Electronic Notes in Theoretical Computer Science 66 No. 1 (2002)
URL: `http://www.elsevier.nl/locate/entcs/volume66.html` 14 pages

What can we do with a Solution?

Simon Langley[1]

School of Computer Science
University of the West of England
Bristol, UK

Daniel Richardson[2]

Department of Computer Science
University of Bath
Bath, UK

Abstract

If $S = 0$ is a system of n equations and unknowns over $\mathbb{C}$ and $S(\alpha) = 0$ to what extent can we compute with the point α? In particular, can we decide whether or not a polynomial expressions in the components of α with integral coefficients is zero? This question is considered for both algebraic and elementary systems of equations.

1 Introduction

In this article, a system of equations is of the form $S = 0$, where $S = (p_1, \ldots, p_n) : \mathbb{C}^n \rightarrow \mathbb{C}^n$, and each p_i is analytic. A solution to such a system is a point $\alpha \in \mathbb{C}^n$ so that $S(\alpha) = 0$. A Newton point is a point α^*, and an associated number $\epsilon > 0$ so that if X_0 is any point within distance ϵ of α^*, the Newton sequence defined by

$$X_{i+1} = X_i - J_S^{-1}(X_i)S(X_i)$$

where J_S is the Jacobian matrix of S, converges to a solution α, and has the property that $|X_i - \alpha| < 10^{-2^i}$. Thus the precision of the approximation to the solution doubles at each iteration. We can specify α^* and ϵ as intervals with rational endpoints.

[1] Email: `Simon.Langley@uwe.ac.uk`

[2] Email: `masdr@bath.ac.uk`

A great deal of effort is directed to finding such solutions. Suppose such an effort succeeds. What can we do then? Should we regard a solution found in this way as a terminal point of our mathematical and computational efforts, as a sort of output which is no longer part of mathematics? Alternatively, to what extent is it possible to add the coordinates of our defined solution to our mathematical vocabulary and to compute with them? This question has been somewhat neglected. A curious fact in this regard is that about half of computer scientists and mathematicians think this question is too easy for serious consideration, and almost all the others believe the question is far too difficult for serious consideration. It is peculiar how little is known about this basic problem.

Definition 1.1 *Let F be a family of systems of equations. The* constant problem *for F is the following: Given system of equations $S = 0$ in F, and a Newton point (α^*, ϵ) for a solution α of the system, and given $q \in Z[x_1, \ldots, x_n]$, decide whether or not $q = 0$ at the point α.*

What is the computational difficulty of this problem, depending on the form of F? Are these problems decidable? Do they have polynomial complexity? Are solutions feasible? Can such a problem be NP hard?

Here are some important special cases of the constant problem. In each case $S = (p_1, \ldots, p_n)$.

(i) The Elementary Case. Each $p_i \in \mathbb{Q}[x_1, e^{x_1}, \ldots, x_n, e^{x_n}]$.

(ii) The Algebraic Case. Each $p_i \in \mathbb{Q}[x_1, \ldots, x_n]$.

(iii) The Irreducible Algebraic Case. The algebraic case with $\langle p_1, \ldots, p_n \rangle$ an irreducible ideal.

(iv) The Univariate case. The algebraic case with each p_i univariate, and irreducible.

(v) The Closed Form Numbers. In this case q can be expressed explicitly in closed form using field operations, exp, log and radicals, starting with the natural numbers.

(vi) Nested Radical Expressions. In this case q can be expressed explicitly in closed form using field operations and radicals, starting with the natural numbers.

For example, to prove that $\sqrt{9 + 4\sqrt{2}} = 1 + 2\sqrt{2}$ define (α_1, α_2) to be the root of

$$x_1^2 - 2 = 0, \qquad x_2^2 - 9 - 4x_1 = 0 \tag{1}$$

satisfying $(\alpha_1, \alpha_2) \in [1.4, 1.5] \times [3.8, 3.9]$. Proving the identity correct is equivalent to showing $\alpha_2 - 2\alpha_1 - 1 = 0$.

2 Approaches to solutions of the constant problem

Suppose $S(\alpha) = 0$, (α^*, ϵ) is a Newton point and $\alpha \equiv (\alpha_1, \ldots, \alpha_n)$. We get a finitely generated field, $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. We wish to determine whether or not two expressions for numbers in this field are equivalent. There are two approaches.

2.1 Equality Catching

In this case we have some method for proving all equalities in $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, for example by reduction to a canonical form. We define a proper set of generators for a complex field F to be $(x_1, \ldots, x_k, y)$ so that $F = \mathbb{Q}(x_1, \ldots, x_k)[y]$, and $(x_1, \ldots, x_k)$ are algebraically independent over $\mathbb{Q}$, and y is algebraic and integral over $\mathbb{Q}(x_1, \ldots, x_k)$. A proper set of generators always exists for a finitely generated subfield of the complex numbers and defines a canonical form. In the algebraic case, we need to construct a primitive element. The elementary case is somewhat more complicated. One approach needs the Schanuel conjecture, as stated below.

Conjecture 2.1 (Schanuel) *If $x_1, \ldots, x_k$ are complex numbers linearly independent over $\mathbb{Q}$, then $\{x_1, e^{x_1}, \ldots, x_k, e^{x_k}\}$ contains at least k algebraically independent numbers.*

This conjecture was used by Wilkie and Macintyre [7] in their proof of the decidability of the theory of the ordered field of the reals with exponentiation. Independently, it was used by Richardson [9] to give an algorithm to decide the elementary constant problem.

Theorem 2.2 *If the Schanuel conjecture is true, then we can effectively construct a proper set of generators for the field generated by the coordinates of a given solution of an elementary system of equations.*

Sketch of proof

Let α be a solution of a nonsingular set of elementary equations. Put the system of equations defining $\alpha \in \mathbb{C}^n$ in the form:

$$S_{n-k} = 0, w_1 = e^{x_1}, \ldots, w_k = e^{x_k}$$

where S_{n-k} is a list of $n-k$ multivariate polynomials with integral coefficients and the Jacobian of the whole system is nonsingular at α. We can arrange (with some difficulty) that $\langle S_{n-k} \rangle$ is irreducible.

Near α in $\mathbb{C}^n$, $S_{n-k} = 0$ defines a set of dimension k. Let F_k be the field of rational functions with integral coefficients defined on this set (so that two functions are regarded as equal if they are equal on the set). We can construct a proper set of generators $(t_1, \ldots, t_k, y)$ for F_k, where $t_1, \ldots, t_k$ are coordinate variables, which can be regarded as independent parameters for the set, and y is algebraic and integral over $\mathbb{Z}[t_1, \ldots, t_k]$.

Let F_α be the field of rational functions evaluated at α. F_α is an image of F_k. We hope F_α and F_k are isomorphic. In this case we are done.

The Schanuel conjecture implies that if there are no integral linear relations among $x_1, \ldots, x_k$ at α then $(x_1, \ldots, x_k, w_1, \ldots, w_k)$ have transcendence rank at least k at α. Since the ideal generated by S_{n-k} is irreducible, this implies that F_α and F_k are isomorphic as required. Therefore the only possible difficulties are caused by integral linear relationships among the arguments of the exponential function at α.

Note that if $a_1x_1 + \cdots + a_kx_k = 0$ at α with $a_1, \ldots, a_k$ integral and not all zero, then this, together with the associated binomial condition $w_1^{a_1} \ldots w_k^{a_k} = 1$ can be used to eliminate one of the exponential conditions.

In general it seems to be necessary to consider the possibility that several independent linear relations hold at α. Suppose the rank of $(z_1, \ldots, z_k)$ over $\mathbb{Q}$ at α is $k - r$, where $r > 0$. Define a resolving matrix $R = (r_{ij})$ to be an r by k matrix of integers with rank r so that $R(z_1, \ldots, z_k)^T = 0$ at α

Some linear relations may hold even in F_k. We can detect these by putting $x_1, \ldots, x_k$ into canonical form with respect to our proper set of generators for F_k, which is after all a vector space over the rationals. For every such relation we can eliminate an exponential condition.

Without loss of generality therefore, we may suppose that $(x_1, \ldots, x_k)$ have rank k over $\mathbb{Q}$ in F_k. Suppose $D = (r_{ij})$ were a resolving matrix of rank r. Consider the $n - k + 2r$ conditions

$$\begin{aligned} S_{n-k} &= 0 \\ \sum r_{ij}x_j &= 0, i = 1, \ldots, r \\ \prod w_j^{r_{ij}} &= 1, i = 1, \ldots, r \end{aligned}$$

Near α these must define a set of dimension $k-r$. This fact allows us either to compute the integers r_{ij} or to show that there is no resolving matrix of rank r. The first step is to consider the set of associated differential conditions:

$$\begin{aligned} d(S_{n-k}) &= 0 \\ \sum r_{ij}d(x_j) &= 0, i = 1, \ldots, r \\ \sum r_{ij}d(w_j)/w_j &= 0, i = 1, \ldots, r \end{aligned}$$

which must have rank $n - k + r$, so that the last group of conditions must be a linear combination of the others.

The construction continues as in [10], where this was done for closed form numbers.

However, all these constructions (of primitive element in the algebraic case or proper set of generators in the elementary case) are infeasible as they stand, except for small problems. In all cases, the dimension of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ as a vector space may grow exponentially with n. Even in the case of radicals, the size of the canonical form may grow exponentially with the size of the problem.

There may be some way to apply a random simplifying transformation to $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, regarded as a vector space, and then to work in the image but at the moment we do not see how to do this.

2.2 Inequality Catching

The idea in this case is to try to prove all the inequalities. One approach (based on [10,11]) is to try to find a gap function, that is, a function g which maps the syntactic objects which constitute definitions of numbers into nonnegative reals, bounding the smallness of the number defined if it is non-zero. For a certain class of definitions, we will say that g is an logarithmic gap function for q if

$$q \neq 0 \rightarrow |\log_2(|q|)| < g(\text{length}(q))$$

In the closed form cases q is the expression itself and the length is the number of characters of the defining expression. In the elementary and the three algebraic cases, its length the sum of the length in bits needed to represent the equations, q itself and the Newton point (α^*, ϵ).

A logarithmic gap function gives the number of bits needed to distinguish q from zero. Thus it is a reasonable measure of the amount of computation needed to recognise zero, or, in the real case, to determine sign.

This approach is not sufficient in itself to solve the algebraic problem in polynomial time. For example, consider the equations $2x_1 - 1 = 0, x_2 - x_1^2 = 0, \ldots, x_n - x_{n-1}^2 = 0$. This has $x_n = (1/2)^{2^n}$ in its unique solution.

For the irreducible algebraic case an effective version of Hilbert's Nullstellensatz (see [3]) can be used to give a logarithmic gap function which increases exponentially with n. In the univariate case, Liouville's theorem can be used [13, p83] and for expressions in radicals see [1] or [6].

In the remainder of the paper we derive a gap function for the general algebraic case and discuss a promising conjecture for the closed form number case.

3 The Algebraic Case using the Dixon resultant

We suppose that $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ is a zero of a system S of n multivariate polynomials and further that $J_S(\alpha)$ is non-singular. Let $\mathcal{E} = q(\alpha)$, and suppose that this is not zero.

The Dixon resultant (see e.g. [5,4]) is a multivariate generalisation of the Bezoutian (it is sometimes called the multivariate Bezoutian). We will show that it can be manipulated to yield a matrix whose determinant evaluates to a polynomial with roots including all values of $1/\mathcal{E}$, arising from conjugates of α. From an upper bound of the roots of the polynomial, a lower bound for $|\mathcal{E}|$ is found.

Since we are interested in finding a lower bound for $|\mathcal{E}|$ rather than a specific value, we will first estimate root bounds from the matrix, the final step is to estimate the matrix parameters from the heights and degrees of the input polynomials.

3.1 The Multivariate Dixon Resultant

Our initial system of equations is $S = (p_1, \ldots, p_n)$ (each $p_i \in \mathbb{Z}[x_1, \ldots, x_n]$). We wish to decide whether or not $q(\alpha) = 0$. Let $p_{n+1} = 1 - zq$, and $P = (p_1, \ldots, p_{n+1})$.

The starting point is to consider polynomials in $\mathbb{Z}[z][x_1, \ldots, x_n, y_1, \ldots, y_n]$. We will use x for $(x_1, \ldots, x_n)$, and y for $(y_1, \ldots, y_n)$.

Definition 3.1 *For $p(z, x) \in \mathbb{Z}[z][x_1, \ldots, x_n]$ and $0 \leq a \leq n$ define $p^{(a)} := p(y_1, \ldots, y_a, x_{a+1}, \ldots, x_n)$. The* Dixon polynomial *of $p_1, \ldots, p_{n+1}$ is*

$$\mathcal{D}(z, x, y) \equiv \frac{1}{\prod\limits_{1 \leq i \leq n} (x_i - y_i)} \begin{vmatrix} p_1^{(0)} & p_1^{(1)} & \cdots & \cdots & p_1^{(n)} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{n+1}^{(0)} & p_{n+1}^{(1)} & \cdots & \cdots & p_{n+1}^{(n)} \end{vmatrix} \tag{2}$$

It is easily seen that $\mathcal{D}(z, x, y)$ is indeed a polynomial since substituting y_i for x_i within the determinant causes it to vanish (two adjacent columns become identical). Further, if $P(z^*, \alpha) = 0$ then $\mathcal{D}(z^*, \alpha, y) = 0$ independently of the values of the y_i.

$\mathcal{D}(z, x, y)$ can be written in polynomial or matrix form as

$$\mathcal{D}(z, x, y) = \sum_{\alpha, \beta \in \mathbb{Z}^n} c_{\alpha,\beta} \mathbf{x}^\beta \mathbf{y}^\alpha = X^T \mathcal{M}(z) Y$$

where $\mathbf{y}^\alpha \equiv \prod_{1 \leq i \leq n} y_i^{\alpha_i}$, $\mathbf{x}^\beta \equiv \prod_{1 \leq i \leq n} x_i^{\beta_i}$ and X (Y) is a vector of the monomials $\mathbf{x}^\beta$ $(\mathbf{y}^\alpha)$ appearing in $\mathcal{D}(z, x, y)$.

3.2 Applying the Dixon Resultant

Consider the Dixon polynomial obtained from P.

$$\begin{aligned} \mathcal{D}_P(z, x, y) &= \frac{1}{\prod\limits_{1 \leq i \leq n} (x_i - y_i)} \begin{vmatrix} p_1^{(0)} & p_1^{(1)} & \cdots & p_1^{(n)} \\ \cdots & \cdots & \cdots & \cdots \\ p_n^{(0)} & p_n^{(1)} & \cdots & p_n^{(n)} \\ 1 - zq^{(0)} & 1 - zq^{(1)} & \cdots & 1 - zq^{(n)} \end{vmatrix} \\ &= X^T \mathcal{M}_P(z) Y \end{aligned}$$

In the sequel $X(\alpha)$ will be the vector X evaluated at α and similarly for $Y(\alpha)$. The dimensions of $\mathcal{M}_P(z)$ will be $N_r \times N_c$. Thus the number of monomials in X is N_r, and the number of monomials in Y is N_c.

The standard resultant argument would be that if $X(\alpha)^T\mathcal{M}_P(1/q(\alpha)Y = 0$ but $q(\alpha) \neq 0$ then $\det(\mathcal{M}_P(z))$ has among its roots the value of $q(\alpha)$. Unfortunately $\mathcal{M}_P(z)$ is not necessarily square and so may have no determinant. Even when it is square, the determinant is often identically zero and so a more indirect approach is needed.

We will show that there exists a sub-matrix $H(z)$ of $\mathcal{M}_P(z)$ so that $H(z)$ is non singular for generic z, but is singular if $q(\alpha) \neq 0$ and $z = 1/q(\alpha)$. By finding a bound for $|H_{ij}|$ we produce an upper bound for $|1/q(\alpha)|$ and so a lower bound for $|q(\alpha)|$. Specifically, since H is a sub-matrix of $\mathcal{M}_P(z)$ we shall show:

Proposition 3.2 *If $N = \min(N_r, N_c)$ and $h = \max_{i,j}(|\mathcal{M}_P(z)|)$ (where $|a + bz| \equiv \max(|a|, |b|)$) then $q(\alpha) \neq 0$ implies*

$$|q(\alpha)| \geq \frac{1}{1 + (h\sqrt{N})^N}$$

Definition 3.3 *We call a sub-matrix, $\mathcal{H}$ of $\mathcal{M}_P(z)$* maximal *if it is square and its determinant does not vanish identically (i.e. for all z) but that of any square sub-matrix of $\mathcal{M}_P(z)$ containing $\mathcal{H}$ does vanish.*

Proposition 3.4 *Let $\mathcal{H}(z)$ be any maximal sub-matrix of $\mathcal{M}_P(z)$. If $q(\alpha) \neq 0$ then $\det(\mathcal{H}(1/q(\alpha))) = 0$.*

Two preliminary result are required to prove the proposition.

Lemma 3.5 *If $S(\alpha) = 0$ then $X(\alpha)^T\mathcal{M}_P(z)Y = (1 - zq(\alpha))B(Y)$ and $X^T\mathcal{M}_P(z)Y(\alpha)) = (1 - zq(\alpha))B'(X)$, where B and B' are linear in Y and X respectively, with coefficients which are polynomials in α also $B(Y(\alpha)) = B'(X(\alpha)) = \det(J_S(\alpha))$.*

Proof. Since $p_i(\alpha) = 0, 1 \leq i \leq n$

$$\begin{aligned}
\mathcal{D}_S(z, \alpha, y) &= \frac{1}{\prod\limits_{1\leq i\leq n}(\alpha_i - y_i)} \begin{vmatrix} 0 & p_1^{(1)}(\alpha) \ldots & p_1^{(n)}(\alpha) \\ 0 & \ldots \quad \ldots & \ldots \\ 0 & p_n^{(1)}(\alpha) \ldots & p_n^{(n)}(\alpha) \\ 1 - zq(\alpha) & \ldots \quad \ldots & \ldots \end{vmatrix} \\
&= (-1)^n \frac{(1 - zq(\alpha))}{\prod\limits_{1\leq i\leq n}(a_i - y_i)} \begin{vmatrix} p_1^{(1)}(\alpha) \ldots & p_1^{(n)}(\alpha) \\ \ldots \quad \ldots & \ldots \\ p_n^{(1)}(\alpha) \ldots & p_n^{(n)}(\alpha) \end{vmatrix} \\
&= (1 - zq(\alpha))B(Y)
\end{aligned}$$

$\mathcal{D}_S(z, \alpha, y) \equiv X(\alpha)^T \mathcal{M}_P(z)Y$. $B(Y)$ is linear in Y with coefficients which are polynomials in α. For the second part, subtracting adjacent columns and writing $\Delta_k p$ for $(p^{(k)} - p^{(k-1)})/(x_k - y_k)$.

$$B(Y) = (-1)^n \begin{vmatrix} \Delta_1 p_1 & \dots & \Delta_n p_1 \\ \dots & \dots & \dots \\ \Delta_1 p_n & \dots & \Delta_n p_n \end{vmatrix}$$

(since $p_i^{(0)}(\alpha) = 0$) but

$$\lim_{\substack{y_i \to a_i \\ 1 \leq i \leq n}} \Delta_j p = \frac{p^{(j)} - p^{(j-1)}}{\alpha_j - y_j} = -\partial p / \partial x_j \mid_\alpha \quad \text{so}$$

$$\lim_{\substack{y_i \to a_i \\ 1 \leq i \leq n}} B(Y) = \det(J_S(\alpha))$$

Exchanging the roles of x and y, the same argument gives $X^T \mathcal{M}_P(z) Y(\alpha)) = (1 - zq(\alpha))B'(X)$. □

Since $J_S(\alpha) \neq 0$ it follows that $\mathcal{D}_S(z^*, \alpha; \alpha) = 0$ iff $z^* = 1/q(\alpha)$.

Lemma 3.6 *Assume $q(\alpha) \neq 0$. The rank of $\mathcal{M}_P(z)$ at $z^* = 1/q(\alpha)$ is at least 1 less than at generic z.*

Proof.

Let $V = (V_1, \dots V_{N_c})$ be an $N_c \times N_c$ matrix with columns $V_1 = Y(\alpha)$ and $V_2, \dots, V_{N_c}$ a basis spanning the space $\Gamma = \{a \in C^{N_c} \mid B(a) = 0\}$. Since B is not identically zero and is linear in a such a basis exists and has dimension $N_c - 1$. Further V_1 is linearly independent of $V_2, \dots, V_{N_c}$ since otherwise we should have $V_1 = Y(\alpha) = \sum_{2 \leq i \leq N_c} c_i V_i$ for some c_i not all zero implying

$$J_S(\alpha) = B(Y(\alpha)) = B(\sum_{2 \leq i \leq N_c} c_i V_i) = \sum_{2 \leq i \leq N_c} c_i B(V_i) = 0$$

contradicting Lemma 3.5. Thus V is non-singular (and independent of z).

Let $U = (U_1, \dots U_{N_r})$ be an $N_r \times N_r$ matrix with $U_1 = X(\alpha)$ with $U_2, \dots, U_{N_r}$ constructed in the same way as the V_i but this time spanning $\Gamma' = \{a \in C^{N_r} \mid B'(a) = 0\}$. U is non singular and independent of z.

Consider the matrix $\mathcal{M}^* = U^T \mathcal{M}_P V$ and let $\{u_i\}$ be the standard basis for $\mathbb{C}^{N_r}$ and $\{v_i\}$ that for $\mathbb{C}^{N_c}$. We have

$$u_i^T U^T \mathcal{M}_P V v_j = U_i^T \mathcal{M}_\mathcal{A} V_j = u_i^T \mathcal{M}^* v_j = \mathcal{M}^*_{i,j}(z)$$

By construction

$$\begin{aligned}\mathcal{M}^*_{1j} &= U_1^T\mathcal{M}_P V_j = X(\alpha)^T\mathcal{M}_P V_j\\ &= (1 - zq(\alpha))B(V_j)\\ &= (1 - zq(\alpha))\det(J_S(\alpha)) \ \text{ if } j = 1 \text{ and } 0 \text{ otherwise}\end{aligned}$$

and so the first row of $\mathcal{M}^*(z)$ is zero apart from the first element. By the same argument $\mathcal{M}^*_{i1} = 0$ if $i \neq 1$, and so the first column is zero except for the first element.

The rank of $\mathcal{M}^*(z)$ is the same as that of $\mathcal{M}_P(z)$, since they are related by non-singular transformations.

All the entries of $\mathcal{M}^*(z)$ depend continuously on z. We suppose $q(\alpha) \neq 0$. Consider the point $z = 1/q(\alpha)$. Suppose the rank of $\mathcal{M}$ at this point is r. This means that there is an r by r non singular sub-matrix, which does not include any entries from the first row or first column, since these are all zero at the point. If z is moved slightly, this sub-matrix will still be non singular, but by appending appropriate entries from the first row and first column, a larger non singular sub-matrix can be constructed.

Thus any maximal sub-matrix of $\mathcal{M}^*(z)$ includes $\mathcal{M}^*_{11}$ (since if it didn't we could append it and the appropriate entries from row/column 1 to get a larger sub-matrix.)

At $z = 1/q(\alpha)$ the first row and column of $\mathcal{M}^*(z)$ become zero and thus its rank, and consequently that of $\mathcal{M}_P(z)$, drops by at least one. □

This proves Prop. 3.4 since the last lemma implies that the rank of any maximal sub-matrix will drop at $z^* = 1/q(\alpha)$.

Proof. (Proof of Prop. 3.2) For any z, $\mathcal{M}_P$ has rank no greater than $N = \min(N_r, N_c)$. Thus a maximal sub-matrix $\mathcal{H}$ has rank at most N.

Expanding $\det(\mathcal{H})$ gives a polynomial in z, $\chi(z) \equiv \sum_{0\leq i\leq N} a_i z^i$ with $|a_i| \leq N^{N/2}h^N$ (using Hadamard's bound). Applying a standard bound on absolute value of polynomial roots gives $|z| < 1 + N^{N/2}h^N$ so $q(\alpha) \neq 0$ implies

$$|q(\alpha)| \geq \frac{1}{1 + (h\sqrt{N})^N} \tag{3}$$

□

Unfortunate Corollary: $\chi(z) = 0$ whenever $z = 1/q(\alpha)$ and α is a nonsingular solution of $S = 0$. Thus the degree of χ and also the number N is as large as the number of distinct values $q(\alpha) \neq 0$ such that α is a non singular solution of $S = 0$.

As an example, Eq. (1) gives a resultant

$$\begin{aligned}&9zx_1 + (1-z)x_2x_1 + (1-z)x_1y_2 + 4zx_1y_1 + zx_1x_2y_2 - 2zx_1x_2y_1\\ &-2zx_1y_1y_2 + 8z - 4zx_2 - 4zy_2 + 9zy_1 + (1-z)x_2y_1 + (1-z)y_1y_2 + zx_2y_1y_2\end{aligned}$$

giving $h = 9$, $N_r = N_c = 4$ and a lower bound of $\approx 0.9 \times 10^{-5}$ (a bound within reach of hardware floating point arithmetic but not impressive considering the true lower bound is ≈ 3.7).

3.3 A Lower Bound from Input Parameters

One of the advantages of the Dixon resultant is that its size is often considerably less than its theoretical maximum. If, however, worst case behaviour is assumed a lower bound can be found by finding upper bounds for N and h directly from the heights and degrees of $<p_1, \ldots, p_n, q>$. This gives, of course, a worse estimate but does obviate the need to compute the resultant.

The following terms are used in what follows:

- $P \equiv \{p_1, \ldots, p_n, p_{n+1} = 1 - zq\}, p_i \in \mathbb{Z}[z][x_1, \ldots, x_n]$
- $d_i \equiv$ the largest exponent of x_i in P, $D \equiv \prod_{1 \le i \le n} d_i$
- $t_i \equiv$ the number of distinct monomials in p_i, $T \equiv \prod_{1 \le i \le n+1} t_i$
- For $p \equiv \sum_{\alpha,\beta \in \mathbb{Z}^n} c_{\alpha,\beta} \mathbf{x}^\beta \mathbf{y}^\alpha$, $\|p\| \equiv \max(|c_{\alpha,\beta}|)$ where $|a + bz| \equiv \max(|a|, |b|)$
- $H \equiv \prod_{1 \le i \le n+1} \|p_i\|$

Proposition 3.7 *i) $N \le n!D$ and ii) $h \le (n+1)!HT$*

Proof. i) In Eq. (2), x_i appears in the first i columns of the determinant and so its expansion contains no monomial with a power of x_i greater than $\delta_i = id_i$ (a better bound would be to define δ_i as the sum of the i highest powers of x_i appearing in the different polynomials). Dividing the determinant by $(x_i - y_i)$ reduces the degree by one and so the Dixon polynomial can include only monomials $\prod_{1 \le i \le n} x_i^{a_i}$ in the x_i with $a_i < \delta_i$. There are $\prod_{1 \le i \le n} \delta_i$ such monomials and so $N \le n! \prod_{1 \le i \le n} d_i$.
ii) Write $p_1 = cm + r$ where m is an arbitrarily chosen monomial in p_1, c is its coefficient and r the rest of p_1. The determinant in Eq. (2) can be written

$$c \begin{vmatrix} m & m^{(1)} & \ldots & \ldots & m^{(n)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{n+1}^{(0)} & p_{n+1}^{(1)} & \ldots & \ldots & p_{n+1}^{(n)} \end{vmatrix} + \begin{vmatrix} r & r^{(1)} & \ldots & \ldots & r^{(n)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{n+1}^{(0)} & p_{n+1}^{(1)} & \ldots & \ldots & p_{n+1}^{(n)} \end{vmatrix}$$

Repeating this process for r and then for subsequent rows, the Dixon Polynomial can be written as

$$D_S = \frac{1}{\prod\limits_{1 \le i \le n} (x_i - y_i)} \sum_{1 \le i \le T} h_i D_i$$

where each h_i is a product of $n + 1$ coefficients taken from the polynomials (i.e. $\prod |h_i| \le H$) and the D_i are determinants following the Dixon pattern but with each entry a single monomial. If D is one of the D_i

$$\frac{D}{\prod\limits_{1\le i\le n}(x_i-y_i)} = \begin{vmatrix} m_1^{(0)} & \Delta_1 m_1 & \ldots\ \ldots & \Delta_n m_1 \\ \ldots & \ldots & \ldots\ \ldots & \ldots \\ m_{n+1}^{(0)} & \Delta_1 m_{n+1} & \ldots\ \ldots & \Delta_n m_{n+1} \end{vmatrix}$$

Now $\Delta_i m = m'(x_i^d - y_i^d)/(x_i - y_i)$ for some $d \le d_i$ where m' is a monomial in $y_1, \ldots, y_{i-1}, x_{i+1}, \ldots, x_n$. $(x_i^d - y_i^d)/(x_i - y_i) = \sum_{j+k=d-1} x_i^j y_i^k$ and so has at most d_i terms.

To determine the height we claim that at most $(n+1)!$ monomials in the expansion can be identical. If $n = 1$ we have a 2×2 determinant and the result is clearly true: each of the two powers of x_1 in the first column can be multiplied by one term in column 2. If it is true for $k-1$ variables then in the k variable case, y_k appears only in column $k+1$ and could appear to the same power in each of the rows. To obtain identical monomials we take equal powers of y_k and expand with respect to column $k+1$. Each of the minors is a version of the $k-1$ size case (except for a factor which is a power of x_k) and the result is proved by induction.

Combining these results, we conclude the height of the Dixon polynomial is $h \le (n+1)!HT$

For the example above this gives $N \le 8$ or $N \le 6$ (using the better bound) and $h \le 3888$ (the true value being 9). With these, the lower bound for the example becomes $\approx 0.4 \times 10^{-32}$.

3.4 What goes wrong?

The complexity of the Dixon method is controlled by N. This is expected to be as large as the Bezout number, since N is also an upper bound for the degree of the polynomial which must have one root for each value $q(\alpha) \ne 0$ where α is any non singular solution of our system.

4 The Uniformity Conjecture

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

(i) $m \in \mathbb{E}$ if m is a representation of a natural number.

(ii) If $u, v \in \mathbb{E}$ so are $(u+v)$, $(u-v)$, and $(u*v)$, (u/v).

(iii) If $u \in \mathbb{E}$ so are $-u$, $\exp(u)$ and $\log(u)$

(iv) If $u \in \mathbb{E}$ and n is a canonical representation of a natural number bigger than 1, then $\sqrt[n]{u} \in \mathbb{E}$. (Note that n^{th} powers with $n > 1$ are not allowed.)

We write $\mathcal{V}(a)$ for the value of an expression a, assuming it is defined, with the proviso that $\mathcal{V}(\log(a))$ is the branch of the function with $-\pi < \mathrm{Im}(\mathcal{V}(\log(a))) \leq \pi$ and $\mathcal{V}(\sqrt[n]{a}) \equiv \mathcal{V}(\exp(\log(a)/n))$

The complex numbers defined in this way are called *closed form* [2].

4.1 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.

We may view expressions as trees with natural numbers at the leaves and operators at the interior nodes. We define the *length* of a nested radical exponential and logarithmic expression to be the sum of the number of interior nodes and the sum of the lengths of the leaves.

For example, in decimal notation, $4 - 3 * (10)^{1/8}$ would have length 8, since it has 5 digits and 3 operator symbols. In general, the length counts the number of operators and the number of digits used.

4.2 The 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. There does not seem to be any other way to get very small non zero numbers.

We will say that an expression a is in expanded form if for any exponential subexpression $\exp(b)$ of a, we have $|\mathcal{V}(b)| \leq 1$. (a is considered a subexpression of itself.)

It appears that it is not possible to define very small non zero numbers using short expressions in expanded form. This somewhat vague idea led to the original statement of the uniformity conjecture, as given below. See [11] (which uses a slightly different definition of length).

Conjecture 4.1 (Uniformity Conjecture) *If $a \in \mathbb{E}$ is in expanded form, and $\mathcal{V}(a) \neq 0$, then $|\mathcal{V}(a)| > 1/N(k)$, where $k = \mathrm{length}(a)$ and $N(k)$ is the number of syntactically correct expanded form expressions of length $\leq k$.*

The number of expressions of length $\leq k$ is bounded by the number of sequences of length k, including sequences which do not represent expressions. Therefore, if we have Σ symbols for operators and digits in our alphabet, the number of syntactically correct expressions of length $\leq k$ is bounded by Σ^k. In case we use decimal notation, for example, Σ would be 17. In binary notation, Σ would be 9.

Assuming decimal notation, $10^k < N(k) < 10^{1.24k}$. Suppose $k > 4$. Consider a string of symbols of length k with digits on the ends, and digits at all the odd numbered positions and either digits or operators $+, -, *, /$ at interior even numbered positions. There are 14 choices for symbols at these interior even numbered positions, and 10 choices for the others. Any such string is syntactically correct. So, assuming $k > 4$, we get $10^{1.04k} < N(k) < 10^{1.24k}$.

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

There is some empirical evidence that this conjecture is true. See [8] and [12]. It is clear that this conjecture makes the constant problem for radicals look rather easy; whereas from the point of view of the effective Nullstellensatz, it looks intractable.

5 Conclusion

The conclusions are quite negative. We do not know whether or not the Schanuel conjecture is true. We do not know whether or not the elementary constant problem is decidable. We expect that it is decidable, and even easily decidable, since there are no known seriously difficult examples.

We do not have any practical solution for the algebraic constant problem. We do not know the theoretical complexity of this basic problem. Direct application of methods based on the Nullstellensatz or methods based on multivariate resultants always gives logarithmic gap functions which increase exponentially with size of problem. The complexity of these constructions always involve the Bezout number. This is because most of the construction is valid for all possible solutions, not just for the one in which we are interested.

On the practical level, however, for closed form numbers the uniformity conjecture does give a way to proceed.

In general, solutions of systems of equations may have very small coordinates which are not zero. This means that we can not solve all of these problems in realistic time via approximation up to some limit defined by a gap function. But this does not in itself imply that the constant problem is essentially difficult. Some new ideas are needed to solve this problem. It may be that progress can be made by applying some simplifying transformation, such as, for example, working in the algebraic closure of a finite field.

References

[1] C Burnikel, R Fleischer, K Melhorn, and S Schirra. A strong and easily computable separation bound for arithmetic expressions involving radicals. *Algorithmica*, 27:87–99, 2000.

[2] T. Y. Chow. What is a closed-form number? *American Mathematical Monthly*, 106(5):440–448, 1999.

[3] T Krick, L Pardo, and M Sombra. Sharp Estimates for the Arithmetic Nullstellensatz. *Archive at Southampton University*, 1999.

[4] D Kapur and T Saxena. Comparison of Various Multivariate Formulations. In *Proc. 1995 Int. Symp. on Symbolic and Algebraic Computation.* ACM Press, 1995.

[5] D Kapur, T Saxena, and L Yang. Algebraic and Geometric Reasoning using Dixon Resultants. In *Proc. 1994 Int. Symp. on Symbolic and Algebraic Computation*, pages 99–107. ACM Press, 1994.

[6] Chen Li. *Exact Geometric Computation.* PhD thesis, New York University, 2001.

[7] A Macintyre and A J Wilkie. *On the Decidability of the Real Exponential Field*, pages 441–467. A K Peters, 1996.

[8] D Richardson. Testing the uniformity conjecture. Submitted for publication, available from `www.bath.ac.uk/~masdr/testu.dvi`.

[9] D Richardson. How to Recognise Zero. *J. Symbolic Computation*, 24(6):627–645, 1997.

[10] D Richardson. Multiplicative independence of algebraic numbers and expressions. In *Mega2000 conference, Bath*, June 2000. also in Journal of Pure and Applied Algebra 164, 2001, pp 231-245, ISSN 0022-4049.

[11] D Richardson. The uniformity conjecture. In *Proceedings of Computability and Complexity in Analysis 2000*, pages 253–272. Springer lecture notes in Computer Science, Volume 2064, 2000.

[12] D Richardson and S Langley. Some observations on familiar numbers. Presented at ISSAC 2002, 2002.

[13] M Waldschmidt. *Diophantine approximation on linear algebraic groups.* Number 326 in Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 2000.