The Theory of a Real Closed Field and its Algebraic Closure

Ron van der Meyden
School of Computer Science and Engineering
University of New South Wales, Sydney 2052, Australia
meyden@cse.unsw.edu.au

Manas K Patra*
Department of Computer Science,
University of York, Heslington, York
YO10 5DD, UK
manas@scm.uws.edu.au

August 15, 2008

Abstract

A first order theory **RC** of a real closed field and its algebraic closure is presented. The non-logical axioms combine the axioms of the theories of real closed fields and the algebraically closed fields, but distinguish the real closed field as a subfield by means of a monadic predicate and a constant for a square root of -1. The resulting theory has several desirable properties: decidability, completeness, model-completeness and quantifier elimination. A decision procedure is presented for the problem of satisfiability of a formula, and its complexity is analysed.

1 Introduction

Two of the most thoroughly studied first order theories in model theory are the theories of algebraically closed fields (**ACF**) and real closed fields (**RCF**) [CK73, Poi00]. In some sense the former is simpler with equality as the only relation. In case of real closed fields we also have the predicate

*Work of this author done primarily while at UNSW.

"<". Both **ACF** and **RCF** have nice properties. They admit quantifier elimination, are decidable and complete. The most common model of **ACF** is the field of complex numbers, and that of **RCF** is the field of real numbers. However, there are other models. We note that any model $\mathcal{M}$ of **RCF** has an algebraic closure $\mathcal{M}'$ which is a model of **ACF**. The model $\mathcal{M}'$ can be obtained from $\mathcal{M}$ by adjoining the "imaginary" element $\sqrt{-1}$.

One of the objectives of the present work is to give a theory of such a pair $(\mathcal{M}, \mathcal{M}')$. We work on first order structures in which the carrier is that of $\mathcal{M}'$ and which (like the theories **RCF** and **ACF**) has operations for addition, multiplication and constants 0 and 1. The novelty is that we distinguish $\mathcal{M}$ as a substructure of $\mathcal{M}'$ by means of a unary predicate R. We also introduce a constant i to represent $\sqrt{-1}$. We axiomatize these structures by a theory $\mathbb{RC}$.

The motivation for this comes from our work on formal reasoning about quantum probabilities [MP03, Pat05]. These probabilities, as usual, are non-negative real numbers ≤ 1 but they arise from *complex* amplitudes characterizing the quantum state. Therefore, we need both real and complex numbers for representing quantum phenomena.

The structure of the paper is as follows. In Section 2 we present the theory $\mathbb{RC}$ and discuss some of its models. Section 3 establishes quantifier elimination and completeness results for $\mathbb{RC}$. This section also establishes decidability of satisfiability and analyses its complexity. The proofs of these results rely on a reduction algorithm which translates a formula of $\mathbb{RC}$ to a formula in **RCF**. We discuss some significant mathematical results that can be expressed in the theory in Section **??**. In the final section we discuss related work.

2 The theory $\mathbb{RC}$

In this section, the language $\mathbb{RC}$ and its semantics are presented. The theory of real and algebraically closed fields have been well studied. A rigorous treatment of the corresponding structures may be found, for example, in van der Waerden's classic text on algebra [vdW53]. A large part of model theory *is* the formal study of such fields, and they have been treated both from model theoretic [Hod93] and algorithmic viewpoints [BPR03]. However, the theory of a real closed field and its algebraic closure, *in combination*, does not appear to have been studied from a logical perspective.

The basic idea for our formalization of the combination is the standard construction of complex numbers as pairs of real numbers. The resulting

theory is called $\mathbb{RC}$. The theory has models other than the field of complex numbers, as the same construction can be applied starting with any real closed field.

The nonlogical symbols of the first order language $\mathcal{L}_{RC}$ are given below. We assume the standard logical symbols, including equality [Sho67].

1. **Function Symbols:** The function symbols include the binary symbols '$+$' and '$\cdot$' in the infix notation. We use x^n as a shorthand for the n-fold product $x \cdots x$

2. **Predicate Symbols:** The only nonlogical symbols are a binary predicate '$<$' and a unary predicate 'R'. The former is written in infix notation. The intended interpretation of $R(x)$ is that x is real.

3. **Constant Symbols:** The four principal constants are $0, 1, -1$ and i.

We use the abbreviations $Rx_1x_2 \ldots x_n$ for $Rx_1 \wedge Rx_2 \wedge \ldots \wedge Rx_n$, and $-x$ for $(-1) \cdot x$. The standard notation and the binding rules for addition and multiplication are used throughout.

When dealing with complexity results, it is important that we have an efficient representation of the integers since the size of the input depends on this representation. The standard representation for the positive integers is $1 + 1 + \cdots + 1$ (unary representation). However, it is more efficient to represent them as a k-ary expansion, where $k > 1$ is a positive integers such that all integers up to and including k are assumed to be defined. For example, for $k = 2$ we first define $2 = 1 + 1$. Then the binary number $a_n a_{n-1} \ldots a_0$, where each $a_i \in \{0, 1\}$, may be written as

$$a_0 + 2(a_1 + 2(a_2 + 2(a_3 + \ldots 2(a_{n-1} + 2a_n) \ldots)$$

This is a term of $\mathbb{RC}$ of size linear in n. In the complexity theory of real or algebraically closed field we often have to deal with multivariate polynomials with integer (or rational) coefficients. The size of the polynomial may be defined to be proportional to the sum of the bitlengths of the coefficients [BKR86].

2.1 Axioms

The axioms of the theory $\mathbb{RC}$ are as follows. Throughout, n and k are positive integers.

FL1 $(x + y) + z = x + (y + z)$
FL2 $x + 0 = x$
FL3 $x + (-1 \cdot x) = 0$
FL4 $x + y = y + x$
FL5 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
FL6 $x \cdot 1 = x$
FL7 $x \neq 0 \Rightarrow \exists y(x \cdot y = 1)$
FL8 $x \cdot y = y \cdot x$
FL9 $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
FL10 $0 \neq 1$
AC $y_n \neq 0 \Rightarrow \exists x(y_n \cdot x^n + y_{n-1} \cdot x^{n-1} + \ldots + y_1 \cdot x + y_0 = 0)$.
CR $\exists xy(Rx \wedge Ry \wedge z = x + i \cdot y)$
R1 $R0 \wedge R1 \wedge R(-1)$
R2 $Rxy \Rightarrow R(x + y) \wedge R(x \cdot y)$
R3 $x < y \Leftrightarrow Rx \wedge Ry \wedge \exists z(Rz \wedge z \neq 0 \wedge y = x + z^2)$
R4 $(Rx_1x_2 \ldots x_n \wedge x_1^2 + x_2^2 + \ldots + x_n^2 = 0) \Rightarrow \bigwedge_i x_i = 0$
I $i^2 + 1 = 0$

The axioms **FL1**-**FL10** specify a field. The axiom **AC** states that the field is algebraically closed. In particular, we have the instance

$$y \neq 0 \Rightarrow \exists x(yx - 1 = 0)$$

so we could dispense with **FL3**. Axioms **R1** and **R2** state that the set of elements x satisfying $R(x)$ forms a subring. It will be shown below that the axioms imply that these elements in fact form a field. **R4** then states this field has characteristic zero, so is a 'formally real field'. This implies that it can be ordered, but the ordering need not be unique. Axiom **R3** defines $<$ as a particular ordering (the ordering properties will be established below). The axiom **CR** states that every number may be obtained by the usual construction of the complex numbers from the reals. The axiom **I** gives the defining property of i.

2.2 Structures and Models

The theory $\mathbb{RC}$ is interpreted in first order structures for the language $\mathcal{L}_{RC}$. These are tuples $(S, +, \cdot, <, R, 1, -1, 0, i)$ where S is a set and the function, predicate and constant symbols are interpreted as functions, relations (of the appropriate arity) over S and elements of S, respectively. We may use the same symbols for the object language $\mathbb{RC}$ and for the structure. The intended interpetation will be clear from the context.

As noted above, it follows from the axioms that $(S, +, \cdot, 1, 0)$ must be a field of characteristic 0. Therefore, any model of $\mathbb{RC}$ must be an extension field of $\mathbf{Q}$. The following are some examples of models.

1. Let $S = \mathbf{C}$ be the set of complex numbers with the usual definition addition and multiplication, the constants $0, 1, -1, i$ and $R(x)$ interpreted as holding for the real numbers. Take the interpretation of the relation $<$ to be the set $\{(x, y)|Rx \text{ and } Ry \text{ and } x < y\}$ where the real numbers have the usual ordering. This yields a model of $\mathbb{RC}$.

2. Recall that an algebraic number is complex number that is a root of a polynomial with integer coefficients. Let $A \subset \mathbf{C}$ be the set of *algebraic* numbers. We identify R_A as the set of real algebraic numbers. The ordering is the one induced from the real numbers. Clearly A contains all the constants. The structure in which we take $S = A$ and $R = R_A$ and all other symbols by restriction from their interpretations for the complex numbers is a model of $\mathbb{RC}$.

3. In the two examples above the ordering is Archimedean. Recall that an ordered field F is Archimedean ordered if for any $x \in F$ there is an integer $n > x$. In the next example the ordering is *not* Archimedean.

   Let $Q(x)$ be the set of polynomials in an indeterminate x with rational coefficients. Define an ordering on $Q(x)$ by defining $p(x) = a_0 + a_1 x + \cdots + a_n x^n > 0$ iff $a_n > 0$. This defines an ordering on the domain $Q(x)$ which can be extended to the field $Q[x]$ of rational functions. Now let $\overline{Q[x]}$ be the *real* closure of $Q[x]$. Such a real closure is always possible [vdW53]. We further extend $\overline{Q[x]}$ to $\overline{Q[x]}(\sqrt{-1})$ by adjoining $\sqrt{-1}$. Take $S = \overline{Q[x]}(\sqrt{-1})$ and $R = \overline{Q[x]}$, interpret the constants and function symbols as in $\overline{Q[x]}(\sqrt{-1})$, and interpret $<$ as the set $\{(x, y)|Rx \text{ and } Ry \text{ and } x < y\}$, i.e., the ordering on $\overline{Q[x]}$. This structure is algebraically closed and is a model of $\mathbb{RC}$.

2.3 Definability

It is worth noting that our language for $\mathbb{RC}$ is a genuine extension of that for **ACF**, in the sense that the new constructs i and R cannot be introduced as defined terms. Given a language $\mathcal{L}$ interpreted in a structure M, say that a value c in the domain of M is *definable* in $\mathcal{L}$ if there exists a formula $\phi(x)$ with one free variable such that $\{x \mid M \models \phi(x)\} = \{c\}$. Similarly, the set S of elements of the domain of M is definable if there exists a formula $\phi(x)$ with one free variable such that $\{x \mid M \models \phi(x)\} = S$.

The folowing result shows that when we consider the complex numbers as the intended model of $\mathbb{RC}$, neither R nor i can be defined in this sense.

Proposition 1 *With respect to the complex number model, the set of real numbers is not definable in the language $\mathcal{L}_{\mathbf{ACF}} \cup \{i\}$. Also i is not definable in $\mathcal{L}_{\mathbf{ACF}} \cup \{R\}$.*

Proof: For any formula $\psi(x_1, x_2, \ldots, x_k)$ let $\mathcal{A}(\psi)$ be the subset of $\mathbf{C}^k$ on which ψ is satisfied.

If $\phi(z)$ is quantifier-free formula of **ACF** and has only the free variable z then from that fact that any boolean formula can be written in disjunctive normal form, we conclude that $\mathcal{A}(\phi)$ is a union of sets of the following form:

$$S = \{z \mid \bigwedge_i p_i(z) = 0 \wedge \bigwedge_i q_i(z) \neq 0\}$$

where $p_i(z)$ and $q_i(z)$ are polynomials in one variable. It is clear that either S or its complement in $\mathbf{C}$ is finite. Hence this is also true for finite union of such sets. We conclude that $\mathcal{A}(\phi(z))$ cannot represent the reals.

The theory of algebraically closed fields admits elimination of quantifiers [CK73, Poi00]. Hence, any formula $\chi(z)$ with one free variable is equivalent to a quantifier-free formula $\phi'(z, \mathtt{y})$. Note that, ϕ' may have other free variables which are grouped together by the "vector" $\mathtt{y}$. Since $M \models \chi z \Leftrightarrow \phi'(z, \mathtt{y})$ we can replace $\mathtt{y}$ by constants and still have the equivalence because the latter are not free in χ. Hence, setting $\mathtt{y} = \mathtt{0}$ (say) we get $\chi(z) \Leftrightarrow \phi'(z, \mathtt{y}|_{\mathtt{0}}) \equiv \phi(z)$. It follows that the set of reals is not definable in $\mathcal{L}_{\mathbf{ACF}}$.

Next we note that in $\mathcal{L}_{\mathbf{ACF}} \cup \{i\}$, an atomic formula is of the form $p(\vec{z}, i) = 0$, where p is a polynomial in the language of $\mathcal{L}_{\mathbf{ACF}}$ in several variables collectively represented by the vector $\vec{z}$. The arguments above still apply, since if we extend the theory **ACF** by adding a new constant i and an axiom $i^2 + 1 = 0$ it will still have quantifier elimination. To see this, given a formula $\chi(\vec{z}, i)$ of $\mathcal{L}_{\mathbf{ACF}} \cup \{i\}$, consider the formula $\chi(\vec{z}, y)$ of $\mathcal{L}_{\mathbf{ACF}}$, where y is a new variable. This is equivalent to a quantifier free formula $\phi(\vec{z}, y)$. Hence, the original formula is equivalent to $\phi(\vec{z}, i)$.

Finally, we observe that if $\psi(x)$ is a formula of $\mathcal{L}_{\mathbf{ACF}} \cup \{R\}$ then we can show by induction that $\mathbf{C} \models \psi(x) \Leftrightarrow \psi(\overline{x})$. Hence if $\psi(x)$ defines i then $i = \bar{i}$, i.e. $i = 0$, a contradiction. Hence i is not definable. $\square$

2.4 Some Theorems

Some simple consequences of the axioms of $\mathbb{RC}$ are given in the following result.

Lemma 1 *The following are theorems of* $\mathbb{RC}$.

$$Rx_1x_2\ldots x_n \Rightarrow x_1^2+\ldots+x_n^2 \neq -1 \qquad \text{for } n>0 \tag{1}$$

$$(x+i\cdot y = x'+i\cdot y' \wedge Rxyx'y') \Leftrightarrow x=x' \wedge y=y' \tag{2}$$

$$Rx \wedge x \neq 0 \Rightarrow \exists y(Ry \wedge x\cdot y = 1) \tag{3}$$

$$Rx \Rightarrow \exists y(Ry \wedge (x=y^2 \vee -x=y^2)) \tag{4}$$

$$R(x) \Rightarrow R(-x) \tag{5}$$

$$\neg Ri \tag{6}$$

$$R\mathbf{a} \qquad \text{if } \mathbf{a} \text{ is variable free term which does not contain } i \tag{7}$$

$$Rxy \Rightarrow (R(x+iy) \Leftrightarrow y=0) \tag{8}$$

$$Rxy \Rightarrow (x+iy>0 \Leftrightarrow x>0 \wedge y=0) \tag{9}$$

Proof: We sketch informal proofs. Formula (1) follows from the fact that $1=1^2$ (**FL6**) and $(Rx_1x_2\ldots x_n \Rightarrow x_1^2+\ldots+x_n^2=-1) \Leftrightarrow (Rx_1x_2\ldots x_n \Rightarrow x_1^2+\ldots+x_n^2+1^2=0)$. Hence, from **R4**, we get $1=0$, which contradicts **FL10**.

For formula (2), it will be sufficient to show that $0=x+i\cdot y \wedge Rxy \Rightarrow x=0\wedge y=0$. The latter follows immediately from the fact that $x+i\cdot y = 0 \Rightarrow x=-i\cdot y$, which in turn implies that $x^2+y^2=0$ (using **I**). Hence from **R4** it follows that $x=y=0$.

For formula (3), note that it follows from **FL7** and **CR** that $z\neq 0 \Rightarrow \exists xy(Rxy\wedge z\cdot(x+i\cdot y)=1)$. From this we deduce that $(z\cdot x-1)^2+(z\cdot y)^2=0$ and thus from **R1**, **R2** and **R4**, $Rz\wedge z\neq 0$ implies that $Rx\wedge z\cdot x=1$.

The formula (4) can be inferred as follows. From **CR** and **AC** it follows that $\exists xy(Rxy\wedge z=(x+i\cdot y)^2)$. Expanding the right side $z=x^2-y^2+2\cdot i\cdot x\cdot y$. If Rz then $2\cdot i\cdot x\cdot y=0$. This follows from arguments similar to those used above. Hence $x=0\vee y=0$ and it follows that $Rz \Rightarrow \exists x(Rx\wedge z=x^2)\vee\exists y(Ry\wedge z=-y^2)$ from which the claim follows easily.

We prove that $R(-1)$. By **CR** $\exists xy(-1=x+iy)$. This implies $(x+1)+iy=0$. Hence $x+1=0$ and $R(-1)$. Formula (5) follows from **R1** and **R2**. Formula (6) follows from **I**, **FL6**, **FL10**, and **R4**.

Formula (7) follows fom **R1** and **R2**.

For formula (8), note that we get from $Rxy \wedge R(x+iy) \wedge y \neq 0$ by **R2**, (3) and the field axioms that Ri, contradicting (6). That $R(x) \wedge y = 0$ implies $R(x+iy)$ is immediate from the field axioms.

Formula (9)is straightforward from **R3**, (8) and the field axioms. □

Formula (2) formalizes the notion that the 'real' and 'imaginary' parts of a complex number are unique. Using this fact, we may introduce complex conjugation as a defined function symbol, with the conjugate of z denoted by $\overline{z}$. The defining axiom is

Conj $Rxy \Rightarrow (z = x + i \cdot y \Leftrightarrow \overline{z} = z = x - i \cdot y)$

It can be proved that $\overline{(z_1 + z_2)} = \overline{z_1} + \overline{z_2}$ and $\overline{(z_1 \cdot z_2)} = \overline{z_1} \cdot \overline{z_2}$.

The definition of real fields is usually in given in the form of formula (1) [Sho67]. The advantage of **R4** over the formula (1) is that with the former we have to only postulate that the reals form a subring, and the fact that they also constitute a subfield can then be deduced. Note that it is also immediate from the field axioms and **R4** that the real elements constitute a formally real field.

A *real closed field* is a formally real field in which every polynomial of odd degree with has a root and in which $\forall x \exists y(x = y^2 \vee -x = y^2)$ holds. The fact that the real elements form a real closed field follows using (4) and the following lemma.

Lemma 2 *For each odd positive integer n, the formula*

RF $Rx_0x_1 \ldots x_n \wedge x_n \neq 0 \Rightarrow \exists y(Ry \wedge x_n \cdot y^n + \ldots + x_1 \cdot y + x_0 = 0.)$

is a theorem of $\mathbb{RC}$.

Proof: To prove this first observe that a polynomial of degree n over any algebraically closed field has exactly n roots (counting repetitions). The standard elementary proof [vdW53] can be formalized using only the field axioms **FL1** through **FL10** and **AC**. We need **AC** to show that for any polynomial $p(x) = y_n x^n + \ldots + y_0$, we have $\forall x(p(x) = 0) \Leftrightarrow \wedge_i y_i = 0$. This can be proved by induction on n. Thus, $\forall x(p(x) = 0) \Rightarrow \forall x(p(x) + 1 \neq 0)$. Hence **AC** implies that $y_n = 0$, and the assertion follows by induction. As a consequence, we have: two polynomials are equal iff all the coefficients are equal. In particular, two polynomials of different degree can not be equal. It follows from the division algorithm that, if a is a root of a polynomial $p(x)$ then $x - a$ divides $p(x)$. Then one proves that a polynomial of degree n has at most n roots. For example, the formula for degree=2 is $\forall y_2 y_1 y_0 \exists x_1 x_2 \forall x(y_2 x^2 + y_1 x + y_0 \Leftrightarrow x = x_1 \vee x = x_2)$.

Now, using complex conjugation it follows that $Rz \Leftrightarrow z = \overline{z}$. Writing $z = x + i \cdot y$ where Rxy, this may be seen as follows. In one direction, $z = \overline{z}$

implies $y = 0$ and $z = x$ and hence Rz. Conversely, suppose Rz. From the identity $((z^2 - x^2 + y^2)^2 + 4x^2y^2 = 0)$ and Rz we have $4x^2y^2 = 0$ by **R2** and **R4**. Hence, $x = 0$ or $y = 0$. If $y = 0$ then $\overline{z} = x = z$. But, if $x = 0$ then $z = iy$ and $z^2 + y^2 = 0$ which implies $z = x = 0$, so again $\overline{z} = x = z$. Thus, in either case $z = \overline{z}$.

If $p(x)$ has real coefficients then $p(z) = 0 \Leftrightarrow p(\overline{z}) = 0$. That is, nonreal roots come in distinct pairs. Hence if n is odd, then a real polynomial of degree n has a real root. We note that the informal arguments above can be formalised in $\mathbb{RC}$. □

Corollary 1 *Suppose M is a model of $\mathbb{RC}$. Let M_R be the restriction of M to the set of elements x satisfying $R(x)$. Then M_R is a model of* **RCF**.

Proof: That all the field axioms **FL1**-**FL10**, except **FL7** hold in M_R is immediate from their universal form. In fact, **FL7** also holds, by Lemma 1 part (3). That M_R is a formally real field follows from the fact that it satisfies **R4**. Every polynomial with odd degree has a root in M_R by Lemma 2, and $\forall x \exists y(x = y^2 \vee -x = y^2)$ holds by Lemma 1 part (4). □

The next lemma shows that the relation $<$ is a total linear order on values satisfying R.

Lemma 3 *It can be proved in $\mathbb{RC}$ that the relation $<$ is irreflexive, asymmetric, and transitive and satisfies the formula*

$$Rxy \Rightarrow x < y \vee x = y \vee y < x. \tag{10}$$

Proof: The formula $\neg(x < x)$ (irreflexivity) can be deduced from $x = x + z \Rightarrow z = 0$ and **R3**. Using the formula (4) and **R4** we deduce

$$Rxy \Rightarrow \exists z(Rz \wedge z^2 = x^2 + y^2)$$

Transitivity $(x < y \wedge y < z \Rightarrow x < z)$ is an easy consequence of this and **R3**. The formula $x < y \Rightarrow \neg(y < x)$ (assymetry) is a consequence of transitivity and irreflexivity.

Observe that $Rxy \Rightarrow x < y \Leftrightarrow x - y < 0$ is a theorem. Hence, to prove (10), it is sufficient to prove $Rx \Rightarrow x < 0 \vee x = 0 \vee 0 < x$. But this follows from (4) and the axiom **R3**. □

3 Quantifier Elimination and Decidability

A theory **T** is said to admit elimination of quantifiers if for any formula A in **T** there is an open (i e. quantifier free) formula B such that $A \Leftrightarrow B$ is provable in **T**. A theory **T** is a *complete* theory if every closed formula **A** is decided, i.e., **A** or $\neg$**A** is a theorem. Complete theories have many pleasant properties [Sho67]. Some of them are listed below for later use.

1. For any two models of a complete theory **T** the same formulas are valid.

2. To prove that a formula F is a theorem it suffices to show its validity in *any* model.

Actually, each of the above properties characterizes complete theories. As a consequence of the second property we may use any method to prove the validity of a formula in some model. For example, since the theory of real closed fields **RCF** is complete we may use analytical tools (e.g. differentiation and integration) in the field of real numbers to prove a formula of **RCF**. Then we are guaranteed that it is a theorem of **RCF**.

The main result of this section is the following.

Theorem 1 *The theory* $\mathbb{RC}$ *admits elimination of quantifiers. It is a complete theory.*

To prove this result, we develop a type of quantifier elimination result for $\mathbb{RC}$. For the following, if ψ is a formula of **RCF**, we define ψ^R to be the formula obtained from ψ by replacing each occurrence of a quantifier $\exists x(\phi)$ by $\exists x(Rx \wedge \phi)$. Note the following: if we have a model M of $\mathbb{RC}$, then we can obtain a model M_R of **RCF** by restriction to the set of elements satisfying R. Moreover, a closed formula ϕ of **RCF** holds in M_R iff ϕ^R holds in M.

We suppose that for each variable x of $\mathbb{RC}$ there is a pair of fresh variables x_r, x_i of **RCF**. If $\vec{z} = xy\ldots$ is a vector of variables, we write $\vec{z_r}$ for $x_r y_r \ldots$, and $\vec{z_i}$ for $x_i y_i \ldots$. We abbreviate $x = x_r + ix_i \wedge y = y_r + iy_i \wedge \ldots$ to $\vec{z} = \vec{z_r} + i\vec{z_i}$.

Lemma 4 *For any formula* $\phi(\vec{z})$ *of* $\mathbb{RC}$ *there is formula* $\psi(\vec{z_r}\vec{z_i})$ *of* **RCF** *such that the following is provable in* $\mathbb{RC}$*:*

$$\forall \vec{z_r}\vec{z_i}(R\vec{z_r}\vec{z_i} \wedge \vec{z} = \vec{z_r} + i\vec{z_i} \Rightarrow (\phi(\vec{z}) \Leftrightarrow \psi^R(\vec{z_r}\vec{z_i})).$$

Moreover, ψ *can be computed from* ϕ *in linear time.*

Proof: We note that by replacing atomic formulas of the form $t_1 = t_2$ by $t_1 - t_2 = 0$, and atomic formulas $t_1 > t_2$ by $t_1 - t_2 > 0$, we may assume that all atomic formulas are of the form $t = 0$, $t > 0$ or Rt.

We define a mapping $T : \mathbf{Fm}(\mathbb{RC}) \to \mathbf{Fm}(\mathbf{RCF})$ from the set of formulas of the theory $\mathbb{RC}$ to the theory **RCF**. Auxilliary to the definition is another mapping $\tau : \mathtt{t}(\mathbb{RC}) \to \mathtt{t}(\mathbf{RCF}) \times \mathtt{t}(\mathbf{RCF})$ from the set of *terms* of $\mathbb{RC}$ to a *pair* of terms of **RCF**, represented by $\tau(t) = (\tau_r(t), \tau_i(t))$. Intuitively, $\tau_r(t)$ and $\tau_i(t)$ are, respectively, the real and imaginary parts of the term t. The definition of τ is given by the recursion

$$\begin{aligned} \tau(\imath) &= (0,1), \text{ and } \tau(k) = (k,0), \ k \text{ an integer} \\ \tau(x) &= (x_r, x_i), \ x \text{ a variable} \\ \tau(t_1 + t_2) &= (\tau_r(t_1) + \tau_r(t_2), \ \tau_i(t_1) + \tau_i(t_2)), \\ \tau(t_1 \cdot t_2) &= (\tau_r(t_1)\tau_r(t_2) - \tau_i(t_1)\tau_i(t_2), \ \tau_r(t_1)\tau_i(t_2) + \tau_i(t_1)\tau_r(t_2)). \end{aligned} \tag{11}$$

Next, we define T. Let ϕ be an atomic formula. Then ϕ must be of the form $t = 0$, $t > 0$ or Rt. We define $T(\phi)$ in each case:

$$\begin{aligned} T(t = 0) \text{ is } T_r(t) = 0 \wedge T_i(t) = 0 \\ T(t > 0) \text{ is } T_r(t) > 0 \wedge T_i(t) = 0 \\ T(Rt) \text{ is } T_i(t) = 0 \end{aligned}$$

The inductive cases are given by:

$$\begin{aligned} T(\exists x \phi) &= \exists x_r x_i (T(\phi)) \\ T(\phi_1 \wedge \phi_2) &= T(\phi_1) \wedge T(\phi_2) \\ T(\neg \phi) &= \neg T(\phi) \end{aligned}$$

Note that for a formula $\phi(\vec{z})$ with free variables $\vec{z}$, the formula $T(\phi(\vec{z}))$ has free variables $\vec{z_r}\vec{z_i}$. We need to show that

$$\forall \vec{z_r}\vec{z_i}(R\vec{z_r}\vec{z_i} \wedge \vec{z} = \vec{z_r} + i\vec{z_i} \Rightarrow (\phi(\vec{z}) \Leftrightarrow T(\phi)^R(\vec{z_r}\vec{z_i})) \tag{12}$$

is a theorem of $\mathbb{RC}$. For ϕ an atomic formula, this follows using Lemma 1 parts (2), (8) and (9) and the fact that if t is a term with variables $\vec{z}$, then it can be shown using the field axioms and **I** that

$$\vec{z} = \vec{z_r} + i\vec{z_i} \Rightarrow t = \tau_r(t) + i\tau_i(t).$$

Proceeding inductively, assume that (12) is a theorem for $\phi(\vec{z})$. For the case of an existential, note that $T(\exists x \phi(\vec{z}))^R \equiv \exists x_r x_i (R(x_r x_i) \wedge T(\phi(\vec{z}))^R)$. Thus, we need to show

$$\forall \vec{y_r}\vec{y_i}(R\vec{y_r}\vec{y_i} \wedge \vec{y} = \vec{y_r} + i\vec{y_i} \Rightarrow (\exists x \phi(\vec{z}) \Leftrightarrow \exists x_r x_i (R(x_r x_i) \wedge T(\phi(\vec{z}))^R))).$$

where y is $\vec{z}$ minus x. For this note that the implication from left to right of the $\Leftrightarrow$ follows from (12) by **AC**, and the implication from right to left follows from (12) by taking $x = x_r + ix_i$. The cases for conjunction and negation are straightforward.

While this construction gives a formula that satisfies the theorem, we note that $T(\phi)$ may be of size exponential in the size of ϕ. This is because if we apply τ to a product $t = t_1 \dots t_n$ of n terms, we obtain that $\tau_r(t)$ and $\tau_i(t)$ are of size exponential in the size of t. To prevent this blowup, we can first massage formulas so as to remove terms that will cause such blowup under τ. We assume that for each term t of $\mathbb{RC}$ there is a distinct fresh variable z_t of **RCF**.

For this, we define the function $N : \mathbf{Fm}(\mathbb{RC}) \to \mathbf{Fm}(\mathbb{RC})$, which reduces the multiplicative depth of subterms as follows. Say that a term t is *basic* if all its multiplicative subterms $t_1 \cdot t_2$, have both t_1 and t_2 equal to either constants or variables. A formula is basic if all its terms are basic. Note that for any atomic formula $\phi(t_1 \cdot t_2)$ containing a multiplicative term $t_1 \cdot t_2$, the formula

$$\phi(t_1 \cdot t_2) \equiv \exists z_{t_1} z_{t_2} (\phi(z_1 \cdot z_2) \wedge z_1 - t_1 = 0 \wedge z_2 - t_2 = 0)$$

is provable. Repeatedly applying this equivalence, we may transform any quantifier free formula ϕ in linear time into an equivalent basic formula $N(\phi)$ of the form $\exists \vec{z}(\phi')$ where ϕ' is quantifier free. We also assume that the variables introduced do not occur in the original formula. We extend the operation N to the case where the original formula ϕ contains quantifiers by the inductive definition

$$\begin{aligned} N(\exists x \phi) &= \exists x (N(\phi)) \\ N(\phi_1 \wedge \phi_2) &= N(\phi_1) \wedge N(\phi_2) \\ N(\neg \phi) &= \neg N(\phi) \end{aligned}$$

A straightforward induction shows that for all formulas ϕ, we have $N(\phi) \equiv \phi$. Moreover, the size of $N(\phi)$ is linear in the size of ϕ.

Observe that for basic terms t, the size of $\tau(t)$ is linear in the size of t. Thus, $\psi = T(N(\phi))$ is a formula satisfying the theorem that is of size linear in the size of ϕ.

□

Since **RCF** admits quantifier elimination, the formula ψ may be assumed to be quantifier free. We remark that Lemma 4 is not quite a quantifier elimination theorem in the usual sense, since ϕ is proved equivalent to a

a quantifier free formula in the context of an assumption that makes use of the outer universal quantifiers and the predicate R; the latter prevents application of the quantifier elimination for $\mathcal{L}_{\mathbf{ACF}} \cup \{i\}$. However, if we introduce function symbols $Re(z), Im(z)$ for the real and imaginary parts of z, then we may eliminate the quantifiers and express the result as

$$\phi(\vec{z}) \Leftrightarrow \psi^R(Re(\vec{z}), Im(\vec{z})).$$

Alernately, a conjugation operation could be used to express $Re(z), Im(z)$.

Lemma 5 *Let ψ be a formula in the language of* **RCF** *without free variables. If ψ is a theorem of* **RCF** *then ψ^R is a theorem of $\mathbb{RC}$.*

Proof: We prove the contrapositive. Suppose that ψ^R is not a theorem of $\mathbb{RC}$. Then by completeness of first order logic, there exists a model M of $\mathbb{RC}$ in which ψ^R is false. Let M_R be the submodel of M obtained by restricting the domain to the set of elements x satisfying $R(x)$. An easy induction on the construction of ψ shows that M_R satisfies $\neg\psi$. By Corollary 1, M_R satisfies the axioms of **RCF**. Hence, by soundness of first order logic, ψ is not a theorem of **RCF**. □

Completeness of $\mathbb{RC}$ is an immediate consequence of this result.

Theorem 2 *If a formula ϕ of $\mathbb{RC}$ has no free variables, then either ϕ or $\neg\phi$ is a theorem of $\mathbb{RC}$.*

Proof: By Lemma 4, $\mathbb{RC}$ has a theorem of the form $\phi \Leftrightarrow \psi^R$ where ψ is a formula of **RCF** without free variables. Since **RCF** is complete, either ψ or $\neg\psi$ is a theorem of **RCF**. By Lemma 5, either ψ^R or $\neg\psi^R$ is a theorem of $\mathbb{RC}$. It follows that $\mathbb{RC}$ decides ϕ. □

We also obtain decidability of $\mathbb{RC}$, and can characterize its complexity.

Theorem 3 *The satisfiability of a formula in* **A** *in $\mathbb{RC}$ may be decided in exponential space. If* **A** *is quantifier free then satisfiability may be decided in polynomial space.*

Proof: By Lemma 4, given a formula $\phi(\vec{z})$ of $\mathbb{RC}$ we can compute in linear time a formula $\psi(\vec{z_r}\vec{z_i})$ of **RCF** such that the following is provable in $\mathbb{RC}$:

$$\forall \vec{z_r}\vec{z_i}(R\vec{z_r}\vec{z_i} \wedge \vec{z} = \vec{z_r} + i\vec{z_i} \Rightarrow (\phi(\vec{z}) \Leftrightarrow \psi^R(\vec{z_r}\vec{z_i})).$$

It follows that if ϕ is satisfiable in a model of $\mathbb{RC}$, then so is $\psi^R(\vec{z_r}\vec{z_i})$, hence $\psi(\vec{z_r}\vec{z_i})$ is satisfiable in a model of **RCF**. Conversely, if $\psi(\vec{z_r}\vec{z_i})$ is satisfiable M in a model of **RCF**, then adjoining $i = \sqrt{-1}$ to M we obtain a model $M[i]$ of $\mathbb{RC}$ and a satisfying assignment of $\psi^R(\vec{z_r}\vec{z_i})$. Hence, taking $z = z_r + iz_i$ we obtain a satisfying assignment of $\psi(\vec{z})$ in $M[i]$.

Thus ϕ is satisfiable in a model of $\mathbb{RC}$ iff ψ is satisfiable in a model of **RCF**. The theorem now follows using the exponential space complexity bounds for deciding **RCF** derived by Ben-Or, Kozen and Reif [BKR86]. In the quantifier free case, the formula ψ is of the form $\exists\vec{x}(\psi')$ where ψ' is quantifier free. This is satisfiable iff ψ' is satisfiable. Hence, in this case, the polynomial space complexity bounds of Canny [Can88] for the quantifier free case of **RCF** gives the result. □

Lemma 4 gives an algorithm for reducing a formula of $\mathbb{RC}$ to a formula of **RCF**. We then use the decision procedure for the latter to decide satisfiability of the former. The best-known decision procedures [BPR03] for **RCF** are improvements over Collins' cylindrical decomposition algorithm [Col75]. Now the time complexity of these algorithms depend crucially on the number of variables (it grows double exponentially). The procedure in Lemma 4 can increase the number of variables. First, consider the case of a single variable. The term z^n will be decompesed into terms terms involving $O(n)$ variables. This will cause an exponential blowup in the complexity. On the other hand, if we write $z = x + iy$ there are only two (real) variables. However, if we use this decomposition on the term $z_1 z_2 \cdots z_k$ then although the number of variables is only $2k$ the number of terms becomes $O(2^k)$. Therefore, a judicious combination of the two decomposition procedures is required. For example, we may combine both. Thus, for a monomial $\mathtt{t} = z_1^{n_1} \cdots z_k^{n_k}$ we replace each $z_i^{n_i}$ by a new variable u_i in $\mathtt{t}$ and follow the decomposition in Lemma 4 and in the equations $u_i = z_i^{n_i}$ we use $z_i = x_i + iy_i$. Combining this with the procedure in [BPR03] Chap. 11, we get that the time complexity of deciding satisfiability in $\mathbb{RC}$ is $O(sdk)^{O(1)^k}$ where s is a bound on the number of *polynomial terms* in at most k variables and d is a bound on their degrees.

4 Examples

The fact $\mathbb{RC}$ is a complete theory implies that a formula valid in *any* model is a theorem. We may use some techniques specific to the model, for example, topological arguments or integration. This is illustrated in the case of real

closed fields by proving the Weirstrass Nullstellansatz: *if a continuous real function f satisfies $f(a)f(b) < 0$ then it has a zero between a and b.* This can be proved for *polynomials* using the axioms of real closed fields [vdW53]. In our case we have a richer language. We prove the continuity and open mapping property of polynomial functions. We use these theorems to prove the maximum principle of complex function theory for the case of polynomials. We will make free use of the absolute value function: $|z| = \sqrt{\bar{z}z}$. The square root is a defined symbol for positive real elements (it can be extended to all elements.) The defining axiom is We can derive all the algebraic properties of square roots, for example, $\sqrt{x} < \sqrt{z} \Leftrightarrow x > 0 \wedge x < z$ and $|xy| = |x||y|$. It is also easy to see that the standard proof of the triangle inequality $|x + y| \leq |x| + |y|$ can be formalized as a theorem. Alternatively, we can deal with $|z|^2 = \bar{z}z$ if we want to avoid new symbols, but the proofs are a bit longer. Further, we have the following

Lemma 6 *The following are theorems in $\mathbb{RC}$, for each positive integer n:*

$$0 \leq x \wedge 0 \leq y \Rightarrow (x^n \leq y^n \Leftrightarrow x \leq y)$$
$$x_n z_0^n + \cdots + x_1 z_0 + x_0 = 0 \Rightarrow$$
$$\exists y_0 y_1 \ldots y_{n-1} \forall z (x_n z^n + \cdots + x_0 = (z - z_0)(y_{n-1} z^{n-1} + \cdots + y_0))$$

Proof: The first formula is proved by use of the identity

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2} y + \cdots + y^{n-1})$$

The second formula is a bit more involved. It expresses the fact that if z_0 is a zero of a polynomial $p(z)$ then $z - z_0$ divides $p(z)$. The standard proof given in any undergraduate textbook can be formalized. We recall that this involves the use of the division algorithm, a purely algebraic process. □

The following result expresses the continuity of polynomials.

Proposition 2 *For every integer $n \geq 0$*

$$\forall x_0 \cdots x_n z_0 w_0 (x_n z_0^n + \cdots + x_1 z_0 + x_0 = w_0) \wedge t > 0 \Rightarrow$$
$$\exists s (s > 0 \wedge \forall z (|z - z_0| < s \Rightarrow |x_n z^n + \cdots + x_0 - w_0| < t))$$

Proof: We first use the first identity in the preceding lemma to show that the mononomials $p(z) = z^k$ satisfy the above inequality. We assume first that $z_0 \neq 0$.

$$|z^k - z_0^k| = |z - z_0||z^{k-1} + z^{k-2} z_0 + \cdots + z_0^{k-1}| \leq |z - z_0|(|z|^{k-1} + \cdots + |z_0|^{k-1}|)$$

Thus if we choose $s = \min(t(2z_0)^{-k}, |z_0|)$ will satisfy the requirements. For $z_0 = 0$ we take $s = t^{\frac{1}{n}}$. The fact that positive real elements of $\mathbb{RC}$ possess unique positive roots of all order can deduced from the two properties: i. every positive real has a unique positive square root, and ii. every polynomial of odd degree has a real root. Now, to prove continuity for an arbitrary polynomial we use induction on the number of additive terms. Thus, assume $x_n \neq 0$. We write $p(z) = x_n z^n + \cdots + x_0$. Then $w_0 = p(z_0)$. We have from the triangle inequality $|p(z) - w_0| \leq |p(z) - x_n z^n - (w_0 - x_n z_0^n)| + |x_n z^n - x_n z_0^n|$. The polynomial $q(z) \equiv p(z) - x_n z^n$ has one less term and $q(z_0) = w_0 - x_n z_0^n$. Thus there is $s_1 > 0$ such that $|z - z_0| < s_1$ implies $|q(z) - q(z_0)| < t/2$ and there exist $s_2 > 0$ such that $|z - z_0| < s_2$ implies $|z^n - z_0^n| < t(2|x_n|)^{-1}$. Then $s = \min(s_1, s_2)$ satisfies the claim for $p(z)$. □

The next result is the open mapping property of polynomials. A complex function f is said to be *open* if it maps open sets to open sets [Ahl79]. This is a topological property. However, we can chracterize it algebraically by reducing it to the case of open disks on the complex plane.

Proposition 3 *The following is a theorem of* $\mathbb{RC}$.

$$\forall s z_0 w_0 (p(z_0) = w_0 \Rightarrow \exists t > 0 \forall w (|w - w_0| < t \Rightarrow \exists y (|y - z_0| < s \wedge p(y) = w)))$$

Proof: We prove that the negation of the above formula **F** leads to a contradiction. The negation says that there are s, z_0, w_0 such that $p(z_0) = w_0$ and for all $t > 0$ there exists w such that $|w - w_0| < t$ and for all y, $|y - z_0| < s$ implies $p(y) \neq w$. Take $t = s^n$, so that $|w_0 - w| < s^n$, and consider the polynomial $p(z) - w$. Since it can be factorized into linear factors (see Lemma 6) we can write $p(z) - w = (z - u_1) \cdots (z - u_n)$. Hence, $\neg$**F** implies that all zeros u_i of $p(z) - w$ must lie on the boundary or outside the circle $|z - z_0| < s$. Hence $|w_0 - w| = |p(z_0) - w| = |z_0 - u_1| \cdots |z_0 - u_n| \geq s^n$. This contradiction proves that **F** is a theorem. □

The proof is similar to one in [Tho86]. Finally we prove the maximum principle for polynomials.

Proposition 4 *The following formulas are theorems of* $\mathbb{RC}$. *For any positive integer* n

$$\forall x_0 \cdots x_n \forall z_0 r c (\neg(x_1 = x_2 = \cdots = x_n = 0) \wedge |z_0 - c| < r \Rightarrow$$
$$\exists y (|y - c| < r \wedge |x_n z_0^n + \cdots + x_1 z_0 + x_0| < |x_n y^n + \cdots + x_1 y + x_0|))$$

Proof: First, let us state the formula in words. Given any non-constatnt polynomial $p(z) = x_n z^n + \cdots + x_1 z + x_0$ of degree n, for any z_0 in the disk $C \equiv |z - c| < r$ there exists a y in the interior of the disk such that $|p(z_0)| < |p(y)|$. Let $w_0 = p(z_0)$. By the previous proposition there is some $t > 0$ such that all w satisfying $|w - w_0| < t$ are in range of $p(z)$ when restricted to the disk C. If $w_0 \neq 0$ then $w = w(1 + t(2|w_0|)^{-1})$ satisfies $|w - w_0| < t$ and $|w| > |w_0|$. Thus there is some y in C such that $p(y) = w$ and $|p(y)| > |w_0| = |p(z_0)|$. □

We presented proofs of three important theorems in complex analysis. However, we have to restrict to polynomial functions whereas all the theorems are true for *analytic* functions. We can extend the theorems to *rational* functions, that is, fractions of polynomial functions.

5 Related Work

The model theory of a pair (F, U) where F is a field and U is a subfield has been discussed before (see e.g. [CK73] Chap. 5 and the references there). These illustrate some special properties like *saturation* and *model completeness*. However, our work was motivated by the need for an axiomatization, and we have also studied algorithmic aspects of the theory. In particlar, we focussed on the pair where F is an algebraic closed field and U is its real closed subfield. As mentioned before, we were also motivated by the basic underlying structures of *quantum information theory*. We have shown elsewhere that based on the theory $\mathbb{RC}$ we can build fairly comprehensive logics [MP03, Pat05] to reason about quantum phenomena.

We also note some more recent works by Zilber [Zil90, Zil03]. The second paper is especially relevant. In it Zilber gives the theory $\mathbf{C}_{\mathbf{R},roots}$ with two unary predicates R and U. The predicate R is for the real axis as in our case. However, the predicate U is for the set of complex roots of unity. He gives a complete axiomatization for the language using some deep results from number theory. In our case we only use the 4th root of unity (i). Plainly, the nth roots of unity for any fixed n are definable in our language. This may be necessary to reason about some quantum protocols notably the Shor algorithm [NC01, Pat06].

References

[Ahl79] L. Ahlfors. *Complex Analysis.* McGraw-Hill, New York, 1979.

[BKR86] M. Ben-Or, D. Kozen, and J. H. Reif. The complexity of elementary algebra and geometry. *Journal of Computer and System Sciences*, 32(1):251–264, 1986.

[BPR03] S. Basu, R. Pollack, and M-F. Roy. *Algorithms in real algebraic geometry*. Springer, 2003.

[Can88] J. F. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. 20th ACM Symp. on Theory of Computing*, pages 460–467, 1988.

[CK73] C.C. Chang and H.J. Keisler. *Model Theory*. North-Holland, Amsterdam, 1973.

[Col75] G.E. Collins. Quantifier elimination for real closed fields by cylindric algebraic decomposition. In *Second GI Conf. on Automata Theory and Formal Languages, Lect. Notes. Comp. Sc., 33*, pages 134–183. Springer, Berlin, 1975.

[Hod93] W. Hodges. *Model Theory*. Cambridge, New York, 1993.

[MP03] R. v. Meyden and M. Patra. A logic for probability in quantum systems. In *Proc. Computer Science Logic and 8th Kurt Godel Colloquium*, Vienna, 2003. Springer-Verlag.

[NC01] M. A. Nielsen and I. L. Chuang. *Quantum computation and information*. CUP, 2001.

[Pat05] M. Patra. A logic for quantum circuits and protocols. In *Theoretical Aspects of Computing*, volume 3722 of *Lecture Notes in Compter Science*, page 424. Springer-Verlag, 2005.

[Pat06] M. Patra. Logics of probability for quantum computing and information. Thesis, University of New South Wales, 2006. (Unpublished).

[Poi00] B. Poizat. *A Course in Model Theory*. Springer, New York, 2000.

[Sho67] J. R. Shoenfield. *Mathematical Logic*. Addison-Wesely, 1967.

[Tho86] R. L. Thompson. Open mappings and the fundamental theorem of algebra. *Mathematics Magazine*, 43(1):39–40, 1986.

[vdW53] B. L. van der Waerden. *Modern Algebra, Vol 1*. Ungar, New York, 1953.

[Zil90] B. Zilber. A note on the model theory of the complex field with roots of unity. http://people.maths.ox.ac.uk/ zilber/publ.html, 1990.

[Zil03] B. Zilber. Complex roots of unity on the real plane. http://people.maths.ox.ac.uk/ zilber/publ.html, 2003.