When Close Enough Is Close Enough

Edward R. Scheinerman

I. PRELUDE: AN INTERCHANGE BETWEEN AN ALGEBRA TEACHER AND STUDENT. A student was asked to demonstrate the following equation:

$$\sqrt{2} + \sqrt{5} - 2\sqrt{6} = \sqrt{3}.$$  

**Teacher:** Please show me your solution to this problem.  

**Student:** Sure. At first I was confused, but then I had a great idea. I just used my calculator. Both sides of the equation evaluate to 1.732050808. So they’re the same!  

**Teacher:** Hmm. That’s a good idea, but it doesn’t really answer the question. You see, your calculator can display only 10 digits. It’s possible that these two numbers agree to 10 decimal places, but aren’t equal.  

**Student:** Get out! I don’t believe that two expressions that agree to that many digits could be different.  

**Teacher:** Actually, they could. Let me give you an example. Do you have your calculator with you?  

**Student:** Yes.  

**Teacher:** Excellent. Please calculate

$$\sqrt{75025} + \sqrt{121393} + \sqrt{196418} + \sqrt{317811}.$$  

**Student:** *(after a brief pause)* I get 1629.259889.  

**Teacher:** Good. Now please calculate

$$\sqrt{514229} + \sqrt{832040}.$$  

**Student:** *(another brief pause)* I get 1629.259889. Hey! That’s the same as before. They’re equal.  

**Teacher:** Well, actually, they’re not equal.  

**Student:** How do you know?  

**Teacher:** Let me show you on my computer. I have a program that will let us calculate these expressions with much greater accuracy than your calculator.  

First I type

```plaintext
sqrt(75025) + sqrt(121393) + sqrt(196418) + sqrt(317811)
```

and the computer responds: 1629.259888633142299848838800.  

**Student:** Wow! That’s 28 digits.  

**Teacher:** It is nice. Now I type

```plaintext
sqrt(514229) + sqrt(832040)
```

and the computer gives 1629.259888630189238404283301. Look closely. Notice that the ninth digits after the decimal points are different. So you see, even though your calculator gives the same
(approximate) value for the two expressions, that does not mean they are exactly equal.
Do you understand?

Student: You bet! You have a much better calculator than I have. May I try?
Teacher: Yes, but . . .
Student: Let’s see. I type sqrt(2) + sqrt(5-2*sqrt(6)) and hit return. I get 1.732050807568877293527446341.
Teacher: Yes, but . . .
Student: And then I type sqrt(3) and—LOOK!—it gives me exactly the same answer: 1.732050807568877293527446341. You see, they are equal.
Will we be allowed to use your computer on the test?
Teacher: Sigh!

2. WHO IS RIGHT? This is not an article bemoaning the state of mathematics education. And I am sure that readers of this MONTHLY will have no trouble verifying that $\sqrt{2} + \sqrt{5 - 2\sqrt{6}}$ and $\sqrt{3}$ are equal. Rather, my purpose is to defend the student.

The student’s intuition is that if two algebraic expressions such as $\sqrt{2} + \sqrt{5 - 2\sqrt{6}}$ and $\sqrt{3}$ agree to 28 digits, then surely they are equal.

We transform the student’s intuition by asking: When does $|\alpha - \beta| < \varepsilon$ imply $\alpha = \beta$? For example, if $\alpha$ and $\beta$ are integers, then if we know that $|\alpha - \beta|$ is (say) less than 0.9, then we may conclude that $\alpha = \beta$.

Here is another example. Suppose $\alpha$ and $\beta$ are both roots of some monic (leading coefficient equal to 1) quadratic polynomial with integer coefficients: $x^2 + bx + c$. Then

$$|\alpha - \beta| = |\sqrt{b^2 - 4c}|.$$ 

Since $b^2 - 4c$ is an integer, we have either $\alpha = \beta$, or else $|\alpha - \beta| \geq 1$. So if we know that $|\alpha - \beta| < 0.9$, we may conclude that $\alpha = \beta$.

The two sides of the equation $\sqrt{2} + \sqrt{5 - 2\sqrt{6}} = \sqrt{3}$ are not integers. It is not a priori obvious that they are roots of a common, monic quadratic polynomial. However, one can show that $\sqrt{2} + \sqrt{5 - 2\sqrt{6}} - \sqrt{3}$ is the root of some monic, integer polynomial; such roots are known as algebraic integers. Thus, one approach to making the student’s intuition rigorous is to develop the theory of algebraic integers; see [16]. Instead, we present an equivalent theory based on eigenvalues of matrices; the proofs are sufficiently straightforward that they can be presented in an undergraduate linear algebra class. This will enable us to answer the question: When is close enough, close enough?

3. EIGENVALUES OF INTEGER MATRICES. Let $n$ and $b$ be positive integers. Let $M(n, b)$ denote the set of all $n \times n$ matrices whose entries are integers bounded in absolute value by $b$. That is, if $A \in M(n, b)$, then $A$ is $n \times n$, $a_{ij} \in \mathbb{Z}$, and $|a_{ij}| \leq b$. Let $\Lambda(n, b)$ denote the set of all eigenvalues of matrices in $M(n, b)$. Note that $\Lambda(n, b)$ is a finite set of complex numbers, and therefore we can bound the absolute values of its nonzero members away from zero (see Theorem 4).
**Proposition 1.** Let $A \in M(n, b)$. Then $\det(\lambda I - A)$ is a monic, integer polynomial.

(By integer polynomial we mean a polynomial whose coefficients are integers.)

Proof: Use induction and the cofactor expansion formula. ■

**Proposition 2.** Let $\alpha$ be a complex number. Then $\alpha$ is an algebraic integer if and only if $\alpha \in \Lambda(n, b)$ for some positive integers $n, b$.

Proof: If $\alpha$ is an algebraic integer, then it is the root of some monic, integer polynomial $p(x)$. Then $\alpha$ is an eigenvalue of the companion matrix of $p$, and so $\alpha \in \Lambda(n, b)$ for some $n, b$.

The converse follows from Proposition 1. ■

**Proposition 3.** Suppose $\alpha \in \Lambda(n, b)$. Then $|\alpha| \leq nb$.

Proof: Suppose $\alpha$ is an eigenvalue of $A \in M(n, b)$ with corresponding eigenvector $v$. Without loss of generality, we may assume that $v$ is a unit vector, i.e., $v \cdot v = 1$.

Since $v \cdot Av = v \cdot \alpha v = \alpha$, we have

$$|\alpha| = |v \cdot Av| = \left| \sum_i \sum_j v_i a_{i,j} v_j \right| \leq b \sum_i \sum_j |v_i v_j| = b \sum_i |v_i| \sum_j |v_j| = b \|v\|_1^2,$$

Since $\|v\|_1 \leq \sqrt{n} \|v\|_2$ (see [8, problem 3, p. 278]) we have $|\alpha| \leq nb$. ■

The bound is best possible: Let $A$ be an $n \times n$ matrix all of whose entries are $b$. Let $1$ be the vector of all 1s. Then $A1 = nb1$.

**Theorem 4.** Suppose $A \in M(n, b)$ and $\alpha$ is a nonzero eigenvalue of $A$. Then $|\alpha| \geq (nb)^{1-n}$.

Proof: Suppose the nonzero eigenvalues of $A$ are $\alpha, \lambda_2, \ldots, \lambda_l$. The last nonzero coefficient of the characteristic polynomial of $A$ is $\pm \alpha \lambda_2 \cdots \lambda_l$. By Proposition 1, this is an integer, hence $|\alpha \lambda_2 \cdots \lambda_l| \geq 1$ and so

$$|\alpha| \geq \frac{1}{|\lambda_2 \cdots \lambda_l|} \geq (nb)^{1-l} \geq (nb)^{1-n}.$$ ■

Theorem 4 is a known as a root separation theorem; see [2], [3], or [14]. It enables us to answer the question: When is close enough, close enough? Suppose we are given an algebraic expression, such as $\alpha = \sqrt{2} + \sqrt[4]{5 - 2\sqrt{6}} - \sqrt[3]{3}$. We need to find integers $n$ and $b$ such that $\alpha \in \Lambda(n, b)$. Then we calculate $\alpha$ to sufficient precision to show that $|\alpha| < (nb)^{1-n}$. From this, it follows that $\alpha = 0$.

The issue, then, is: Given an algebraic expression $\alpha$, how do we find positive integers $n$ and $b$ such that $\alpha \in \Lambda(n, b)$? The next result gives us tools to find $n$ and $b$. 

---

June–July 2000] WHEN CLOSE ENOUGH IS CLOSE ENOUGH 491
Theorem 5. Let \( n, n_1, n_2, b, b_1, b_2 \) be positive integers.

1. If \( \alpha \) is a root of a monic, integer polynomial of degree \( n \) whose coefficients have absolute value no larger than \( b \), then \( \alpha \in \Lambda(n, b) \).
2. If \( n_1 \leq n_2 \) and \( b_1 \leq b_2 \), then \( \Lambda(n_1, b_1) \subseteq \Lambda(n_2, b_2) \).
3. If \( \alpha \in \Lambda(n, b) \), then \( -\alpha \) and \( \overline{\alpha} \in \Lambda(n, b) \).
4. If \( k \) is an integer, then \( k \in \Lambda(1, |k|) \).
5. If \( \alpha \in \Lambda(n_1, b_1) \) and \( \beta \in \Lambda(n_2, b_2) \), then \( \alpha \beta \in \Lambda(n_1 n_2, b_1 b_2) \).
6. If \( \alpha \in \Lambda(n_1, b_1) \) and \( \beta \in \Lambda(n_2, b_2) \), then \( \alpha + \beta \in \Lambda(n_1 n_2, b_1 + b_2) \).
7. If \( k \) is a positive integer and \( \beta^k \in \Lambda(n, b) \), then \( \beta \in \Lambda(nk, b) \).

We illustrate the use of Theorem 5 by solving the following type of problem: Given an algebraic expression \( \alpha \), determine integers \( n \) and \( b \) such that \( \alpha \in \Lambda(n, b) \).

Consider the expression:

\[
\alpha = \sqrt[3]{7} \times \sqrt{5} - \sqrt{2} .
\]

The atoms of this expression are the integers 2, 5, and 7. By part 4, we have

\[
2 \in \Lambda(1, 2), \quad 5 \in \Lambda(1, 5), \quad \text{and} \quad 7 \in \Lambda(1, 7) .
\]

Next we classify \( \sqrt{2} \) and \( \sqrt[3]{7} \); by part 7, we have

\[
2 \in \Lambda(1, 2) \Rightarrow \sqrt{2} \in \Lambda(2, 2) \quad \text{and} \quad 7 \in \Lambda(1, 7) \Rightarrow \sqrt[3]{7} \in \Lambda(2, 7) .
\]

The classification of \( 5 - \sqrt{2} \) follows from parts 3 and 6:

\[
\sqrt{2} \in \Lambda(2, 2) \Rightarrow -\sqrt{2} \in \Lambda(2, 2) \Rightarrow 5 + (-\sqrt{2}) \in \Lambda(1 \cdot 2, 5 + 2) = \Lambda(2, 7) .
\]

To classify the cube root of \( 5 - \sqrt{2} \) we use part 7:

\[
5 - \sqrt{2} \in \Lambda(2, 7) \Rightarrow \sqrt[3]{5 - \sqrt{2}} \in \Lambda(2 \cdot 3, 7) = \Lambda(6, 7) .
\]

Finally, part 5 gives us the final classification:

\[
\begin{align*}
\sqrt[3]{7} \in \Lambda(2, 7) \\
\sqrt[3]{5 - \sqrt{2}} \in \Lambda(6, 7)
\end{align*}
\]

\[
\Rightarrow \alpha = \sqrt[3]{7} \times \sqrt[3]{5 - \sqrt{2}} \in \Lambda(2 \cdot 6, 7 \cdot 7) = \Lambda(12, 49) .
\]

These calculations are illustrated in Figure 1.

![Figure 1](image_url)

Figure 1. Using Theorem 5 to classify an algebraic expression.
The proof of Theorem 5 is given in the next section. However, we encourage the reader to be impatient and to proceed directly to Section 5. Return to the proof on your second reading.

4. PROOF OF THEOREM 5

Proof: For part 1, see the proof of Proposition 2.

For part 2, suppose \( \alpha \) is an eigenvalue of \( A \in M(n_1, b_1) \). Let \( B \) be the \( n_2 \times n_2 \) matrix \( \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix} \in M(n_2, b_2) \). Since \( \alpha \) is also an eigenvalue of \( B \), it follows that \( \alpha \in \Lambda(n_2, b_2) \).

For part 3, suppose \( \alpha \) is an eigenvalue of \( A \in M(n, b) \). Then \( \bar{\alpha} \) is also an eigenvalue of \( A \) and \( -\alpha \) is an eigenvalue of \( -A \). Hence \( -\alpha, \bar{\alpha} \in \Lambda(n, b) \).

For part 4, note that \( k \) is the eigenvalue of the matrix \([k]\).

For parts 5 and 6 we use the Kronecker (tensor) product of matrices [6]. Suppose \( A \) is a \( p \times q \) matrix and \( B \) is an \( r \times s \) matrix. The Kronecker product of \( A \) and \( B \) is the \( pr \times qs \) matrix

\[
A \otimes B = \begin{bmatrix}
a_{11}B & a_{12}B & \cdots & a_{1q}B \\
a_{21}B & a_{22}B & \cdots & a_{2q}B \\
\vdots & \vdots & \ddots & \vdots \\
a_{p1}B & a_{p2}B & \cdots & a_{pq}B
\end{bmatrix}
\]

One checks that if \( v \) is a \( p \)-vector and \( w \) is a \( q \)-vector, then

\[
(A \otimes B)(v \otimes w) = (Av) \otimes (Bw).
\]

Now suppose \( \alpha \) is an eigenvalue of \( A \in M(n_1, b_1) \) corresponding to an eigenvector \( v \). Likewise, suppose \( \beta \) is an eigenvalue of \( B \in M(n_2, b_2) \) corresponding to an eigenvector \( w \). Then \( A \otimes B \in M(n_1n_2, b_1b_2) \) and

\[
(A \otimes B)(v \otimes w) = (Av) \otimes (Bw) = (\alpha v) \otimes (\beta w) = (\alpha \beta)(v \otimes w),
\]

and so \( \alpha \beta \) is an eigenvalue of \( A \otimes B \) and hence is in \( \Lambda(n_1n_2, b_1b_2) \).

Next, let \( C = A \otimes I_{n_2} + I_{n_1} \otimes B \), so \( C \in M(n_1n_2, b_1 + b_2) \). Observe that

\[
C(v \otimes w) = (A \otimes I_{n_2})(v \otimes w) + (I_{n_1} \otimes B)(v \otimes w)
= (Av \otimes w) + (v \otimes Bw)
= \alpha(v \otimes w) + \beta(v \otimes w) = (\alpha + \beta)(v \otimes w).
\]

Hence \( \alpha + \beta \) is an eigenvalue of \( C \) and therefore is in \( \Lambda(n_1n_2, b_1 + b_2) \).

Finally, for part 7, let \( k \) be a positive integer and let \( \alpha \in \Lambda(n, b) \). Suppose \( \beta \) is a \( k^{th} \) root of \( \alpha \), i.e., \( \beta^k = \alpha \). Let \( A \in M(n, b) \) be a matrix for which \( \alpha \) is an eigenvalue and let \( v \) be a corresponding eigenvector.

Let \( B \) be the \( nk \times nk \) matrix with block structure

\[
B = \begin{bmatrix}
0 & I & 0 & 0 & \cdots & 0 \\
0 & 0 & I & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & I & \cdots & 0 \\
A & 0 & 0 & 0 & \cdots & 0
\end{bmatrix}
\]

Note that \( B \in M(nk, b) \).
Define the vector $\mathbf{w}$ to be
\[
\mathbf{w} = \begin{bmatrix}
\mathbf{v} \\
\beta \mathbf{v} \\
\beta^2 \mathbf{v} \\
\vdots \\
\beta^{k-2} \mathbf{v} \\
\beta^{k-1} \mathbf{v}
\end{bmatrix}
\]

We calculate
\[
B \mathbf{w} = \begin{bmatrix}
\beta \mathbf{v} \\
\beta^2 \mathbf{v} \\
\beta^3 \mathbf{v} \\
\vdots \\
\beta^{k-1} \mathbf{v} \\
A \mathbf{v}
\end{bmatrix} = \begin{bmatrix}
\beta \mathbf{v} \\
\beta^2 \mathbf{v} \\
\beta^3 \mathbf{v} \\
\vdots \\
\beta^{k-1} \mathbf{v} \\
\alpha \mathbf{v}
\end{bmatrix} = \beta \mathbf{w}
\]

and therefore $\beta$ is an eigenvalue of $B$. Thus $\beta \in \Lambda(nk, b)$. ■

5. PROOF OF AN IDENTITY. Theorems 4 and 5 give us a technique to prove identities. We begin by re-expressing the identity in the form $\alpha = 0$. We use Theorem 5 to find $n$ and $b$ for which $\alpha \in \Lambda(n, b)$. By Theorem 4, if $\alpha \neq 0$, then $|\alpha| \geq (nb)^{1-n}$. We then calculate $\alpha$ to sufficiently many digits to show $|\alpha| < (nb)^{1-n}$, and we conclude $\alpha = 0$.

We illustrate this technique by proving the student's identity:
\[
\sqrt{2} + \sqrt{5 - 2\sqrt{6}} = \sqrt{3}.
\]

The first step is to apply Theorem 5 to find integers $n$ and $b$ so that $\alpha = \sqrt{2} + \sqrt{5 - 2\sqrt{6}} - \sqrt{3} \in \Lambda(n, b)$.

Since $2 \in \Lambda(1, 2)$ (part 4) we have $\sqrt{2} \in \Lambda(2, 2)$ (part 7).

Likewise, $\sqrt{3} \in \Lambda(2, 3)$, and so $-\sqrt{3} \in \Lambda(2, 3)$ (part 3).

Since $\sqrt{6} \in \Lambda(2, 6)$ and $-2 \in \Lambda(1, 2)$, we have $-2\sqrt{6} \in \Lambda(2, 12)$ (part 5). Since $5 \in \Lambda(1, 5)$, we have $5 - 2\sqrt{6} \in \Lambda(2, 17)$ (part 6). Hence $\sqrt{5 - 2\sqrt{6}} \in \Lambda(4, 17)$.

Finally, $\alpha = \sqrt{2} + \sqrt{5 - 2\sqrt{6}} - \sqrt{3}$ is in $\Lambda(2 \cdot 4 \cdot 2, 2 + 17 + 3) = \Lambda(16, 22)$ (part 6).

Now we apply Theorem 4. If $\alpha \neq 0$ we would have
\[
|\alpha| \geq (16 \cdot 22)^{-15} \approx 6.3 \times 10^{-39}.
\]

However, calculating $\alpha$ to (say) 45 digits enables us to conclude that $|\alpha| < 10^{-44}$ and so $\alpha = 0$.

To ease the computational burden, we want to find the smallest $n$ and $b$ for which $\alpha \in \Lambda(n, b)$. For example, consider the term $2\sqrt{6}$. We showed that $2\sqrt{6} \in \Lambda(2, 12)$. Can we do better? Rewriting $2\sqrt{6}$ as $\sqrt{24}$ doesn’t help, because $24 \in \Lambda(1, 24)$ and then part 7 gives $2\sqrt{6} = \sqrt{24} \in \Lambda(2, 24)$. However, it is easy to see that $\sqrt{24}$ is an eigenvalue of $\begin{bmatrix} 0 & 6 \\ 4 & 0 \end{bmatrix}$. Thus, $2\sqrt{6} \in \Lambda(2, 6)$.
In general, we have the following.

**Proposition 6.** If \(a\) and \(b\) are integers, then \(\sqrt{ab} \in \Lambda(2, \max\{|a|, |b|\})\).

Using \(2\sqrt{6} \in \Lambda(2, 6)\) improves our earlier analysis to \(\alpha \in \Lambda(16, 16)\) and so the separation bound is \((16 \cdot 16)^{-15} \approx 7.5 \times 10^{-37}\), a modest gain of two digits.

We can improve the bound a little more by recognizing \(5 - 2\sqrt{6}\) as a root of the quadratic equation \(x^2 - 10x + 1 = 0\), giving \(5 - 2\sqrt{6} \in \Lambda(2, 10)\), leading to \(\alpha \in \Lambda(16, 15)\) and a separation bound of roughly \(2 \times 10^{-36}\).

However, the recognition of \(5 - 2\sqrt{6}\) as a root of \(x^2 - 10x + 1\) is far from automatic and such recognition may be difficult for more complicated expressions. Fortunately, this can be reduced to a calculation.

Given a numeric approximation of an expression, such as \(5 - 2\sqrt{6}\), symbolic mathematics software can find a low-degree polynomial with a root (nearly) equal to the given expression.

For example, in *Mathematica*, we can calculate as follows:

```mathematica
Needs["NumberTheoryRecognize"]
a = 5 - 2Sqrt[6];
Recognize[N[a], 2, x]

2
1 - 10 x + x
```

The first line loads the Recognize package. The second line defines \(a\) to be \(5 - 2\sqrt{6}\). The third line asks *Mathematica* to find a degree-2 polynomial in \(x\) of which (a numerical approximation of) \(a\) is a root.

The recognition of \(\alpha\) as a root of some polynomial is a computation. Can we also reduce the proof that \(\alpha\) is the root of some polynomial to a computation?

For example, if we let \(\alpha = \sqrt[3]{5\sqrt{13} - 18}\), *Mathematica* asserts that \(\alpha\) is a root of \(x^2 + 3x - 1 = 0\). We might try to verify this by expanding \(\alpha^2 + 3\alpha - 1\) and checking to see if we get zero. However, that leads to the messy expression

\[
(5\sqrt{13} - 18)^{2/3} + 3(5\sqrt{13} - 18)^{1/3} - 1
\]

and I don’t want to be bothered wrestling with that. I want to crunch those numbers, get something near zero, and be convinced.

One way to verify that \(\alpha\) is a root of \(p(x) = x^2 + 3x - 1\) is to apply the earlier method, i.e., find \(n\) and \(b\) so that \(p(\alpha) \in \Lambda(n, b)\). However, the techniques we have presented lead to \(p(\alpha) \in \Lambda(9288, 1893)\). Thus, to verify \(p(\alpha) = 0\) we need to show that

\[
|p(\alpha)| < (9288 \cdot 1893)^{-1892} \approx 10^{-13708}.
\]

And while computers can calculate to that level of accuracy, a looser bound is clearly desirable.

Using Theorem 5 and Proposition 6, we can place \(\alpha = \sqrt[3]{5\sqrt{13} - 18} \in \Lambda(6, 43)\). Therefore, there is an \(A \in M(6, 43)\) with eigenvalue \(\alpha\). Note that \(p(\alpha)\) is an eigenvalue of \(B = p(A)\). We can bound the absolute value of the entries of \(B\) as follows. Let \(J\) be the \(6 \times 6\) matrix of all 1s. Then

\[
|B| = |p(A)| \leq |A^2| + 3|A| + I \leq (43J)^2 + 3(43J) + I \leq 11098 J.
\]

(For a matrix \(X\) whose \(i, j\)-entry is \(x_{ij}\), we write \(|X|\) for the matrix whose \(i, j\)-entry is \(|x_{ij}|\).)
Therefore \( p(\alpha) \in \Lambda(6, 11098) \). To prove that \( p(\alpha) = 0 \) it is enough to show that
\[
|p(\alpha)| < (6 \cdot 11098)^{-5} \approx 7.6 \times 10^{-23}.
\]
The computer easily verifies this, and therefore \( \alpha \) is a root of \( x^2 + 3x - 1 \). Since \( \alpha \approx 0.3028 \) and since the two roots of \( x^2 + 3x - 1 = 0 \) are \( \frac{1}{2}(-3 \pm \sqrt{13}) \) we have proved that
\[
\frac{\sqrt{\sqrt{5} \sqrt{13}} - 18}{2} = -3 + \frac{\sqrt{13}}{2}.
\]

We return to the earlier student/teacher example: We want to show that \( \alpha = \sqrt{2} + \sqrt{5 - 2\sqrt{6}} \) is a root of \( p(x) = x^2 - 3 = 0 \). By Theorem 5 and Proposition 6, we have \( \alpha \in \Lambda(8, 13) \), and so there is a matrix \( A \in M(8, 13) \) of which \( \alpha \) is an eigenvalue. Hence, \( p(\alpha) = \alpha^2 - 3 \) is an eigenvalue of \( B = p(A) \). We have
\[
|B| = |p(A)| = |A^2 - 3I| \leq \left| (13J)^2 \right| + 3I = 1352J + 3I
\]
where \( J \) is the \( 8 \times 8 \) matrix of all ones. Thus \( B \in M(8, 1355) \). So, by Theorem 4, if \( \beta \neq 0 \) we would have
\[
|p(\alpha)| = |\beta| \geq (8 \cdot 1355)^{-7} \approx 5.7 \times 10^{-29}.
\]
However, the result of calculating \( p(\alpha) \) to (more than) 30 decimal places is zero, and so we may conclude that \( p(\alpha) = 0 \), and so \( \sqrt{2} + \sqrt{5 - 2\sqrt{6}} = \sqrt{3} \).

In general, suppose \( \alpha \in \Lambda(n, b) \) and \( p \) is a monic, integer polynomial of degree \( d \) whose coefficients are bounded in absolute value by \( c \). Then we can easily calculate a positive \( \varepsilon_{n, b, d, c} \) so that
\[
|p(\alpha)| < \varepsilon_{n, b, d, c} \Rightarrow p(\alpha) = 0.
\]

6. A MORE COMPLICATED EXAMPLE. We have presented a simple method for proving algebraic identities formed from integers using the operations \( +, -\), \( \times \), and \( \sqrt[k]{\cdot} \). One applies the rules in Theorem 5 to find \( n \) and \( b \) with \( \alpha \in \Lambda(n, b) \). Then we calculate \( \alpha \) to sufficient precision to verify that \( |\alpha| < (nb)^{\frac{1}{n}} \). Then Theorem 4 implies that \( \alpha = 0 \).

Now for a harder example. We solve Problem #10756 from the October 1999 issue of this MONTHLY. The problem asks us to prove:
\[
\cos \frac{\pi}{7} = \frac{1}{6} + \frac{\sqrt{7}}{6} \left[ \cos \left( \frac{1}{3} \arccos \frac{1}{2\sqrt{7}} \right) + \sqrt{3} \sin \left( \frac{1}{3} \arccos \frac{1}{2\sqrt{7}} \right) \right].
\]

From
\[
\cos(n\theta) + i\sin(n\theta) = (\cos \theta + i\sin \theta)^n = \sum_{k=0}^{n} \binom{n}{k} (\cos \theta)^k (i\sin \theta)^{n-k}
\]
and the identity \( \cos^2 \theta + \sin^2 \theta = 1 \) we get the following identities:
\[
\cos 3\theta = 4\cos^3 \theta - 3\cos \theta
\]
and
\[
\cos 7\theta = 64\cos^7 \theta - 112\cos^5 \theta + 56\cos^3 \theta - 7\cos \theta.
\]
Substituting \( \theta = \pi \) and \( \alpha = 2\cos(\pi/7) \) into the second identity gives
\[
-1 = \frac{1}{2} \alpha^7 - \frac{7}{2} \alpha^5 + 7\alpha^3 - \frac{7}{2} \alpha.
\]
or equivalently
\[ 0 = \alpha^7 - 7\alpha^5 + 14\alpha^3 - 7\alpha + 2 = (\alpha^3 - \alpha^2 - 2\alpha + 1)^2 (\alpha + 2). \]
Clearly \(\alpha \neq -2\), so \(\alpha = 2\cos(\pi/7) \in \Lambda(3, 2)\).

Next we tackle the term
\[ \sqrt{7} \cos \left( \frac{1}{3} \arccos \frac{1}{2\sqrt{7}} \right). \]
In \(\cos 3\theta = 4\cos^3\theta - 3\cos \theta\) we take
\[ \theta = \frac{1}{3} \arccos \frac{1}{2\sqrt{7}} \]
and let \(\beta_0 = \cos \theta\). Then we have
\[ \frac{1}{2\sqrt{7}} = 4\beta_0^3 - 3\beta_0. \]
Taking \(\beta = 2\sqrt{7}\beta_0\) this becomes \(\beta^3 - 21\beta - 7 = 0\), so
\[ \beta = 2\sqrt{7} \cos \left( \frac{1}{3} \arccos \frac{1}{2\sqrt{7}} \right) \in \Lambda(3, 21). \]

Now we deal with the sine term. From \(\sin 3\theta = -4\sin^3\theta + 3\sin \theta\) with \(\theta\) defined by (1) we have \(\sin 3\theta = \sqrt{27/28}\). Let \(\gamma_0 = \sin \theta\) and we have
\[ 4\gamma_0^3 - 3\gamma_0 + \sqrt{\frac{27}{28}} = 0. \]
Let \(\gamma = 2\sqrt{7} \cdot \sqrt{3} \gamma_0\) to rewrite this as \(\gamma^3 - 63\gamma + 189 = 0\). Therefore, \(\gamma = 2\sqrt{7} \cdot \sqrt{3} \sin \theta \in \Lambda(3, 189)\).

Recapping, we have
\[ \alpha = 2\cos \frac{\pi}{7} \in \Lambda(3, 2), \quad \beta = 2\sqrt{7} \cos \theta \in \Lambda(3, 21), \quad \text{and} \]
\[ \gamma = 2\sqrt{7} \cdot \sqrt{3} \sin \theta \in \Lambda(3, 189) \]
where \(\theta\) is defined by (1).

We can reexpress the MONTHLY problem as
\[ \zeta = 6\alpha - 2 - \beta - \gamma^2 = 0. \]
Since \(6\alpha \in \Lambda(3, 12)\), we have
\[ \zeta \in \Lambda(3 \cdot 3 \cdot 3, 12 + 2 + 21 + 189) = \Lambda(27, 224). \]
Therefore, if \(\zeta \neq 0\) we would have \(|\zeta| \geq (27 \cdot 224)^{-26} \approx 4.77 \times 10^{-90}\), but calculating \(\zeta\) with more than 100 digits of accuracy shows that \(|\zeta| < 10^{-100}\) and so \(\zeta = 0\).

7. COMPUTER SCIENCE APPLICATIONS. This “close enough” technique for proving algebraic identities is a fun application of algebraic integers via linear algebra. Surprisingly, this method finds direct application in computer science.

Computational geometers develop their algorithms using a model of computation known as “the real RAM”. In this model, an arbitrary real number consumes a single unit of storage, and the primitive operations are exact real arithmetic and exact tests of equality and order.
Initially, when these algorithms were deployed on actual computers, the idealized real RAM was replaced by floating point arithmetic. The results were disappointing. Round-off errors resulted in program failure.

Consequently, computer scientists sought a way to handle real numbers on real computers. The basic geometric objects handled by computational geometries are points, lines/line segments, and circles/arcs. Hence, the arena of today's computational geometries is the same as that of the ancient Greeks, and the real numbers they encounter are all constructible: formed from integers using the basic operations of $+,-,\times, \div$, and $\sqrt{\cdot}$.

Computational geometry “kernels” are now being developed that hold real numbers as a data structure of nested radicals; see [4], [15], and [17]. Equality testing is done by numerically approximating the expressions to sufficiently many digits to guarantee the results.

The close-enough method for verifying identities can be computationally inefficient. The verification of a modestly complicated expression might require an enormous number of digits. The expression of the form $\sqrt{a_1} \pm \sqrt{a_2} \pm \cdots \pm \sqrt{a_i}$ is, by Theorem 5, in $\Lambda(2^t, a_1, a_2, \cdots, a_i)$, and to check if it is equal to zero, we must show that it is less than $(2^t a_1 a_2 \cdots a_i)^{1/2^t}$, i.e., exponentially many (as a function of $t$) digits.

Computational geometers are aware of this issue, and some have developed an approach to geometric algorithm design that studies the asymptotic running time of algorithms that are restricted to using primitives involving algebraic quantities whose polynomial is of bounded degree; see [12].

However, automatic verification of nested radical identities need not be so computationally intensive. For an alternate, algebraic approach, see the work of Landau in [9], [10], and [11].

8. FINAL REMARKS. We have presented a technique for proving identities involving algebraic integers. We classify the quantities involved as members of the classes $\Lambda(n, b)$ and then calculate numerically to sufficiently high precision to conclude equality. The technique can be extended to more general algebraic numbers by judiciously clearing denominators.

The technique raises a final question: Does a computer-assisted, calculation proof of a radical identity truly constitute a rigorous proof? The issue we need to consider is: Can we trust the computer and the programs it runs? In light of the early Pentium floating point flaws, it seems prudent to question the accuracy of calculations performed by computers. The CPU-resident floating point operations are beyond the inspection of nearly all computer users. However, there are public domain, arbitrary precision software programs (such as pari [1] and the Gnu MP package [7]) whose source code is available for inspection. In principle, one could check these programs in the same manner that one checks proofs in mathematics. Has this been done?

ACKNOWLEDGMENTS. Many thanks to Susan Landau and Michael Goodrich for their help with the computer science background material. Thanks also to Lara Diamond and David Marchette for their comments on early drafts of this article.

REFERENCES


498 © THE MATHEMATICAL ASSOCIATION OF AMERICA [Monthly 107]

EDWARD R. SCHEINERMAN is a professor in the Mathematical Sciences Department at the Johns Hopkins University. He was an undergraduate mathematics major at Brown, and received his Ph.D. in mathematics from Princeton. His research interests are in discrete mathematics. During academic year 1999–2000, he is an “internal visitor” to the Department of Mechanical Engineering at Hopkins.

*Department of Mathematical Sciences, The Johns Hopkins University, Baltimore, MD 21218*

ers@jhu.edu 

June–July 2000] WHEN CLOSE ENOUGH IS CLOSE ENOUGH 499