A note on the axiomatisation of real numbers

Thierry Coquand and Henri Lombardi

September 17, 2007

Abstract

Is it possible to give an abstract characterisation of constructive real numbers? This question may be for instance of interest if one wants to specify an abstract data type of real numbers for exact real computations. A condition should be that all axioms are valid for Dedekind reals in any topos, or for constructive reals in Bishop mathematics. We present here a possible first-order axiomatisation of real numbers, which becomes complete if one adds the law of excluded middle. As an application of the forcing relation defined in [3, 2], we give a proof that the formula which specifies the maximum function is not provable in this theory.

Introduction

Is it possible to give an abstract characterisation of constructive real numbers? This question may be for instance of interest if one wants to specify an abstract data type of real numbers for exact real computations. A condition should be that all axioms are valid for Dedekind reals in any topos, or for constructive reals in Bishop mathematics[1]. We present here a possible first-order axiomatisation of real numbers, which becomes complete if one adds the law of excluded middle. As an application of the forcing relation defined in [3, 2], we give a proof that the formula

$$\forall x\ y.\exists m.\forall z.\ \ [z < m \leftrightarrow (z < x \vee z < y)]$$

which specifies the maximum function, is not provable in this theory.

1 A theory of reals

We consider the following theory, divided in four parts D,S,C,H.

This theory is a first-order theory in the language of rings together with two unary predicate $x > 0$ and $x \geq 0$. We write $x \leq y$ for $y - x \geq 0$ and $x < y$ for $y - x > 0$. We recall that a *positive* formula is a formula built from the grammar

$$\phi \ ::= \ \top \mid \ \bot \ \mid \phi \wedge \phi \mid \phi \vee \phi \mid \exists x.\phi \mid A$$

where A ranges over atomic formulae, and a *coherent* formula is an implication between positive formulae. Since ϕ and $\top \to \phi$ are equivalent, any positive formula can be considered to be also a coherent formula. A *coherent* theory is a set of coherent formulae.

[1] There are subtle differences. For instance the formula $\forall p\ q.\exists x.x^3 + px + q = 0$ holds for reals in Bishop framework, but is not valid for Dedekind reals in topos theory [7]. This is essentially because the proof uses the axiom of dependent choice.

The first part D consists in the axioms of commutative rings together with the direct axioms [3] of *proto-ordered rings*.

$$\begin{array}{cccc} & x^2 \geq 0 & x \geq 0 \wedge y \geq 0 \rightarrow x+y \geq 0 & x \geq 0 \wedge y \geq 0 \rightarrow xy \geq 0 \\ 1 > 0 & x > 0 \rightarrow x \geq 0 & x \geq 0 \wedge y > 0 \rightarrow x+y > 0 & x > 0 \wedge y > 0 \rightarrow xy > 0 \end{array}$$

The second part S consists in the *simplification axioms*, or axioms of *quasi-ordered rings* [3]

$$\begin{array}{ll} x^2 \leq 0 \rightarrow x \geq 0 & c \geq 0 \wedge cs > 0 \rightarrow s > 0 \\ s > 0 \wedge cs \geq 0 \rightarrow c \geq 0 & c \geq 0 \wedge x(x^2+c) \geq 0 \rightarrow x \geq 0 \end{array}$$

The third part C consists in the coherent axioms

$$\begin{array}{ll} x+y > 0 \rightarrow x > 0 \vee y > 0 & xy > 0 \rightarrow x > 0 \vee y < 0 \\ x > 0 \rightarrow \exists y . xy = 1 & \neg(x \geq 0 \wedge x < 0) \end{array}$$

Following [4] we add the following coherent axiom of *separable closure*, where p denotes a monic polynomial

$$\delta_0(p) \rightarrow \exists x . 0 < x < 1 \wedge p(x) = 0$$

where $\delta_0(p)$ is a positive formula which is equivalent modulo the theory of real closed field to the formula

$$p(0)p(1) < 0 \wedge \forall x . 0 \leq x \leq 1 \rightarrow p'(x) > 0$$

We cannot add the stronger form of this axiom that any monic polynomial whose sign changes between a and b has a root in (a,b) for $a < b$, since this axiom is not valid for Dedekind reals in topos theory [7]. This stronger form is coherent however, since it can be formulated as

$$p(0)p(1) < 0 \rightarrow \exists x . 0 < x < 1 \wedge p(x) = 0$$

We call C' the version of C with this stronger form.

The second axiom of part C is equivalent to the formula

$$xy > 0 \leftrightarrow (x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)$$

Indeed, this formula clearly implies $xy > 0 \rightarrow x > 0 \vee y < 0$. Conversely, assume $xy > 0 \rightarrow x > 0 \vee y < 0$. If we have $xy > 0$ then $x > 0 \vee 0 > y$ and $y > 0 \vee 0 > x$. We have also $\neg(x > 0 \wedge 0 > x)$ since $\neg(x \geq 0 \wedge x < 0)$ and $x > 0 \rightarrow x \geq 0$, and similarly $\neg(y > 0 \wedge 0 > y)$. So we get $(x > 0 \wedge y > 0) \vee (x < 0 \wedge y < 0)$. From T_1 we have $x > 0 \wedge y > 0 \rightarrow xy > 0$ and since $0 > x \leftrightarrow -x > 0$ and $(-x)(-y) = xy$ we also have $x < 0 \wedge y < 0 \rightarrow xy > 0$.

The last part H, consists in the axiom of *Heyting ordered field*

$$\neg(0 > x) \rightarrow x \geq 0$$

Lemma 1.1 *The Dedekind reals $\mathbb{R}$ form a model of the theory D,S,C,H*

Proof. It is direct that $\mathbb{R}$ is a model of D,S,H. The fact that $\mathbb{R}$ form a model of C is proved in [4]. □

2 A non provable statement

One can use Lemma 1.1 to prove that some statements are not derivable in the theory D,S,C,H, simply because they do not hold intuitionistically for Dedekind reals. Here is a simple example.

Proposition 2.1 *The formula*

$$\forall x.\exists z.x^2 z = x$$

is not provable in the theory D,S,C,H.

Proof. Using Lemma 1.1, it is enough to show that this formula cannot hold for $\mathbb{R}$. We show that it implies the Limited Principle of Omniscience [7]: if it holds then we can decide $x = 0$ or $x \neq 0$. Indeed, if it holds there exists z such that $x(1 - xz) = 0$. We can then find $N > 0$ such that $|z| \leq N$. We have also $|x| < 1/2N$ or $|x| > 1/4N$. If $|x| < 1/2N$ holds we have $|xz| \leq 1/2$ and so $|1 - xz| \geq 1/2$ and $x(1 - xz) = 0$ implies $x = 0$. On the other hand, if $|x| > 1/4N$ we have $x \neq 0$. □

The main goal of this note is to show that in the theory D,S,C,H we cannot deduce using only intuitionistic logic the following formula which specifies the maximum function

$$(*) \qquad \exists m.\forall z.z < m \leftrightarrow (z < x \vee z < y)$$

Notice that that this formula is valid intuitionistically for $\mathbb{R}$, since we can define the function $max : \mathbb{R} \to \mathbb{R} \to \mathbb{R}$. Hence we cannot use Lemma 1.1 and soundness of derivations in first-order logic like for Proposition 2.1.

Notice also that the situation is much different from the classical case. If we add classical logic, the formula $(*)$ becomes provable. Actually, this formula is a simple intuitionistic consequence of $\forall x.x > 0 \vee x \leq 0$. More generally, if we add classical logic, we get a *complete* first-order axiomatisation of the reals. Indeed, it is shown in [4] that any model of S, D, C satisfies that, if p is a separable monic polynomial of odd degree then p has a root. Hence with classical logic, any model of D,S,C is a real closed field.

Lemma 2.2 *In the theory D,S,C,H the formulae*

$$\forall z.z < m \leftrightarrow (z < x \vee z < y)$$

and

$$m \geq x \wedge m \geq y \wedge (m - x)(m - y) = 0$$

are equivalent.

Proof. Assume $\forall z.z < m \leftrightarrow (z < x \vee z < y)$. Since $\neg(m < m)$ we have $\neg(m < x \vee m < y)$ and hence $\neg(m < x)$ and $\neg(m < y)$. Because of the axiom of Heyting ordered field this implies $x \leq m$ and $y \leq m$. For showing $(m - x)(m - y) = 0$, it is enough in D,S,C,H to show $\neg((m - x)(m - y) > 0)$ and $\neg((m - x)(m - y) < 0)$. We have that $(m - x)(m - y) < 0$ implies $m < x$ or $m < y$, which contradicts $x \leq m \wedge y \leq m$. Also $(m - x)(m - y) > 0$ would imply $m > x \wedge m > y$ or $x > m \wedge y > m$. The second alternative is not possible since it contradicts $x \leq m$. In the first alternative we can find $z < m$ such that $x < z \wedge y < z$ and this contradicts $z < x \vee z < y$.

Conversely, assume $m \leq x$, $m \leq y$ and $(m - x)(m - y) = 0$. We show

$$z < m \leftrightarrow (z < x \vee z < y)$$

for an arbitrary z. Assume $z < x$. We have then $z < x \wedge x \leq m$ and so $z < m$. Similarly $z < y$ implies $z < m$. Conversely, assume $z < m$. We have then $z < x \vee x < m$ and $z < y \vee y < m$. Also, $x < m \wedge y < m$ implies $(m - x)(m - y) > 0$, which contradicts $(m - x)(m - y) = 0$. So we have $z < x \vee z < y$. □

The theory D,S,C is a *coherent* theory. We can thus consider a forcing relation associated to this theory [2]. The forcing conditions X are determined by a finite number of parameters $x_1, \dots, x_p$ and a finite number of conditions $C = f_1 > 0, \dots, f_n > 0, g_1 \geq 0, \dots, g_m \geq 0$ with $f_i, g_j \in \mathbb{Z}[x_1, \dots, x_p]$. We write $X \Vdash \phi$ if ϕ is forced at the condition C. The main result of [2] is the following.

Proposition 2.3 *If $\phi_1, \dots, \phi_n \vdash \phi$ and $X \Vdash \phi_1, \dots, X \Vdash \phi_n$ then $X \Vdash \phi$*

This implies that $\Vdash \phi$ holds whenever $\vdash \phi$ for any formula ϕ. An important result is also that if ϕ is coherent, we have $X \Vdash \phi$ iff $X \vdash \phi$ in the theory D,S,C [2].

The following Lemma is proved in [3] for the *stronger* coherent theory D,S,C'.

Lemma 2.4 *The conditions X collapse, i.e. we can prove $X \vdash \perp$ in the theory D,S,C iff we can write $m + p = 0$ where m is in the multiplicative monoid generated by $f_1, \dots, f_n$ and p is in the positive cone generated by $f_1, \dots, f_n, g_1, \dots, g_m$. If the conditions $X, f > 0$ and $X, g > 0$ collapse then so does the condition $X, f + g > 0$. If the conditions $X, f > 0$ and $X, g < 0$ collapse then so does the condition $X, fg > 0$. Finally if the condition $X, xf = 1$ collapses, where x is a fresh parameter, then so does the condition $X, f > 0$.*

Corollary 2.5 *We have $X, f > 0 \vdash \perp$ iff $X \vdash f \leq 0$ and $X, f \geq 0 \vdash \perp$ iff $X \vdash f < 0$.*

Proof. Assume $X, f > 0 \vdash \perp$. We can write $fm + fp + p' = 0$ where m is in M, the mutiplicative monoid generated by $f_1, \dots, f_n$ and p, p' are in P, the cone generated by $f_1, \dots, f_n, g_1, \dots, g_m$. The simplification axioms then imply $f \leq 0$ [3]. The second clause has a similar proof. □

Corollary 2.6 *We have $\Vdash \neg(f > 0) \to f \leq 0$.*

Proof. Assume that we have $X \Vdash \neg(f > 0)$. We then have $X, f > 0 \vdash \perp$ and hence $X \vdash f \leq 0$ by Corollary 2.5. Thus $X \Vdash f \leq 0$. This shows $\Vdash \neg(f > 0) \to f \leq 0$. □

This means that the axiom of Heyting ordered field, though being not derivable, is *forced*. This is analogous to the fact that the axiom $(\neg \exists y. xy = 1) \to x = 0$ is forced, but not provable, for the theory of local rings [5].

Corollary 2.7 *If $D, S, C, H \vdash \phi$ then $\Vdash \phi$.*

Proof. If $D, S, C, H \vdash \phi$ we have $\Vdash \phi$ using Proposition 2.3 and Corollary 2.6. □

Corollary 2.8 *If ϕ is coherent, we have ϕ is provable in D,S,C iff it is provable in D,S,C,H.*

Proof. Since ϕ is coherent we know that $\Vdash \phi$ is equivalent to $D, S, C \vdash \phi$ [2]. The result follows then from Corollary 2.7. □

Theorem 2.9 *The formula*

$$(*) \qquad \exists m. \forall z. z < m \leftrightarrow (z < x \vee z < y)$$

is not provable in the theory D,S,C,H.

Proof. By Lemma 2.2 it is enough to show that the formula

$$\exists m.m \geq x \wedge m \geq y \wedge (m-x)(m-y) = 0$$

is not provable in D,S,C,H. Since this formula is coherent, by Corollary 2.8, it is enough to show that this formula is not provable in the theory D,S,C.

We give first the argument without the axiom of separable closure. If $(*)$ was provable, we would have a finite covering of the plane by open U_i and over each U_i we have a fraction $p_i(x,y)/q_i(x,y)$ such that $q_i(x,y) > 0$ on U_i and $p_i(x,y)/q_i(x,y) = max(x,y)$ on U_i. This would imply $p_i(x,y)/q_i(x,y) = x$ or $p_i(x,y)/q_i(x,y) = y$, since this equality holds on a non trivial open set. We get a contradiction by taking U_i which contains the point $(1,1)$.

The argument with the axiom of separable closure is more subtle, but follows the same pattern. If $(*)$ was provable, we would have a finite covering of the plane by open U_i and over each U_i we have a Nash function $f_i(x,y)$ [1] such that and $f_i(x,y) = max(x,y)$ on U_i. This would imply $f_i(x,y) = x$ or $f_i(x,y) = y$ on any connected open which does not meet the diagonal, since this equality holds on a non trivial open set (Proposition 8.1.13 of [1]). We get a contradiction by taking U_i which contains the point $(1,1)$. □

This note suggests the following problems.

Problem 1. The theory presented in [4] is not explicitely given (the formula $\delta_0(p)$ in the axiom of separable closure is not explicit), and the proofs are given using classical logic. Is there an explicit theory of separably real closed local rings, with a constructive proof that it indeed captures this notion?

Problem 2. We have proved that the theory D,S,C,H is incomplete intuitionistically. The second author [6] has suggested a coherent theory which contains as one axiom the existence of virtual roots for monic polynomials (without the axiom of separable closure). The formula $(*)$ is a special instance, stating the existence of virtual roots for the polynomial $(X-x)(X-y)$. Is separable closure provable intuitionistically in this theory?

References

[1] J.Bochnak, M. Coste, M-F. Roy. *Géometrie algébrique réelle.* Springer-Verlag, 1987.

[2] Th. Coquand. A Completness Proof for Geometrical Logic in *Logic, Methodology and Philosophy of Sciences*, Hajek, Valdes-Villuaneva, Westertahl, editors, 79-90, 2005.

[3] M. Coste, H. Lombardi, and M.F. Roy. Dynamical methods in algebra: effective Nullstellensätze, *Annals of Pure and Applied Logic* **111**(3):203–256, 2001.

[4] A. Joyal, G.E. Reyes. Separably real closed local rings. *J. Pure Appl. Algebra* 43 (1986) 271–279.

[5] A. Kock. Universal projective geometry via topos theory. *J. Pure Appl. Algebra* 9 (1976/77), no. 1, 1–24.

[6] H. Lombardi. Constructive real algebra Talk given at the MAP meeting, Leiden, 2007.

[7] A. Troelstra and D. van Dalen. *Constructivism in Mathematics. An Introduction.* Volume II, North-Holland, 1988.