A practical deterministic method for zero recognition of polynomial terms

Daniel Richardson,
Computer Science, Bath University,
Bath BA2 7AY, UK
email: masdr@bath.ac.uk,
and
Ahmed El-Sonbaty,
email: mapaae@bath.ac.uk
Computer Science, Bath University

February 21, 2002

Abstract

The uniformity conjecture postulates a relationship between the syntactic length of expressions built up from the natural numbers using field operations, radicals and exponentials and logarithms, and the smallness of non zero complex numbers defined by such expressions. The Uniformity Conjecture claims that if the expressions are written in an expanded form in which all the arguments of the exponential function have absolute value bounded by 1, then a small multiple of the syntactic length gives a bound for the number of decimal places needed to distinguish the defined number from zero.

A polynomial term is a tree with operators $\ast, +, -$ on the interior nodes and natural numbers and variables on the frontier. We decide whether or not such a tree represents the zero polynomial by substituting algebraically independent real numbers for the variables and approximating the resulting constant with the accuracy which we believe, according to the uniformity conjecture, is sufficient to distinguish it from zero if it is not zero.
The result is that if a polynomial term has \( s(T) \) nodes, and the natural numbers on the frontier have logarithmic height bounded by \( h(T) \), then the bit complexity of zero recognition is bounded by \( O(s(T)M(s(T)^2 h(T))) \), where \( M(n) \) is the bit complexity of multiplication of two \( n \) digit natural numbers.

1 Introduction

The nested radical and exponential-logarithmic expressions are, roughly speaking, those which can be constructed from expressions for rational numbers using the operators \( \{ +, -, \times, \div, \sqrt{\cdot}, \exp, \log \} \).

In the section below, the family of nested radical exponential-logarithmic expressions, (exp-log expressions for short), is described and the field of closed form numbers is defined. An expanded form is defined for the exp-log expressions, and the Uniformity Conjecture is stated. This claims that for expressions in expanded form, a small multiple of the syntactic length bounds the number of decimal places needed to distinguish the defined number from zero, if it is non zero.

2 Closed Form Numbers and the Uniformity Conjecture

2.1 Expressions

We assume, to begin with, some canonical representation for the natural numbers. Then the set of nested radical exponential and logarithmic expressions is the smallest set of expressions so that:

1. All the representations of natural numbers are in the set.
2. If \( A \) and \( B \) are in the set so are \((A + B), (A - B), (A \times B), (A/B)\).
3. If \( A \) is in the set, so are \(-A, \exp(A) \text{ and } \log(A)\)
4. If \( A \) is in the set and \( n \) is a canonical representation of a natural number bigger than 1, then \( A^{1/n} \) is in the set.

Each nested radical exponential and logarithmic expression \( E \) is either undefined, or is interpreted as a real or complex number \( V(E) \), as follows.
1. If $E$ is a representation of an natural number, $V(E)$ is that natural number.

2. The operators are given the usual precedence in the absence of brackets.

3. If $A$ and $B$ are defined, then $V(A + B), V(A - B), V(A * B)$ and $V(-A)$ are defined with the usual interpretation of the operators. If $B$ is defined, and $V(B)$ is not zero, then $V(A/B)$ is defined, with the usual interpretation.

4. If $A$ is defined, then $\exp(A)$ is defined with meaning $e^A$.

5. If $A$ is defined, and $V(A) \neq 0$, then $\log(A)$ is defined, as the branch of the logarithm base $e$ so that $-\pi < \text{Im}(\log(A)) \leq \pi$.

6. If $A$ is defined and and $V(A) \neq 0$, and $n$ is a canonical representation of a natural number bigger than 1, then $A^{1/n}$ is defined and equal to $\exp(\log(A)/n)$.

The operator $V$ is called evaluation.

The complex numbers defined in this way are called closed form numbers [Chow]. We define the real closed form numbers to be the closed form numbers which happen to have zero imaginary part. Thus the real closed form numbers are closed under trigonometric functions as well as exponentiation and logarithms of positive numbers.

A field with good closure properties including the closed form numbers is the field of elementary numbers. These are numbers of the form $q(\alpha)$, where $q$ is in $\mathbb{Q}[x_1, \ldots, x_n]$, and $\alpha \in \mathbb{C}^n$ is a non singular solution of a system of equations $(p_1, \ldots, p_n) = 0$ and each $p_i$ is in $\mathbb{Z}[x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}]$. It has been shown that this is an effective field i.e., equality is decidable if the Schanuel conjecture is true. See [Richardson], [Richardson2].

Please notice that although we have expressions here for $n \text{ th roots}$, we do not have expressions for $n \text{ th powers}$. If we want $A^2$, for example, we have to write it as $A * A$.

2.2 Length of an expression

Our set of nested radical exponential and logarithmic expressions depends on a choice of canonical representation for the natural numbers. Assume that we have chosen some base $b$ for representation of the
natural numbers. We define the length of an natural number in this representation to be the number of digits base $b$ which are used.

Each exp-log expression may be considered as a tree with representations of natural numbers on the frontier and operators among $\{+, -, *, /, \sqrt{}, \exp, \log\}$ on the interior nodes. We allow $-$ to have arity either 1 or 2. The radical sign has arity 2, and one of its arguments must be a natural number in canonical form. We define the length of an expression to be the sum of the number of interior nodes, i.e. the number of operators, and the sum of the lengths of the representations of natural numbers on the frontier. We use $\text{length}(E)$ to denote the length of expression $E$.

So, for example, in decimal notation, $4 - 3 \times (10)^{1/8}$ would have length 8, since it has 5 digits and 3 operator symbols.

2.3 Gap Functions

**Definition 1** A gap function for the closed form numbers is a function $g : \text{Exp} \rightarrow \mathbb{R}_+$, where $\text{Exp}$ is the set of nested radical exponential and logarithmic expressions, so that if $x$ is a closed form number represented by an expression $A$, and $x \neq 0$ then $|x| > 10^{-g(A)}$

A gap function tells us the amount of decimal precision which is needed to distinguish a non zero number from zero. Of course gap functions exist. We hope that there is a computable gap function, and even an easily computable gap function.

An important question is: How does the evaluation operator $\cdot V$, behave with respect to the two natural measures we have namely, the length of an expression and the logarithm of the absolute value of complex numbers? For some more discussion of this question, (with a slightly different definition of length) one can refer to [Richardson2000].

2.4 Uniformity Conjecture

Using iterated exponentiation, it is possible to define very large numbers. Since we have division, it is also possible to define very small numbers with expressions involving iterated exponentiation, followed by division. There does not seem to be any other way to get very large numbers, or very small non zero numbers. ( Note that although we allow $n$th roots, we do not have $n$th powers. So we can not easily write
a short expression for the result of a sequence of repeated squarings, for example.)

**Definition 2** We consider an expression $E$ to be a subexpression of itself. We will say that an expression $E$ is in expanded form if for any exponential subexpression $e^A$ of $E$, we have $| V(A) | \leq 1$.

It appears to be true that it is not possible to define any very large numbers, or any very small non-zero numbers using small expressions in expanded form.

**Uniformity Conjecture**: If $E$ is an expression in expanded form, and $V(E) \neq 0$, then $| V(E) |$ is bigger than $1/N(k)$, where $k$ is the length of $E$, and $N(k)$ is the number of syntactically correct expanded form expressions of length $\leq k$.

Expressions of length less than $k$ can be coded as sequences of symbols of length $k$ by padding with an initial sequence of right brackets. This shows that the number of expressions which are syntactically correct of length no more than $k$ is bounded by the number of sequences of symbols of length $k$. Therefore, if we have $S$ symbols for operators and digits in our alphabet, the number of syntactically correct expressions of length $\leq k$ is bounded by $S^k$. In case we use decimal notation, for example, $S$ would be 17. In binary notation, $S$ would be 9.

Roughly speaking, the conjecture says that the amount of base $S$ precision which is needed to discriminate the value of an expanded form expression from zero is proportional to the length of the expression.

We will say that a number occurs at level $k$ if it has an exp-log expression representing it with length no more than $k$.

A weaker form of the uniformity conjecture may be obtained by replacing $N(k)$ by $N(Ck)$ for some universal constant $C$. A reason why at least this weaker form of the conjecture may seem plausible is that if a number $\alpha$ occurs at level $j$, then the neighbourhood of 0 at level $k$ translates to a subset of neighbourhood of $\alpha$ at level $k + j + 1$, since if $\alpha$ is represented by expression $A$, and a number $\epsilon$ is represented by an expression $E$, then $A + E$ will represent $\alpha + \epsilon$. Similarly, a neighbourhood of $\alpha$ at one level gets translated to a subset of a neighbourhood of 0 at a higher level; and so we would expect all the neighbourhoods of points, graded by level, to look alike, except for a change of scale.
The expressions we know which have small evaluations are not even close to being counterexamples. \(4/3 - 10^{1/8}\) is zero to three decimal places; \(7\log 2 - 3\log 5\) is zero to 2 decimal places, for example. Even if we add \(\pi\) as a constant to our language, We still do not know a counterexample in the enlarged language. The famous \(3 \ast \log(640320)/\sqrt{163} - \pi\) is only zero to 15 decimal places, whereas its syntactic length is 16 plus the length of \(\pi\). We can substitute \(\pi = \log(-1)/(-1)^{1/2}\) in which case the length of \(\pi\) would be 8.

The Uniformity conjecture is related to a family of conjectures, called Witness conjectures, originating with Joris van der Hoeven. See [VDH95, VDH97, VDH2000]. It is also related to the famous Schanuel conjecture. See [Lang].

Note that we can replace any expression which defines a value by an equivalent one in expanded form. But this is unlikely to be a good way to decide zero equivalence over the set of all nested radical exponential and logarithmic expressions. Joris van der Hoeven [VDH95] has suggested that expressions not in expanded form could be put into some sort of asymptotic form, as if the large numbers were exp-log functions which tended to infinity.

3 Polynomial Terms

We would like to consider representation of polynomials as trees with \(+, -, \ast\) on the interior nodes and with variables and natural numbers on the the leaves. Such a representation is significantly more succinct than any of the usual canonical representations of \(\mathbb{Z}[x_1, \ldots, x_n]\). On the other hand, it is much weaker than the computation tree representation discussed in the famous book Complexity and Real Computation see [BCSS]; and also much weaker than the standard straight line program representation. It is known that there is a probabilistic polynomial time method for zero recognition of straight line programs. See [Ibarra and Moran]. On the other hand, there is no known deterministic polynomial time solution for this problem. This question was discussed in in the PhD thesis of Bill Naylor [Naylor], who constructs GCD for polynomials represented as SLP (straight line programs). In general, the zero recognition problem for non canonical representations of polynomials is of much interest in computer algebra. See [Zippel] for a discussion. In this article we solve it by substituting algebraically.
independent numbers (see section 5) in place of the variables and assuming the Uniformity Conjecture. If $k$ is the length of the resulting nested exp-log expression we could recognise whether the given polynomial was zero by approximation with decimal precision $\log_{10}(17) k$. The resulting algorithm is not only polynomial time in theory, it is also feasible in practice. It compares very well in practice with other known deterministic algorithms.

For example, let $q(x)$ be some univariate polynomial with integer coefficients. Let $p_n(x_1, \ldots, x_n) = \prod_{i=1}^{n} q(x_i)$. The length of $p_n$ increases only linearly with $n$. If we are given the fact that $p_n$ has degree less than $d$ in each variable, we could deterministically verify that $p_n$ was not the zero polynomial by evaluating it on the cross product $(\{1, 2, \ldots, d\})^n$. We need $d^n$ elements in the product to avoid all the roots. It seems therefore that the method of zero recognition by substitution of integers uses a number of substitutions which must increase exponentially with the number of variables. However, if we can compute with algebraically independent numbers, we only need one substitution. This gives us an extra motivation for learning more about how to compute with classical non-algebraic numbers.

**Definition 3** size($T$) where $T$ is a polynomial term is defined by induction as follows:

$$\text{size}(A + B) = \text{size}(A - B) = \text{size}(A \ast B) := \text{size}(A) + \text{size}(B) + 1.$$  

For every natural number $n$, $\text{size}(n) := \text{length}(n)$

For the variables $x_1, \ldots, x_n$ we define $\text{size}(x_i) := i$.

By induction on the number of nodes or the size of a polynomial term one can prove the following

**Lemma 1** If $T$ is an polynomial term with real numbers on the frontier, $\text{s}(T)$ nodes, and the real numbers are bounded by $10^{k(T)}$ then the value $|T|$ represented by $T$ is bounded by $10^{k(T) \cdot \text{s}(T)}$.

## 4 Square roots of square free numbers

**Lemma 2** If $p_1, \ldots, p_n, q_1, \ldots, q_m ; n + m > 0$ are all different primes then

$$\frac{\prod_{i} \sqrt{p_i}}{\prod_{j} \sqrt{q_j}} \notin \mathbb{Q}$$
Proof.
The well known proof squares numerator and denominator and then uses unique factorisation among the integers. Similarly,

**Lemma 3** If \( x \in \mathbb{N} \) is a square-free natural number then \( \sqrt{x} \) is an irrational number.

A more general form of the last lemma is

**Lemma 4** If \( x \in \mathbb{N} \) is not a perfect square then its square root is an irrational number.

**Proof.** \( x \) is not a perfect square means that it is of the form \( x = a^2 s \) where \( s \) is the square free part of \( x \). So we have \( \sqrt{x} = a \sqrt{s} \) and hence \( \sqrt{x} \in \mathbb{Q} \iff \sqrt{s} \in \mathbb{Q} \). But by the last lemma we have \( \sqrt{s} \) is irrational and hence \( \sqrt{x} \) is irrational.

Now to prove the main result of this section we need some notions from algebra.

**Theorem 1** \( \sqrt{p_n} \notin \mathbb{Q} \left( \sqrt{p_1}, \ldots, \sqrt{p_{n-1}} \right) \) where, for all \( i \), \( p_i \) is the \( i \)'th prime number.

**Proof.** We make the convention: \( \mathbb{Q}_0 := \mathbb{Q} \) and by recursion we define for every natural number \( k \)

\[
\mathbb{Q}_k := \mathbb{Q} \left( \sqrt{p_1}, \ldots, \sqrt{p_k} \right)
\]

We assume that \( \sqrt{p_n} \in \mathbb{Q}_{n-1} = \mathbb{Q}_{n-2} \left( \sqrt{p_{n-1}} \right) \) for the sake of contradiction. This means that

\[
\sqrt{p_n} = a + b \sqrt{p_{n-1}}
\]

for some \( a, b \in \mathbb{Q}_{n-2} \). Depending on the values of \( a, b \) we get the following possibilities:

1. \( \sqrt{p_n} \in \mathbb{Q}_{n-2} \). This happens when \( b = 0 \).
2. \( -\sqrt{p_n} \in \mathbb{Q}_{n-2} \). This happens when \( a = 0 \).
3. \( \sqrt{p_{n-1}} \in \mathbb{Q}_{n-2} \). This is the case when \( a \) and \( b \) are not zero. In this case we square both sides of the equation above and arrange the resulting terms.
Continuing with this process, we reach at last a relation like this

\[ \frac{\sqrt{p_i}}{\prod_{j \in S} \sqrt{p_j}} \in \mathbb{Q}_0 = \mathbb{Q} \]

Where the product in the last relation is to be taken over some finite subset \( S \) of \( \{1, 2, \ldots, i - 1\} \). (As usual the empty product is the unity). The above relation contradicts either lemma 2) or lemma 3) and hence the theorem follows.

**Remarks:**

1. Using the conventions of the preceding proof we have \( \sqrt{p_i} \notin \mathbb{Q}_i \) for all \( i < n \). And more generally we have

\[ \sqrt{p_i} \notin \mathbb{Q} \left( \sqrt{p_1}, \ldots, \sqrt{p_j} \right) \]

where \( p_1, p_i, \ldots, p_j \) are any different primes. Here they are not necessarily subsequent primes.

2. We also conclude from the argument of the proof of the preceding theorem that the dimension of \( \mathbb{Q}_i \) over \( \mathbb{Q}_{i-1} \) is exactly two for every pair of such fields. This also extends to be: the dimension of \( \mathbb{Q}_n \) over \( \mathbb{Q} \) is \( 2^n \).

**Corollary 1** The square roots of any finite number of different primes are linearly independent over the rationals. Also, we have that: the square roots of any finite number of reciprocals of different primes are linearly independent over the rationals.

**Proof.**

Assume a relation \( a_1 \sqrt{p_1} + \cdots + a_n \sqrt{p_n} = 0 \) where \( p_i \) is the \( i \)th prime and the coefficients \( a_i \in \mathbb{Q} \) are not all zero. Since we have some non zero rationals we get \( \sqrt{p_i} \in \mathbb{Q}_i \) for some \( i < n \) which contradicts the first remark above. Similarly we get the case of the reciprocals.

In the same way, we have the following general result

**Corollary 2** If \( n_1, \ldots, n_k \) are different square free numbers then \( (\sqrt{n_1}, \ldots, \sqrt{n_k}) \) are linearly independent over the rationals; Also \((1/\sqrt{n_1}, \ldots, 1/\sqrt{n_k})\) are linearly independent over the rationals.
5 Algebraic Independence

**Definition 4** Complex numbers $a_1,\ldots,a_n$ are algebraically independent if $p(a_1,\ldots,a_n) \neq 0$ for all not identically zero polynomials $p$ in $\mathbb{Z}[x_1,\ldots,x_n]$.

5.1 Lindemann’s Theorem.

**Theorem 2** For any distinct algebraic numbers $\alpha_1,\ldots,\alpha_n$ and non zero algebraic numbers $\beta_1,\ldots,\beta_n$ we have

$$\beta_1 e_1^\alpha + \cdots + \beta_n e_n^\alpha \neq 0$$

**Corollary 3** If the algebraic numbers $\alpha_1,\ldots,\alpha_n$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1},\ldots,e^{\alpha_n}$ are algebraically independent.

For proof, see [Baker]. Applying Lindemann’s theorem to the results of the last section we get

**Corollary 4** If $p_1,\ldots,p_n$ are different square free natural numbers, then

$$e^{1/\sqrt{p_1}},\ldots,e^{1/\sqrt{p_n}}$$

are algebraically independent.

**Note.** We use the reciprocals of the radicals above and not the radicals themselves to fulfill the requirements of applying the uniformity conjecture i.e., to have the value of the exponent no more than 1 so that the resulting expressions are in expanded form.

**Theorem 3** (Using the uniformity conjecture). Suppose polynomial $p(x_1,\ldots,x_n)$ is represented by polynomial term $T(x_1,\ldots,x_n)$ with $s(T)$ nodes and logarithmic height $h(T)$. Then $p$ is the zero polynomial if and only if

$$|p(e^{p_1^{-1/2}},\ldots,e^{p_n^{-1/2}})| < 10^{-k}$$

where $k = 2 * s(T) * \max(h(T),n+1)$ and $p_1,\ldots,p_n$ are the first square free natural numbers $> 1$.

**Proof.**

By the remarks above, $e^{p_1^{-1/2}},\ldots,e^{p_n^{-1/2}}$ are algebraically independent. So $p$ is the zero polynomial if and only if $p(e^{p_1^{-1/2}},\ldots,e^{p_n^{-1/2}}) = 0$. 

10
According to the uniformity conjecture, $p(e^{P_{n^{1/2}}}, \ldots, e^{P_{n^{1/2}}}) = 0$ if and only if $|p(e^{P_{n^{1/2}}}, \ldots, e^{P_{n^{1/2}}})| < 10^{-\log_{10}(17)k}$, where $k$ is the length of the expression for $p(e^{P_{n^{1/2}}}, \ldots, e^{P_{n^{1/2}}})$.

There are $s(T)$ nodes in the tree for the polynomial $p(x_1, \ldots, x_n)$. In the corresponding tree for the constant which results from substitution, $p(e^{P_{n^{1/2}}}, \ldots, e^{P_{n^{1/2}}})$, the interior nodes contribute length 1 each, the frontier nodes with natural numbers on them contribute length at most $h(T)$ each, and the frontier nodes with exponentials on them contribute length at most $n+1$ each, since the first $n$ square free numbers all have length no more than $n$. (This follows from the Bertrand postulate, which states that the $n$th prime number is always below $2^n$. See [Zippel].)

6 Complexity of Approximation

Using the results mentioned in [Borwein, Borwein 1988], [Brent] we can get $e^{1/\sqrt{T}}$ to precision $n > \text{length}(p)$ decimal places in $O(M(n))$ bit operations, where $M(n)$ is the bit complexity of multiplying two $n$-digit natural numbers.

We have a bound of $B = 10^{s(T)h(T)}$ on the numbers which appear in the tree (See lemma 1.)

At each operation $+, *, -$ within the polynomial term we lose no more than $O(s(T)h(T))$ decimal places. To do one operation of multiplication for example, $xy$ to $k$ decimal places, we have

$$\|(x + \epsilon_1)(y + \epsilon_2) - xy\| < (\epsilon_1 + \epsilon_2)\max(|x|, |y|)$$

and therefore we would need $(\epsilon_1 + \epsilon_2)10^{s(T)h(T)} < 10^{-k}$.

It suffices, according to the above theorem, to finish the computation with precision $k = 2 \times s(T) \times \max(h(T), n + 1)$.

The precision needed for the whole computation is bounded by

$$2s(T)\max(h(T), n + 1) + O(s(T)(s(T)h(T))) = O(s(T)^2h(T))$$

Since we have $s(T)$ interior nodes (operations), the bit complexity of the computation is $O(s(T)M(s(T)^2h(T)))$.

**Theorem 4 (Assuming the uniformity conjecture).** Suppose a polynomial $p(x_1, \ldots, x_n)$ is represented by polynomial term $T(x_1, \ldots, x_n)$
with \( s(T) \) nodes and logarithmic height \( h(T) \). Then the bit complexity of deciding whether or not \( p \) is the zero polynomial is bounded by

\[
O \left( s(T) M(s(T)^2 \ h(T)) \right)
\]

### 7 Testing the Derivatives

We claim that we can also decide the zero equivalence of the derivatives in polynomial time using algebraically independent numbers and assuming the uniformity conjecture.

By definition of algebraically independent numbers, we can test whether a polynomial \( p(x_1, x_2, \ldots, x_n) \) is identically zero or not by substituting \( n \) algebraically independent numbers \( a_1, a_2, \ldots, a_n \) for the variables \( x_1, x_2, \ldots, x_n \). We can use the same idea to test the derivatives of \( p \) as well. For the rest of this subsection we assume \( p \in \mathbb{Z}[x, y_1, y_2, \ldots, y_n] \) and test the different derivatives with respect to \( x \). We prove this claim as follows.

1. \( Dxp \equiv 0 \) is equivalent to each of the following statements
   - \( p \) does not depend on \( x \).
   - \( (\forall x_1, x_2, y_1, \ldots, y_n) \quad p(x_1, y_1, \ldots, y_n) = p(x_2, y_1, \ldots, y_n) \)
   - \( p(x_1, y_1, \ldots, y_n) - p(x_2, y_1, \ldots, y_n) \equiv 0 \)
   - \( h(a_1, a_2, b_1, \ldots, b_n) = 0 \) where \( a_1, a_2, b_1, \ldots, b_n \) are algebraically independent.
   - \( p(a_1, b_1, \ldots, b_n) - p(a_2, b_1, \ldots, b_n) = 0 \) (in terms of \( p \))

2. \( D^2xp \equiv 0 \iff p \) linearly depends on \( x \) i.e., \( p = Ax + B \) where \( A, B \in \mathbb{Z}[y_1, \ldots, y_n] \).

\( \iff (\forall x_1, x_2, x_3; y_1, \ldots, y_n) (x_1, p_1), (x_2, p_2), (x_3, p_3) \) are collinear points

in the \( p \ vs. \ x \) plane where we mean by \( p_i \) the value \( p(x_i, y_1, \ldots, y_n) \).

From this collinearity we get the equivalent condition:

\[
\begin{vmatrix}
  p_1 & 1 & x_1 \\
  p_2 & 1 & x_2 \\
  p_3 & 1 & x_3 \\
\end{vmatrix} \equiv 0
\]

Treating the left hand determinant as a new polynomial \( h(x_1, x_2, x_3, y_1, \ldots, y_n) \) yields the analogous condition of the first derivative (case 1) in the form

\[
(a_2 - a_3)p_1 - (a_1 - a_3)p_2 + (a_1 - a_2)p_3 = 0
\]
where \( p_i := p(a_i, b_1, \ldots, b_n) \) and the numbers \( a_1, a_2, a_3, b_1, \ldots, b_n \) are algebraically independent.

3. Similarly \( D^2_p \equiv 0 \iff p \) quadratically depends on \( x \) which yields the following condition:

\[
\begin{pmatrix}
p_1 & 1 & a_1^2 \\
p_2 & 1 & a_2^2 \\
p_3 & 1 & a_3^2 \\
p_4 & 1 & a_4^2 \\
\end{pmatrix} = 0
\]

where \( p_i := p(a_i, b_1, \ldots, b_n); i = 1, 2, 3, 4 \) and \( a_1, \ldots, a_4, b_1, \ldots, b_n \) are algebraically independent numbers. Upon expanding using the entries of the first column we equivalently have

\[
p_1 v_1 - p_2 v_2 + p_3 v_3 - p_4 v_4 = 0
\]

where

\[
\begin{align*}
v_1 &= (a_4 - a_3)(a_4 - a_2)(a_3 - a_2) \\
v_2 &= (a_4 - a_3)(a_4 - a_1)(a_3 - a_1) \\
v_3 &= (a_4 - a_2)(a_4 - a_1)(a_2 - a_1) \\
v_4 &= (a_3 - a_2)(a_3 - a_1)(a_2 - a_1)
\end{align*}
\]

4. Now we can easily generalise the above result to the \( m^{th} \) derivative case as follows

\[
D^m_x p \equiv 0 \iff p_1 v_1 - p_2 v_2 + p_3 v_3 - \cdots + (-1)^m p_{m+1} v_{m+1} = 0
\]

where \( p_i := p(a_i, b_1, \ldots, b_n); i = 1, 2, \ldots, m+1 \) and \( a_1, \ldots, a_{m+1}, b_1, \ldots, b_n \) are as usual algebraically independent. The general form of \( v_i \) is given by

\[
v_i = \det(V(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{m+1})))
\]

Here, we used the expansion of the determinant of the Vandermonde matrix \( V(a_1, \ldots, a_{i-1}, a_{i+1}, a_{m+1}) \) as a product of differences. The underlined Vandermonde matrix is given below.

\[
\begin{pmatrix}
1 & a_1 & a_1^2 & a_1^3 & \cdots & a_1^{m-1} \\
1 & a_2 & a_2^2 & a_2^3 & \cdots & a_2^{m-1} \\
& \vdots & \ddots & \ddots & \ddots & \ddots \\
1 & a_{i-1} & a_{i-1}^2 & a_{i-1}^3 & \cdots & a_{i-1}^{m-1} \\
1 & a_{i+1} & a_{i+1}^2 & a_{i+1}^3 & \cdots & a_{i+1}^{m-1} \\
& \vdots & \ddots & \ddots & \ddots & \ddots \\
1 & a_{m+1} & a_{m+1}^2 & a_{m+1}^3 & \cdots & a_{m+1}^{m-1}
\end{pmatrix}
\]
For more details about the Vandermonde matrix and related things in computer algebra one may consult [Zippel].

**Corollary 5** If \( p \in \mathbb{Z}[x, y_1, \ldots, y_m] \) is represented as polynomial term \( T \) with \( s(T) \) nodes and \( h(T) \) height then we can decide whether the \( n \)th derivative with respect to \( x \) is zero in time polynomial in \( s(T), h(T) \) and \( n \).

This seems to depend on the the special form of the Vandermonde determinant, which allows a fairly compact representation as a term. We do not know whether or not any determinant with polynomial entries can be represented as a polynomial term with size bounded polynomially in the size of the determinant and the size of the entries. (It has been conjectured that this is not the case. See [Bürgisser].) We also do not know whether or not any polynomial term can be represented as a determinant with entries which are either natural numbers or variables in some compact way.

We can use the last corollary to determine the degree of \( x \) in \( T \) in polynomial time. This can be done using derivative testing until we get the first identically zero derivative.

Furthermore, we can compute the coefficients of \( T \) with respect to \( x \) as follows: Suppose \( T \) is polynomial term with degree \( n \) i.e., \( p = c_0 + c_1 x + \cdots + c_n x^n \) where the coefficients are polynomials (polynomial terms) in the other variables. We get the following system of equations by substituting \( 0, 1, \ldots, n \) for \( x \).

\[
\begin{align*}
T[x := 0] &= c_0 \\
T[x := 1] &= c_0 + c_1 1 + c_2 1^2 + \cdots + c_n 1^n \\
T[x := 2] &= c_0 + c_1 2 + c_2 2^2 + \cdots + c_n 2^n \\
&\vdots \\
T[x := n] &= c_0 + c_1 n + c_2 n^2 + \cdots + c_n n^n
\end{align*}
\]

In matrix form, we have

\[
A. (c_0, \ldots, c_n)^T = (T[x := 0], T[x := 1], \ldots, T[x := n])^T
\]

Where \( A \) is the matrix of coefficients in this system of equations given by \( a_{ij} := i^j ; i, j \geq 0 \) and \( 0^0 := 1 \). Clearly \( A \) is invertible (again it gives rise to a Vandermonde matrix) and hence

\[
(c_0, \ldots, c_n)^T = A^{-1}. (T[x := 0], \ldots, T[x := n])^T.
\]
8 The Class NC

The complexity class NC used poly-logarithmic time but allows polynomially many processors. We can show that our zero recognition algorithm for polynomial terms is in class NC. In order to do this we need to show that evaluation of terms can be done in parallel efficiently. This can be done as follows. Suppose given a large term $T$. Find a subterm $T_x$ whose size is more than a quarter the size of $T$ but no more than a half of the size of $T$. This can be done by starting at the root of $T$ and going down, always choosing the larger of two subtrees, while the size of the subtree exceeds half the size of $T$. Replace the subtree $T_x$ by indeterminant $x$; call the result $T(x)$. Construct terms $A$ and $B$ which are no bigger than $T(x)$ so that $T(x) = Ax + B$. Now evaluate $A, B, x$ in parallel and then compute $Ax + B$.

Let $p(n)$ be the number of processors needed for a problem of size $n$ and let $t(n)$ be the time. We have $p(n) \leq 3p(3n/4) + \sigma$ and $t(n) \leq t(3n/4) + \tau$ where $\sigma$ is the number of processors needed and $\tau$ is the time needed for the computation of $Ax + B$ from $A, x, B$. These inequalities imply that we can do the computation in poly logarithmic time with polynomially many processors.

9 Analysis of the Algorithm

What are the properties of $e^{1/\sqrt{n}}, \ldots, e^{1/\sqrt{n}}$ that were needed to apply this algorithm?

- calculating their $k$th digit can be done quickly in the sense of Borwein see [Borwein, Borwein 1988]. See, as well, [Brent].
- They are algebraically independent.
- We assumed also the Uniformity Conjecture. We can use a weaker version of the uniformity conjecture and still get a useful result.
For example, in Theorem 3, we need
\[ \left| p \left( e^{1/\sqrt{m}}, \ldots, e^{1/\sqrt{m}} \right) \right| < 10^{-k} \rightarrow p \left( e^{1/\sqrt{m}}, \ldots, e^{1/\sqrt{m}} \right) = 0. \]

We would still have a polynomial complexity test if we defined \( k \) to be any polynomial in \( s(T) \) and \( h(T) \).

We, thus, can use any list of numbers satisfying these properties to recognise zero polynomials. So either the zero recognition problem for polynomial terms can be solved in polynomial time, or there is no such list of numbers (which seems highly unlikely, even if we do not believe the uniformity conjecture).

### 9.1 Further Work

- What is a good lower bound for the value of a non singular determinant whose entries are \( \exp \)-\( \log \) expressions? Is the precision necessary to distinguish such a value from zero polynomial in the size of the determinant and the lengths of the entries? A more specific question: Does there exist a non singular matrix whose entries are \( \exp \)-\( \log \) expressions, but whose determinant is smaller in absolute value than \( 10^{-m} \), where \( m \) is the sum of the lengths of the entries of the matrix? (This is related to the question of whether or not the matching problem is in NC.)

- Consider

\[ \Gamma_n = \{ (x_1, \ldots, x_n) \in \mathbb{C}^n : \forall k \exists \text{polynomial term } T(x_1, \ldots, x_n) \]\n
with \( s(T) \) nodes and height \( h(T) \) so that
\[ T \neq 0 \text{ but } |T(x_1, \ldots, x_n)| < 10^{-k(s(T)h(T))} \]

Does \( \Gamma_n \) have measure 0?

Note that if \( (x_1, \ldots, x_n) \notin \Gamma_n \) and have decimal expansion which can be computed in polynomial time then they can be used to test zero equivalence of polynomial term.

### References


[BCSS] Blum,Cucker,Shub,Smale, Complexity and Real Computation, Springer.


