Математические структуры и моделирование
2015, вып. XX, с. 1–??

УДК 000.000

ONCE WE KNOW THAT A POLYNOMIAL MAPPING IS RECTIFIABLE, WE CAN ALGORITHMICALLY FIND A RECTIFICATION

J. Urenda[1], D. Finston[2], V. Kreinovich[1]

It is known that some polynomial mappings $\varphi : \mathbb{C}^k \to \mathbb{C}^n$ are *rectifiable* in the sense that there exists a polynomial mapping $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ whose inverse is also polynomial and for which $\alpha(\varphi(z_1, \ldots, z_k)) = (z_1, \ldots, z_k, 0, \ldots, 0)$ for all $z_1, \ldots, z_k$. In many cases, the existence of such a rectification is proven indirectly, without an explicit construction of the mapping α.

In this paper, we use Tarski-Seidenberg algorithm (for deciding the first order theory of real numbers) to design an algorithm that, given a polynomial mapping $\varphi : \mathbb{C}^k \to \mathbb{C}^n$ which is known to be rectifiable, returns a polynomial mapping $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ that rectifies φ.

The above general algorithm is not practical for large n, since its computation time grows faster than 2^{2^n}. To make computations more practically useful, for several important case, we have also designed a much faster alternative algorithm.

1. Formulation of the Problem

It is known that several classes of polynomial mappings are rectifiable in the following sense.

Definition 1. *Let $\mathbb{C}$ denote the field of all complex numbers. A polynomial mapping $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ is called a* polynomial automorphism *if this mapping a bijection, and the inverse mapping $\beta = \alpha^{-1}$ is also polynomial.*

Definition 2. *A polynomial mapping $\varphi : \mathbb{C}^k \to \mathbb{C}^n$ is called* rectifiable *if these exists a polynomial automorphism $\alpha : \mathbb{C}^n \to \mathbb{C}^n$ 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 α, without explaining how to actually compute it. In this paper, we show how to compute α.

[1]University of Texas at El Paso, El Paso, Texas 79968, USA
[2]New Mexico State University, Las Cruces, New Mexico 88003, USA
E-mail: jcurenda@utep.edu, dfinston@nmsu.edu, vladik@utep.edu

2. Main Result

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 and may not even be computable.

Definition 3. *A real number is called* algebraic *if this number is a root of a non-zero polynomial with integer coefficients, A complex number $a + b \cdot \mathrm{i}$ is called* algebraic *if both a and b are algebraic.*

Comment. In the computer, an algebraic real number can be represented by the integer coefficients of the corresponding polynomial and – if this polynomial has several roots – by a rational-valued interval that contains this particular root and does not contain any other roots of this polynomial.

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

Lemma 1. *If a polynomial mapping φ with algebraic coefficients is rectifiable, then there exists a rectifying polynomial automorphism α with algebraic coefficients.*

Proposition 1. *There exists an algorithm that, given a rectifiable polynomial mapping φ with algebraic coefficients, computes the coefficients of a polynomial automorphism α that rectifies φ.*

Discussion. It is desirable to extend this algorithm to the general case, when the coefficients of the original mapping φ are not necessarily algebraic and may not even be computable. 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.

Definition 4. *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.*

Comment. Of course, when the real numbers are algebraic, these operations are algorithmically computable.

Proposition 2. *There exists a generalized algorithm that, given the coefficients of a rectifiable polynomial mapping φ, computes the coefficients of a polynomial automorphism α that rectifies φ.*

Discussion. Propositions 1 and 2 show that if a polynomial mapping is rectifiable, then the corresponding rectification can be algorithmically computed.

Comments. Our proof uses the Tarski algorithm. While this algorithm produces the desired results, it is known to be hyper-exponential: as the length ℓ of the formula increases, its running time grows faster than 2^{2^ℓ}. Thus, from the application viewpoint, it is desirable to come up with a faster algorithm. For some important cases, such faster algorithm was proposed in [3]; it should be mentioned that, in contract to our algorithms which are limited to the field of all complex numbers, algorithms from [3] can applied to other fields (and rings) as well.

Comment. The main results were first announced in [4].

3. Proofs

Tarski-Seidenberg algorithm: reminder. In this paper, we will use Tarski-Seidenberg algorithm; see, e.g., [1, 2]. This algorithm deals with the *first-order theory of real numbers.* Formulas of this theory are defined as follows:

- we start with real-valued variables $x_1, \ldots, x_n$;
- *elementary formulas* are formulas of the type $P = 0$, $P > 0$, or $P \geq 0$, where P is a polynomial with integer coefficients;
- finally, a general formula can be obtained from elementary formulas by using logical connectives ("and" $\&$, "or" $\vee$, "implies" $\rightarrow$, and "not" $\neg$) and quantifiers over real numbers ($\forall x_i$ and $\exists x_i$).

For example, a formula describing that the given polynomial $P(x_1, \ldots, x_n)$ with integer coefficients has a solution with $x_i > 0$ for all i is a first-order formula:

$$\exists x_1 \ldots \exists x_n \, ((P(x_1, \ldots, x_n) = 0) \,\&\, (x_1 > 0) \,\&\, \ldots \,\&\, (x_n > 0)).$$

Another example is a formula that show that every quadratic polynomial with non-negative determinant has a solution:

$$\forall a \forall b \forall c \, ((b^2 - 4a \cdot c \geq 0) \rightarrow \exists x \, (a \cdot x^2 + b \cdot x + c = 0)).$$

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 noticed that Tarski's algorithm works by "eliminating" quantifiers one by one, i.e., by sequentially reducing a given formula to a one with one fewer quantifier. Because of this fact, he showed that we can use a similar construction to reduce each first-order formula with free variables to a quantifier-free form.

Tarski-Seidenberg algorithm: corollary. From the above reduction, it follows that if a formula with free variables has a solution, then it also has an algebraic solution. Namely, we can reduce the original formula to a quantifier-free formula $F(x_1, \ldots, x_n)$.

The formula $\exists x_2 \ldots \exists x_n \, F(x_1, x_2, \ldots, x_n)$ can be similarly reduced to a quantifier-free expression, i.e., to a combination of equalities and inequalities of the type $P(x_1) = 0$, $P(x_1) > 0$, and $P(x_1) \geq 0$. If one of them is an equality, then we

get an algebraic number x_1; if all of them are strict inequalities, then the whole range of values satisfies these inequalities and thus, we can select a rational (hence, algebraic) value from this interval.

Once we plug in the algebraic value x_1 into the original formula, we can then similarly find an algebraic value x_2, etc. – and after n stages, we will get a tuple of algebraic numbers $x_1, \ldots, x_n$ that satisfies the original formula $F(x_1, \ldots, x_n)$.

Proof of Lemma 1 and Proposition 1. Let us show that by using the Tarski-Seidenberg algorithm, we can come up with the desired algorithm for proving Proposition 1.

Let d be the largest degree of polynomials α_i and β_i forming the mappings α and $\beta = \alpha^{-1}$. Each of these polynomial can be described by listing all the coefficients – to be precise, by listing real and imaginary values of all these coefficients. The condition that α and β are inverse to each other means that

$$\forall z_1 \ldots, \forall z_n \, ((\alpha_1(\beta(z_1, \ldots, z_n)) = z_1) \,\&\, \ldots \,\&\, (\alpha_n(\beta(z_1, \ldots, z_n)) = z_n))$$

and

$$\forall z_1 \ldots, \forall z_n \, ((\beta_1(\alpha(z_1, \ldots, z_n)) = z_1) \,\&\, \ldots \,\&\, (\beta_n(\alpha(z_1, \ldots, z_n)) = z_n)).$$

Substituting the expressions for α and β in terms of their coefficients, we get a first order formula.

Similarly, the condition that α rectifies φ, i.e., that

$$\forall t_1 \ldots \forall t_k \, ((\alpha_1(\varphi(t_1, \ldots, t_k) = t_1) \,\&\, \ldots \,\&\, (\alpha_k(\varphi(t_1, \ldots, t_k) = t_k)),$$

is clearly a first-order formula. Thus, due to the above result, if there exists a solution, then there exists a solution in which all the coefficients of all the polynomials α_i and β_i are algebraic numbers.

For each tuple of algebraic numbers, checking whether the corresponding polynomials constitute a rectifying automorphism means checking whether a given first order formula is true, and this checking can be done by using the original Tarksi's algorithm.

To find the desired polynomial mappings α and β with algebraic coefficients, it is sufficient to enumerate all possible tuples of such coefficients, and 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. This can be easily done if we take into account that each algebraic number is represented in a computer as a sequence of integers. Thus, an arbitrary finite sequence of algebraic numbers can also be represented 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.

Proof of Proposition 2. 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 equalities and inequalities between expressions which polynomially depend on the given coefficients and 0. 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.

Thus, for each d, we have a generalized algorithm that checks whether a rectifying polynomial automorphism of degree d is possible.

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 there exists a rectifying rectifying polynomial automorphism of degree d.

To complete the proof, we need to show how we can compute the coefficients of the corresponding polynomial maping α. 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 us start with computing c_1. We want to find c_1 for which

$$\exists c_2 \ldots \exists c_N \, (F(c_1, c_2, \ldots, c_N) = 0).$$

We can use Tarski-Seidenberg theorem to reduce this formula to a quantifier-free one, i.e., to a sequence of polynomial equalities and inequalities $P_i(c_1) = 0$ and $P_j(c_1) > 0$. All equalities $P_i(c_1)$ be combined into a single equality $P(c_1) = 0$, where $P(c_1) \stackrel{\text{def}}{=} \sum_i (P_i(c_1))^2$. 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 this polynomial equation. 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. 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 that satisfies the formula

$$\exists c_3 \ldots \exists c_N \, (F(c_1, c_2, c_3, \ldots, c_N) = 0),$$

etc. After N steps, we will compute all the coefficients of the rectifying polynomial α. The proposition is proven.

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.

The authors are thankful to all the participants of the NMSU/UTEP Workshop on Mathematics, Computer Science, and Computational Science (Las Cruces, New Mexico, April 11, 2015) for valuable suggestions.

References

1. S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, Springer-Verlag, Berlin, 2006.
2. A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, 2nd ed., Berkeley and Los Angeles, 1951, 63 pp.
3. J. Urenda, *Algorithmic Aspects of the Embedding Problem*, PhD Dissertation, Department of Mathematical Sciences, New Mexico State University, Las Cruces, New Mexico, May 2015.
4. J. Urenda, D. Finston, and V. Kreinovich, "Once We Know that a Polynomial Mapping Is Rectifiable, We Can Algorithmically Find a Rectification", *Abstracts of the 16th Joint NMSU/UTEP Workshop on Mathematics, Computer Science, and Computational Science*, Las Cruces, New Mexico, April 11, 2015.