If g is the polynomial ± 1, we shall permit, and indeed insist, that it be omitted, with the sign of f being reversed if necessary. Although we require that the polynomial f be nonzero, the numerator of (5) might nevertheless be equivalent to 0. For example, it might be the expression $\exp(z_1+z_2)-\exp(z_1)\exp(z_2)$. In this case f is the nonzero polynomial defined by $f(a, b, c)=a-bc$.)

(b) the degree of f in ω_m is less than the degree of the minimal polynomial of ω_m; and

(c) $p_1, \cdots, p_n (n \geqq 0)$ are distinct weakly simplified REX expressions other than 0 or U.

A weakly simplified REX expression is said to be *simplified* if it is 0 or U; *or* if it has the form (5), and

(d) $p_1, \cdots, p_n$ are simplified, and

(e) the set $\{p_1, \cdots, p_n, i\pi\}$ is linearly independent over the rationals.

The significance of this last condition will become clear in Section 4.

3. The fundamental conjecture. This section discusses the fundamental conjecture on which our zero-test algorithm depends. The simplification algorithm also depends on it, but only in that no use is made of the presently unknown identities whose existence would be implied by its falsity.

ROUGH STATEMENT. *Roughly speaking, the conjecture is that the only algebraic relations involving π and the z's and exponentials of rational exponential expressions are those which follow directly from the fact that roots of unity are algebraic numbers and from the identities*

$$\begin{aligned} \exp(0) &= 1 \\ \exp(i\pi) &= -1 \\ \exp(z_1 + z_2) &= \exp(z_1)\exp(z_2). \end{aligned} \tag{6}$$

PRECISE STATEMENT. *Let $p_1, \cdots, p_n$ be nonzero rational exponential expressions such that the set $\{p_1, \cdots, p_n, i\pi\}$ is linearly independent over the rationals. Then the set $\{\exp p_1, \cdots, \exp p_n, z, \pi\}$ is algebraically independent over the rationals.*

Proof of the Converse. Suppose the set $\{p_1, \cdots, p_n, i\pi\}$ were linearly dependent over the rationals. Then there would exist integers $a_0, \cdots, a_n$ such that

$$a_0 i\pi + \sum_{i=1}^{n} a_i p_i = 0. \tag{7}$$

Using (6),

$$\prod_{i=1}^{n} (\exp p_i)^{a_i} = (-1)^{a_0}, \tag{8}$$

so the set $\{\exp p_1, \cdots, \exp p_n\}$, and *a fortiori* the set $\{\exp p_1, \cdots, \exp p_n, z, \pi\}$, would be algebraically dependent over the rationals.

COROLLARY. *Setting $n=1$ and $p_1=1$ in the precise statement of the fundamental conjecture, we obtain the corollary that π and e are algebraically independent.*

4. Zero-equivalence theorem for simplified REX expressions. *Let p be a simplified REX expression other than 0 or U. Then p is not equivalent to 0 or U.*

Proof. Since p is simplified, we can write it in the form (5) where (5a)–(5e) hold. The proof is by induction on the *depth* of p, defined as follows. If $n=0$ in (5), then the depth of p is 0. Otherwise the depth of p is

$$\max(d_1, \cdots, d_n) + 1$$

where $d_1, \cdots, d_n$ are the depths of $p_1, \cdots, p_n$ respectively.

Now let d be the depth of p. If $d=0$, then the proof is straightforward. In the case $d>0$, we assume inductively that the theorem is true for expressions of depth less than d. It follows, using (5c) and (5d), that none of the $p_1, \cdots, p_n$ is equivalent to U. Therefore neither the numerator nor the denominator of (5) is equivalent to U.

Viewed as a polynomial in the elements of the set

$$\{\exp p_1, \cdots, \exp p_n, z, \pi\}, \tag{9}$$

which is algebraically independent by (5e) and the fundamental conjecture, the numerator of (5) has, by (5a), at least one nonzero coefficient. This coefficient is a polynomial in ω_m (over the integers), whose degree, by (5b), is less than the degree of the minimal polynomial of ω_m. It follows that this polynomial is not equivalent to 0, and therefore the numerator of (5) is not equivalent to 0. A similar argument shows that the denominator of (5) is not equivalent to 0, and it follows immediately that p is not equivalent to 0 or U.

5. Simplification algorithm. The purpose of this algorithm is to transform a weakly simplified REX expression, other than 0 or U, into a simplified REX expression. The given expression has the form (5), and conditions (5a) through (5c) are satisfied. We now define the *innermost exponentials* in a REX expression as those whose arguments do not involve the exponential function. The algorithm proceeds from the innermost exponentials outward.

Step 1 (*Initialize*). Set $k=0$, so that $\{q_1, \cdots, q_k\}$ and $\{r_1, \cdots, r_k\}$ denote the empty set. Now rewrite (5) in the form

$$\frac{f(\exp p_1, \cdots, \exp p_n, r_1, \cdots, r_k, z, \pi, \omega_m)}{g(\exp p_1, \cdots, \exp p_n, r_1, \cdots, r_k, z, \pi)}. \tag{10}$$

Step 2 (*Begin loop with test for completion*). At this point the expression (10), with $r_1, \cdots, r_k$ viewed as additional indeterminates, is weakly simplified. Furthermore, $r_1, \cdots, r_k$ are abbreviations for $\exp q_1, \cdots, \exp q_k$ respectively, and $q_1, \cdots, q_k$ are simplified expressions of the form

$$q_i = \frac{f_i(r_1, \cdots, r_{i-1}, z, \pi, \omega_{l_i})}{g_i(r_1, \cdots, r_{i-1}, z, \pi)} \qquad i = 1, \cdots, k. \tag{11}$$

Finally, the set $\{q_1, \cdots, q_k, i\pi\}$ is linearly independent over the rationals, and the set $\{r_1, \cdots, r_k, z, \pi\}$ is algebraically independent over the rationals. Note that the $p_1, \cdots, p_n$ may depend on the $r_1, \cdots, r_k$.

If n is zero in (10), then replace $r_1, \cdots, r_k$ by $\exp q_1, \cdots, \exp q_k$ respectively. Now (10) has the form (5) with $q_1, \cdots, q_k$ playing the role of $p_1, \cdots, p_n$, and (5a) through (5e) are satisfied. Therefore we are finished.

Otherwise (that is, if $n>0$), proceed to Step 3.

Step 3 (*Introduce q_{k+1} and r_{k+1}*). Let q_{k+1} be the argument of any innermost exponential in (10), and replace $\exp q_{k+1}$ by the abbreviation r_{k+1}. In general, q_{k+1} will be a subexpression of one of the $p_1, \cdots, p_n$. Clearly it has the form

$$q_{k+1} = \frac{f_{k+1}(r_1, \cdots, r_k, z, \pi, \omega_m)}{g_{k+1}(r_1, \cdots, r_k, z, \pi)}. \tag{12}$$

If we replace $r_1, \cdots, r_k$ by $\exp q_1, \cdots, \exp q_k$, then (12) has the form (5) with $q_1, \cdots, q_k$ playing the role of $p_1, \cdots, p_n$, and (5a) through (5e) are satisfied. Therefore q_{k+1} is simplified.

Step 4 (*Test for linear dependence*). Recall that the set $\{q_1, \cdots, q_k, i\pi\}$ is linearly independent over the rationals. If q_{k+1} can be expressed as a linear combination of $i\pi$ and $q_1, \cdots, q_k$, then we shall rewrite (10) accordingly (see Step 5a). Otherwise, we shall adjoin q_{k+1} to the set (see Step 5b).

Consider the linear dependence equation

(13) $$a_0 i\pi + \sum_{i=1}^{k+1} a_i q_i = 0$$

where $a_0, \cdots, a_{k+1}$ are undetermined rationals. Substituting (11) and (12) into (13), replacing all of the ω_{l_i} by powers of ω_l for some sufficiently large l, and rearranging terms, we obtain a polynomial in $r_1, \cdots, r_k, z, \pi$, and ω_l whose degree in ω_l is less than the degree of the minimal polynomial of ω_l and whose coefficients are integral linear combinations of $a_0, \cdots, a_{k+1}$. Because of the algebraic independence of the set $\{r_1, \cdots, r_k, z, \pi\}$, equation (13) implies that all of these coefficients vanish. Thus we obtain a set of homogeneous integral linear equations in the unknowns $a_0, \cdots, a_{k+1}$. Since the set $\{q_1, \cdots, q_k, i\pi\}$ is linearly independent, a_{k+1} must be nonzero in any nontrivial solution vector, and the solution space, if any, must be one dimensional. Using standard linear methods we can determine whether or not a solution exists, and if so, we can find it.

If a solution exists, go on to Step 5a. Otherwise, proceed to Step 5b.

Step 5*a* (*Linear dependence—replace* q_{k+1} *and* r_{k+1}). In this case we can write

(14) $$q_{k+1} = \frac{b_0 i\pi}{2c_0} + \sum_{i=1}^{k} \frac{b_i q_i}{c_i},$$

where b_i and c_i are relatively prime integers for $i=0, \cdots, k$. Letting

(15) $$q_i' = \frac{q_i}{c_i}, \qquad r_i' = \exp q_i', \qquad i = 1, \cdots, k$$

we have

(16) $$r_i = \exp(q_i) = \exp(c_i q_i') = (r_i')^{c_i}, \qquad i = 1, \cdots, k$$

and

(17) $$r_{k+1} = \exp(q_{k+1}) = \omega_{c_0}^{b_0} \cdot \prod_{i=1}^{k} (r_i')^{b_i}.$$

Substitute (16) and (17) into (10), set $k'=k$, and proceed to Step 6.

Step 5*b* (*Linear independence—adjoin* q_{k+1}). In this case the set

$$\{q_1, \cdots, q_{k+1}, i\pi\}$$

is linearly independent. Now, in (10), replace r_i by r_i' for all $i=1, \cdots, k'=k+1$, and proceed to Step 6.

Step 6 (*Simplify* (10) *weakly*). Simplify (10) weakly, treating $r_1', \cdots, r_{k'}'$ as indeterminates. The result is an expression of the form

(10′) $$\frac{f(\exp p_1', \cdots, \exp p_{n'}', r_1', \cdots, r_{k'}', z, \pi, \omega_m')}{g(\exp p_1', \cdots, \exp p_{n'}', r_1', \cdots, r_{k'}', z, \pi)}$$

where the $p_1', \cdots, p_{n'}'$ may depend on the $r_1', \cdots, r_{k'}'$. Note that the set $\{r_1', \cdots, r_{k'}', z, \pi\}$ is algebraically independent, by the fundamental conjecture.

Step 7 (*Iterate*). Drop all primes, so that (10′) replaces (10), and return to Step 2.

Acknowledgment. The author wishes to thank A. J. Goldstein for many valuable discussions throughout the course of this work.

References

1. Daniel Richardson, Some unsolvable problems involving functions of a real variable, Notices, Amer. Math. Soc., 13 (1966) 135.

2. B. F. Caviness, On canonical forms and simplification, Carnegie Institute of Technology Ph.D. Thesis, 1967.

3. David Hilbert, Mathematische Probleme, Bull. Amer. Math. Soc., 8 (1901–02) 437–479.

4. Martin Davis, Hilary Putnam, and Julia Robinson, The decision problem for exponential diophantine equations, Ann. of Math., 74 (1961) 425.

5. C. L. Siegel, Transcendental Numbers, Princeton University Press, Princeton, 1949, p. 84.

6. Harry Pollard, The Theory of Algebraic Numbers, MAA, Carus Monograph No. 9, Wiley, New York, 1950, p. 38.

MATHEMATICAL NOTES

Edited by David Drasin

Manuscripts for this Department should be sent to David Drasin, Division of Mathematical Sciences, Purdue University, Lafayette, IN 47907.

AN AREA-WIDTH INEQUALITY FOR CONVEX CURVES

Paul R. Chernoff, University of California, Berkeley

Theorem. *Let C be a closed convex plane curve, bounding a region of area A. Let $w(\theta)$ denote the width of C in the θ-direction. Then*

$$A \leqq \frac{1}{2}\int_0^{\pi/2} w(\theta)w\left(\theta+\frac{\pi}{2}\right)d\theta \tag{1}$$

with equality if and only if C is a circle.

Proof. We shall employ a method due to A. Hurwitz (see Courant [1] p. 213) to prove the isoperimetric inequality. It clearly suffices to establish the theorem for the case of C^2 curves such that for each θ, $0 \leq \theta < 2\pi$, there is exactly one point, say $(x(\theta), y(\theta))$, at which the normal to C makes an angle θ with the X-axis. Then, as Courant indicates, there is a C^2 periodic function $p(\theta)$ such that

$$\begin{aligned} x(\theta) &= p(\theta)\cos\theta - p'(\theta)\sin\theta \\ y(\theta) &= p(\theta)\sin\theta + p'(\theta)\cos\theta. \end{aligned} \tag{2}$$