If a Polynomial Mapping Is Rectifiable, then the Rectifying Polynomial Automorphism Can Be Algorithmically Computed

Julio Urenda\textsuperscript{1,2}, David Finston\textsuperscript{1}, and Vladik Kreinovich\textsuperscript{3}
\textsuperscript{1}Department of Mathematical Sciences
New Mexico State University, Las Cruces, NM 88003, USA
jcurenda@utep.edu, dfinston@nmsu.edu
\textsuperscript{2}Department of Mathematical Sciences
\textsuperscript{3}Department of Computer Science
University of Texas at El Paso
El Paso, TX 79968, USA, vladik@utep.edu
1. Formulation of the Problem

- Let $\mathbb{C}$ denote the field of all complex numbers.
- A polynomial mapping $\alpha : \mathbb{C}^n \rightarrow \mathbb{C}^n$ is called a polynomial automorphism if:
  - this mapping a bijection, and
  - the inverse mapping $\beta = \alpha^{-1}$ is also polynomial.
- A polynomial mapping $\varphi : \mathbb{C}^k \rightarrow \mathbb{C}^n$ is called rectifiable if:
  - these exists a polynomial automorphism $\alpha : \mathbb{C}^n \rightarrow \mathbb{C}^n$
  - for which $\alpha(\varphi(t_1, \ldots, t_k)) = (t_1, \ldots, t_k, 0, \ldots)$ for all $(t_1, \ldots, t_k)$.
- Most existing proofs of rectifiability just prove the existence of a rectifying automorphism $\alpha$.
- In this talk, we show how to compute $\alpha$. 
2. Definitions

• We will formulate two versions of the main result:
  – for the case when the coefficients of the original polynomial mapping are algebraic numbers, and
  – for the general case, when these coefficients are not necessarily algebraic.

• A number is called *algebraic* if this number is a root of a non-zero polynomial with integer coefficients.

• In the computer, an algebraic real number can be represented by:
  – the integer coefficients of the corresponding polynomial and
  – by a rational-valued interval that contains only this root.

• Once this information is given, we can compute the corresponding root with any given accuracy.
3. First Result

• Lemma.  
  – If a polynomial mapping \( \varphi \) with algebraic coefficients is rectifiable,
  – then there exists a rectifying polynomial automorphism \( \alpha \) with algebraic coefficients.

• Proposition. There exists an algorithm that:
  – given a rectifiable polynomial mapping \( \varphi \) with algebraic coefficients,
  – computes the coefficients of a polynomial automorphism \( \alpha \) that rectifies \( \varphi \).
4. Need for a General Case

- In general, the coefficients of the original mapping $\varphi$ are not necessarily algebraic.
- These coefficients may not even be computable.
- It is desirable to extend this algorithm to this general case.
- When the coefficients are not necessarily computable, we cannot represent them in a computer.
- So, we need to extend the usual notion of an algorithm to cover this case.
5. Definitions

- By a *generalized algorithm*, we mean a sequence of the following elementary operations with real numbers:
  - adding, subtracting, multiplying, and dividing numbers;
  - checking whether a number is equal to 0, whether it is positive, and whether it is negative;
  - given the coefficients of a polynomial that has a root, returning one of the roots.

- Of course, when the real numbers are algebraic, these operations are algorithmically computable.
6. Second Result

• **Proposition.** There exists a generalized algorithm that:
  
  – given the coefficients of a rectifiable polynomial mapping \( \varphi \),
  
  – computes the coefficients of a polynomial automorphism \( \alpha \) that rectifies \( \varphi \).

• This shows that:
  
  – if a polynomial mapping is rectifiable,
  
  – then the corresponding rectification can be algorithmically computed.
7. Discussion

- Our proof uses the Tarski algorithm.
- As the length $\ell$ of the formula increases, the running time of this algorithm grows faster than $2^{2\ell}$.
- Thus, from the application viewpoint, it is desirable to come up with a faster algorithm.
- For some important cases, such faster algorithms were also proposed.
- These faster algorithms can be applied to other fields (and rings) as well.
- They are described in J. Urenda’s NMSU PhD dissertation *Algorithmic Aspects of the Embedding Problem*. 
8. Tarski-Seidenberg Algorithm: Reminder

- This algorithm deals with the \textit{first-order theory of real numbers}: follows:
  - we start with real-valued variables $x_1, \ldots, x_n$;
  - \textit{elementary formulas:} $P = 0$, $P > 0$, or $P \geq 0$, where $P$ is a polynomial with integer coefficients;
  - a general formula can be obtained from elementary formulas by using:
    - \textbf{logical connectives} (“and” \&, “or” $\lor$, “implies” $\rightarrow$, and “not” $\neg$) and
    - \textbf{quantifiers} over real numbers ($\forall x_i$ and $\exists x_i$).
- Example: every quadratic polynomial with non-negative determinant has a solution:
  $\forall a \forall b \forall c ((b^2 - 4a \cdot c \geq 0) \rightarrow \exists x (a \cdot x^2 + b \cdot x + c = 0))$. 
9. Tarski-Seidenberg Algorithm (cont-d)

- Tarski designed an algorithm that:
  - given a formula from this theory,
  - returns 0 or 1 depending on whether this formula is true or not.

- Seidenberg used a similar construction to
  - reduce each first-order formula with free variables
  - to a quantifier-free form.

- It follows that if a formula with free variables has a solution, then it also has an algebraic solution.
10. Proof of Lemma

- Let \( d \) be the largest degree of polynomials \( \alpha_i \) and \( \beta_i \) forming the mappings \( \alpha \) and \( \beta = \alpha^{-1} \).
- Each of these polynomial can be described by listing real and imaginary values of all its coefficients.
- The condition that \( \alpha \) and \( \beta \) are inverse to each other means that \( \forall z_1 \ldots \forall z_n (\&_i \alpha_i(\beta(z_1, \ldots, z_n)) = z_i) \) and \( \forall z_1 \ldots \forall z_n (\&_j \beta_j(\alpha(z_1, \ldots, z_n)) = z_j) \).
- Substituting the expressions for \( \alpha \) and \( \beta \) in terms of their coefficients, we get a first order formula.
- Similarly, the condition that \( \alpha \) rectifies \( \varphi \) is \( \forall t_1 \ldots \forall t_k (\&_\ell \alpha_\ell(\varphi(t_1, \ldots, t_k) = t_\ell) \) – a first-order formula.
- Thus, if \( \exists \) a solution, then \( \exists \) a solution in which all coefficients of all polynomials \( \alpha_i \) and \( \beta_i \) are algebraic.
11. Proof of First Result

- Due to Tarski’s algorithm:
  - for each tuple of algebraic numbers,
  - we can check whether the corresponding polynomials constitute a rectifying automorphism.

- To find the desired polynomial mappings $\alpha$ and $\beta$ with algebraic coefficients, it is sufficient to:
  - enumerate all possible tuples of such coefficients,
  - try them one by one,
  - until we find a tuple which corresponds to the rectifying automorphism.

- Since we assumed that a rectification is possible, we will eventually find the desired coefficient.

- The only thing that needs to be clarified is how to enumerate all possible tuples of algebraic numbers.
12. Proof of First Result (cont-d)

- We need to enumerate all possible tuples of algebraic numbers.
- This can be easily done if we take into account that:
  - each algebraic number is represented in a computer
  - as a sequence of integers.
- It is easy to come with an algorithm that enumerates all possible sequences of integers.
- For example, for $M = 0, 1, \ldots$, we can enumerate all the sequences $(n_1, \ldots, n_k)$ for which
  
  \[ |n_1| + \ldots + |n_k| + k = M. \]

- For each $M$, there are finitely many such sequences, and it is easy to enumerate them all.
- The proposition is thus proven.
13. Proof of Second Result

- For each degree $d$, the Tarski-Seidenberg algorithm
  - reduces the formula describing the existing of a rectifying polynomial automorphism of degree $d$
  - to a finite list of (in)equalities between expressions polynomially depending on the given coefficients.
- In our definition of a generalized algorithm, we allowed:
  - additions and multiplications (all we need to compute the value of a polynomial) and
  - checking whether a given value is equal to 0 or greater than 0.
- So, $\forall d \exists$ a generalized algorithm that checks whether $\exists$ a rectifying polynomial automorphism of degree $d$. 
14. Proof of Second Result (cont-d)

• Since we assume that a rectification is possible:
  – by trying all possible degrees \( d = 0, 1, 2 \ldots \),
  – we will eventually find \( d \) for which \( \exists \) a rectifying rectifying polynomial automorphism of degree \( d \).

• To complete the proof, we need to compute the coefficients of the corresponding polynomial mapping \( \alpha \).

• We want to find the coefficients \( c_1, \ldots, c_N \) that satisfy a quantifier-free formula \( F(c_1, \ldots, c_N) = 0 \).

• Let’s find \( c_1 \) s.t. \( \exists c_2 \ldots \exists c_N (F(c_1, c_2, \ldots, c_N) = 0) \).

• We can use Tarski-Seidenberg theorem to reduce this formula to a sequence of formulas

\[
P_i(c_1) = 0 \text{ and } P_j(c_1) > 0.
\]
15. Proof of Second Result (cont-d)

- All equalities $P_i(c_1)$ be combined into a single equality $P(c_1) = 0$, where $P(c_1) \overset{\text{def}}{=} \sum_i (P_i(c_1))^2$.

- We know that this polynomial equation has a solution.

- We can therefore use one of the elementary steps of a generalized algorithm to compute a solution to it.

- If the solution $s$ produced by this elementary step does not satisfy the inequalities, then:
  - we get a new polynomial of a smaller degree
  - by dividing $P(c_1)$ by $c_1 - s$.

- It is clear that $c_1$ is a root of this polynomial.

- Division is algorithmic since it can also be reduced to (allowed) arithmetic operations with coefficients.
16. Proof of Second Result: Conclusion

- We can then repeat this procedure with the new polynomial of smaller degree, etc.
- At each step, either we find the desired $c_1$ or the degree decreases.
- Since the degree cannot decrease below 0, this means that we will eventually find $c_1$.
- Substituting this value $c_1$ into the above formula, we will then similarly compute a value $c_2$ for which
  \[ \exists c_3 \ldots \exists c_N \ (F(c_1, c_2, c_3, \ldots, c_N) = 0), \text{ etc.} \]
- After $N$ steps, we will compute all the coefficients of the rectifying polynomial $\alpha$.
- The proposition is proven.
17. Acknowledgments

This work was supported in part by the National Science Foundation grants:

- HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence), and
- DUE-0926721.
18. References