Boolean-valued logic and the theory of the algebraic integers

1. Booleanization

1.1. **Boolean algebras.** A compact Hausdorff space X is called *zero-dimensional* or *totally disconnected* if it has a basis of clopen sets. In this case, the clopen subsets from a Boolean algebra B, and the points of X can be identified with homomorphisms $B \to \{0,1\}$ (namely x maps b to 1 iff $x \in b$.)

A *pointed Boolean algebra* is a Boolean algebra with a distinguished maximal ideal, given by a unary predicate.

Definition 1.2. The theory $\widetilde{BA}$ of *atomless Boolean algebras*: is the theory BA of Boolean algebras along with $1 > 0$ and

$$(\forall x \in B)(x > 0 \implies (\exists y)(x > y > 0))$$

Definition 1.3. The theory $\widetilde{BA}_\infty$ of atomless Boolean algebras with distinguished maximal ideal has the language of Boolean algebras with an additional unary predicate I_∞; the axioms are $\widetilde{BA}$ along with: I_∞ is a maximal ideal.

A model of $\widetilde{BA}_\infty$ corresponds to a totally disconnected compact space without isolated points and with one distinguished point.

Like $\widetilde{BA}$, $\widetilde{BA}_\infty$ is complete, and eliminates quantifiers. It is the model-completion of the theory BA_∞ of pointed Boolean algebras. The main point to check is the amalgamation property for *finite* Boolean-algebras-with-distinguished-maximal ideal. Dualizing, this amounts to the co-amalgamation property - existence of fiber products - for *finite* pointed compact spaces, i.e. for for finite pointed sets. This is straightforward.

1.4. **Booleanization.** Let T be a theory in a language L. We will assume (without any real loss of generality) that T admits elimination of quantifiers.

1.5. **Language of T_{bool}.** Let L_{bool} be a language with the sorts of L and one additional sort B. (For simplicity we will use notation as if L has a single sort K.) On B we have the operations of a Boolean algebra, and the equality relation. In addition, for any formula $\phi(x_1, \ldots, x_n)$ of L, we have a function symbol $[\phi]$: $K^n \to B$ with the same variables. We view $[\phi]$ as giving the Boolean truth value of ϕ.

1.6. **Axioms of T_{bool}.**

(1) B is a Boolean algebra.
(2) If $T \models (\forall x)\phi$, then $[\phi(a)] = 1$.
(3) For any a, $\phi \mapsto [\phi](a)$ is a Boolean homomorphism.
(4) Assume $T \vdash \psi_i(y) \implies (\exists x)\phi_i(x, y)$, $i = 1, \ldots, n$. Then

$$(\forall b_1, \ldots, b_n)(\bigwedge_{i \neq j} b_i \cap b_j = 0 \& \bigwedge [\psi_i(y)] \geq b_i \implies (\exists x) \bigwedge_i [\phi_i(x, y)] \geq b_i$$

1.7. **Discussion.** .

(1) (1-3) are universal axioms. (4) contains the AE axioms. For $n = 1$ it is a *local-global* principle: fixing a, if there is no local obstruction (at some point of X) to the existence of b with $\phi(a, b)$, then such a b actually exists. In addition, we have a *glueing principle* over disjoint $b_1, \ldots, b_n$.
(2) As a special case of (4), for any formula $\phi(x)$, then the image of the function $\{b : [(\forall x)\phi] \leq b \leq [(\exists x)\phi]\}$. Assume $T \models (\exists x)(\exists y)(x \neq y)$; applying this for formulas with parameters, namely to $x = a$, we have $B = \{[c = a] : c \in K\}$.
(3) Let $M \models T_{bool}$. Given a Boolean homomorphism $f : B \to \{0, 1\}$, we can define a structure M_x such that $M_x \models T$ for all $x \in Hom(B, \{0, 1\})$; the interpretation of ϕ is $x([\phi])$.
(4) If $M \models T_{bool}$, then M is determined as a structure by B and the values of $[\phi]$ for atomic formulas ϕ. Indeed by (4), $[(\exists x)\phi(x, b)]$ is the least upper bound in B of $\{[\phi(a, b)] : a \in M\}$.

Remark 1.8. When ϕ is a sentence, $[\phi]$ is a new constant symbol in the sort B. We call these the *characteristic constants*.

The quantifier-elimination axioms of T easily translate via 1.6 (4) to quantifier-elimination axioms for T_{bool}:

Lemma 1.9. *Assume T eliminates quantifers over some sort K; Then T_{bool} eliminates K- quantifiers.*

If T eliminates all quantifiers, then T_{bool} is complete modulo the theory of B in the language of Boolean algebras with additional constants (namely the characteristic constants from 1.8).

Exercise 1.10. Let X be a topological space.

(1) Define the notion of a *sheaf of L-structures*.
(2) Let $M \models T_{bool}$, with Boolean algebra B. Let X be the Stone space of B. For $p \in X$, let M_p be the two-valued model corresponding to p. Show that this is a sheaf of L-structures, such that every stalk is a model of T.
(3) Conversely, assume X is totally disconnected and A is a sheaf of L-structures, such that every stalk M_p is a model of T. Let M be the set of global sections. For an L-formula ϕ, define $[\phi] = \{p : M_p \models \phi\}$. Show that this is a model of T_{bool}.

Example 1.11 (lattice-ordered groups.)**.** Let $L = (0, +, <)$ the language of ordered Abelian groups, and let DOA be the theory of divisible ordered Abelian groups. A a divisible ordered Abelian group. Let X be the Stone space of B, and let , $A_B = C(X, M)$ be the set of continuous functions $X \to A$ (with A viewed as discrete.) We define: $f \leq g$ iff $f(x) \leq g(x)$ for all x. Similarly define $+, 0$. Let $[\phi(a_1, \ldots, a_n)] = \{x : A \models \phi(a_1(x), \ldots, a_n(x))\}$. Then $(A_B, B) \models DOA_{bool}$.

Exercise 1.12. In particular A_B as a partially ordered Abelian group is interpretable in DOA_{bool}. Conversely show that B and the structure (A_B, B) can be interpreted in A_B.

Exercise 1.13. ACF_{bool} is (equivalent to) the theory of algebraically closed commutative rings with no nonzero nilpotent elements. Explain.

1.14. **A pointed / locally compact variant.** A variant corresponding to a *locally compact space* Y. We can let $X = Y \cup \{\infty\}$ be the 1-point compactification. We may wish to specify that a specified extension T_∞ holds at ∞.

Assume now given a specified competion T_∞ of T is given.

1.15. **Axioms of $T_{bool,\infty}$.** $L_{bool,\infty}$ consists of L_{bool} along with a distinguished maximal ideal I_∞ of B. We let $T_{bool,\infty} = T_{bool} + [\neg\phi] \in I$ for all quantifier-free ϕ such that $T_\infty \vdash \phi$.

Exercise 1.16. $T_{bool,\infty}$ eliminates K-quantifiers. It is complete modulo the theory of B in the language of Boolean algebras with a distinguished maximal ideal I and additional constants (namely the characteristic constants from 1.8 (1)).

2. Booleanization relative to a sublanguage

Let T be a theory in a language L, with a distinguished sublanguage $L_!$. Let $T_! = T|L_!$.

Assume T admits elimination of quantifiers.

We define the *Booleanization relative to* $L_!$ where the formulas of $L_!$ remain absolute. A model will be a model of $T_!$ and *a sheaf of expansions of M to a model of T, over a compact zero-dimensional space X.*

Remark 2.1. When the equality symbol is in L but not in $L_!$, an *expansion* of a model S of $L_!$ should be understood to include the interpretation E of equality; i.e. the universe of the expansion is S/E for an appropriate congruence E, rather than S itself. This is the case in the construction of ultraproducts, and in the sheafification over $\emptyset$ considered above. However, in the case of main interest to us equality does lie in $L_!$.

2.2. **Quantifiers over finite sets.** The local-global axiom 2.4(5) is usually unreasonable for *finite* definable sets. For instance $RCF \models (\exists x)(x^2 = 2 \& x > 0)$. Let $L = \mathbb{Q}[\sqrt{2}]$, $X = Hom(L, \mathbb{R})$, and for a formula ϕ in the language of ordered rings, let $[\phi] = \{x \in X : \mathbb{R} \models \phi^x\}$. In L there exists a square root a of 2, but $[a > 0], [a < 0]$ form a partition of unity in the Boolean algebra; in no field extension of L can there exist an element a with $[a > 0] = 1$.

This will force us to accept *bounded quantifers*; quantifiers of the form $(\exists x)(\phi_!(x, y) \& \psi(x, y))$, where ϕ is a formula of $L_!$ with finitely many solutions in each x (for each y.)

In the case that $T_!$ is a theory of fields, one can reduce to $(\exists x)(f(x,y) = 0 \& \psi(x,y))$, where f is a monic polynomial in one variable x, whose coefficients are definable functions of y. If the coefficients can be taken to be *rational* functions of y (piecewise in y), we say that the theory is *algebraically bounded.*

In certain situations, it is possible to reduce all other quantifiers to bounded quantifiers. The idea is due to Ax, in the setting of pseudo-finite fields. We need to assume that definable sets of $T_!$ decompose into finite ones and *irreducible* ones, and the irreducible ones carry definable types, given uniformly in the parameters.

For definiteness, we will just consider strongly minimal irreducible sets.

Let us assume a family Φ of formulas $\phi(x,y)$ of $L_!$ is given, where x, y are tuples of variables. (In practice these will be the absolutely irreducible affine curves.) We will write $D \in \Phi(M)$ if $D = \{x : \phi(x,b)\}$ for some b from M. Assume, in any model $M \models T$ and $D \in \Phi(M)$:

2.3. **Properties of irreducible definable sets of $L_!$.**

1. (algebraic boundedness) If $F = \{x \in D : \phi(x,c)\}$ is finite, then for some $\psi(x,y) \in L_!$, $\psi(x,c)$ is finite and contains F.
2. D is strongly minimal in $T_!$. I.e. for $\phi \in L_!$, $\{x \in D : \phi(x,c)\}$is finite or cofinite.
3. (Density of Φ). Let $M \leq N \models T_!$, $M \neq N$. Then there exists $N' \leq N$, $M \leq N'$, $M \neq N'$, such that for any $c_1, \ldots, c_k \in N'$ there exists $D \in \Phi(M)$ with $(c_1, \ldots, c_k) \in D$.

From (1),(2) it follows that for $\phi(x,y) \in \Phi$ as above, $(\exists^\infty x)\psi(x,y,u) \& \phi(x,y)$ is a *definable* property of (y,u) (necessarily equivalent, for some n, to $(\exists^{>n} x)\psi(x,y,u) \& \phi(x,y)$.)

We can now formulate the final version of the Boolean-valued theory; we assume now that the equality symbol lies in $L_!$.

2.4. **Axioms of $T^*_{bool,\infty}$.**

1. B is a Boolean algebra.
2. If $T \models (\forall x)\phi$, then $[\phi] = 1$.
3. If $\phi \in L_!$, then $[\phi] = 0 \bigvee [\phi] = 1$.
4. For any a, $\phi \mapsto [\phi](a)$ is a Boolean homomorphism.
5. (Limit at ∞) $[\neg\phi] \in I$ for all quantifier-free ϕ such that $T_\infty \vdash \phi$
6. Let ψ be a quantifier-free formula of $L_!$ such that $(\forall y)(\exists x)\psi \in T$. Then $(\forall y)(\exists x)[\phi(x,y)] = 1$ is an axiom of T_{bool}.
7. (local-global) Let $\phi(x,y) \in \Phi$. Assume, for $i = 1, \ldots, n$:

   $$T \vdash \theta_i(y,u) \implies (\exists^\infty x)\phi(x,y) \& \psi_i(x,y,u)$$

   Then the universal closure of the formula:

   $$\bigwedge_{i \neq j} b_i \cap b_j = 0 \& \bigwedge [\theta_i(y,u)] \geq b_i \implies (\exists x) \bigwedge_i [\phi(x,y) \& \psi_i(x,y,u)] \geq b_i$$

is an axiom of $T^*_{bool,\infty}$.

Here (1-5) are universal axioms. (6) can be restricted to say that the restriction to $L_!$ is algebraically closed. Any model (M, B) of (1-5) can be extended - with the same Boolean algebra part! - to a model where (5) is true, by extending the restriction $M_!$ to $L_!$ to an algebraically closed structure $N_!$ in the sense of $T_!$, and then extending each expansion M_x of $M_!$ to an expansion N_x of $N_!$ in some way. Also, (M, B) can be extended, again without changing B, to a model of (1-5) where a given instance of (7) holds. Namely, let $\phi(x, y) \in \Phi$, and let $D = \phi(x, a)$ for some $a \in M$. Let $b_1, \dots, b_n$ be a given partition of B, let d be a parameter (for u). Extend $M_!$ to $N_! = M_!(c)$ by adding a generic element of D (recall D is strongly minimal when restricted to $L_!$.) Then for $x \in X$ with $x \in b_i$, expand $N_!$ to an extension of M_x in such a way that $\psi_i(c, a, d)$ holds. This shows that $T^*_{bool,\infty}$ is true in any existentially closed model of (1-5).

Proposition 2.5. *$T^*_{bool,\infty}$ admits QE to the level of bounded quantifiers.*

Proof. By 2.3 (3), it suffices to eliminate quantifiers $(\exists x)\psi(x, y)$ where $\psi(x, y)$ implies $\phi(x, y)$ for some $\phi \in \Phi$. Fix a, d, let $D = \{x : \phi(x, a)\}$. Let $b_1, \dots, b_n$ be a given partition of B. Let $\psi_i(x, a, d)$ be a formula implying $\phi(x, a)$. We have to show that in a model (M, B) of T^*_{bool}, we can tell, based on the bounded-quantifier type of (a, d) alone, whether there exists x with $[\psi_i(x, a, d)] \geq b_i$. Let θ be a qf formula of T equivalent to $(\exists^\infty x)\psi$. If for each i, $[\theta(a, d)] \geq b_i$, then such an x exists by axiom (6). Otherwise for some i, $[\neg\theta(a, d)] \cap b_i = b > 0$. So in M_x (for $x \in b$), there are finitely many solutions $c_1, \dots, c_k$ to $\psi_i(x, a, d)$. Then there exists x with $\bigwedge[\psi_i(x, a, d)] \geq b_i$ iff one of these c_i is a solution of the same. This can be checked using bounded quantifiers.

□

3. The algebraic integers

We present the theory of the algebraic integers as a Boolean-valued theory of valued fields, namely the Booleanization of $ACVF_0$ with $ACVF_{0,0}$ at ∞, over an atomless pointed Boolean algebra.

This description is inspired by [2]; see [3], [1] for other presentations.

Theorem 3.1. *The theory of non-trivially valued algebraically closed valued fields admits quantifier-elimination in the language of fields, with a map v into a model of DOA.*

This was proved by A. Robinson in the pure field language; the above version is easily deduced, cf. [].

Proposition 3.2. *Let R be the ring of algebraic integers, $U = G_m(R)$ the units of R; for $a, b \in \bar{\mathbb{Q}}$, define $a \leq b$ iff $a^{-1}b \in R$; then $Th(K^*/U) = BDOA_\infty$.*

Proof. For a number field K, let $\underline{\Gamma}_K$ be the group of maps with finite support: $\Omega_K^{fin} \to \mathbb{Q}$. We have a natural map $K^* \to \underline{\Gamma}_K$. The quotient $\underline{\Gamma}_K/K^*$ is a *torsion group.* [1] At the limit we obtain a map $\bar{\mathbb{Q}}^* = \lim_K K^* \to \lim_K \underline{\Gamma}_K$. Now $\underline{\Gamma}$ is torsion-free; but $Im(\bar{\mathbb{Q}}^*)$ is divisible; so $\underline{\Gamma}_K/(Im(\bar{\mathbb{Q}}^*) \cap \underline{\Gamma}_K)$ is divisible; as it is also finite, it must be trivial, i.e. $\underline{\Gamma} \subset Im(\bar{\mathbb{Q}}^*)$. Thus the map $\bar{\mathbb{Q}}^* \to \underline{\Gamma}_K$ is surjective; it has kernel U. So $\bar{\mathbb{Q}}^*/U \cong \lim_K \underline{\Gamma}_K$. Now $\lim_K \underline{\Gamma}_K$ can be identified with the group of continuous maps with compact support $\Omega_{\bar{\mathbb{Q}},fin} \to \mathbb{Q}$. □

Let $T = ACVF0$ be the theory of nontrivially valued algebraically closed valued fields of characteristic 0. Let $T_\infty = TVF0$ be the theory of trivially valued fields of char. 0. The language is the language of valued fields, and the sublanguage $L_!$ is the language of fields (or rings), so that $T_! = ACF0$.

By Proposition 2.5, ${T^*}_{bool,\infty}$ is complete up to existential sentences. Let T^*_{max} be tT^*_{bool} along with the sentences asserting that all valuations of number fields are Booleanly possible: $[v(p) > 0] > 0$, $p = 2, 3, \ldots$, and more generally, for any irreducible polynomial $F(x)$ over $\mathbb{Z}$ whose leading coefficient is an integer > 1, $(\exists x)([F(x) = 0 \& v(x) > 0] > 0)$.

Let VAL be the space of all valuations v of $\bar{\mathbb{Q}}$ lying above a standard v_p of $\mathbb{Q}$, or the trivial valuation v_{triv}. A basic open set has the form $\{v : v(a) > v(b)\}$, or $\{v : v(a) = v(b)\}$, where $a, b \in \bar{\mathbb{Q}}$. [2] So $\bar{\mathbb{Q}}_v$, the field $\bar{\mathbb{Q}}$ with this valuation, is a model of ACVF. Above the trivial valuation of $\mathbb{Q}$ we have a unique point $\infty \in VAL$. Let B be the Boolean algebra of clopen subsets of VAL; let I be the maximal ideal corresponding to the point ∞. For a quantifier-free ϕ, define:

$$[\phi] = \{v \in VAL : \bar{\mathbb{Q}}_v \models \phi\}$$

Lemma 3.3. *$[\phi]$ is a clopen subset of VAL.*

We will refer to this structure as $\bar{\mathbb{Q}}$.

Theorem 3.4. *$\bar{\mathbb{Q}} \models \widetilde{T^*}_{bool,\infty}$, and so T^*_{max}.*

Axioms (1),(2),(3),(4),(5), (6) are clear. (7) follows from Proposition **??** and *Rumely's local-global principle*:

Let $C \subset \mathbb{A}_n$ be an irreducible curve over K If for all v there exists $c_v = (c_1, \ldots, c_n) \in C(K_v))$ with $v(c_i) \geq 0$ then there exists $c \in C$ such that for all v, $v(c_i) \geq 0$

The truth of this in $\bar{\mathbb{Q}}$ is due to Rumely, with further proofs by Szpiro, Moret-Bailly, Green-Pop-Roquette. (The treatment here directly requires the principle only for curves, but it can be stated for higher-dimensional varieties.)

Proposition 3.5 ([2])**.** *$Th(\widetilde{\mathbb{Z}})$ is bi-interpretable with $Th(\bar{\mathbb{Q}})$*

[1] This is a basic theorem of algebraic number theory, whose proof is global and will be discussed later.

[2] This is not the topology we will use when we move to real-valued logic!

3.6. **Interpretation of $\widetilde{\mathbb{Z}}$.** $\mathcal{O} = \{x : [V(x) \geq 0] = 1\}$.

3.7. **Interpretation of T in $\widetilde{\mathbb{Z}}$.** The field K is the field of fractions of $\widetilde{\mathbb{Z}}$, interpretable in the usual way.

For $x \in \widetilde{\mathbb{Z}}$, let $J(x)$ be the *radical ideal* $\sqrt{\widetilde{\mathbb{Z}}x}$ generated by x. Any quotient of $\widetilde{\mathbb{Z}}$ by a nonzero prime ideals is a *locally finite* integral domain (a finite extension of a finite field), hence it is a field. Thus the radical ideal generated by x equals the the *Jacboson radical*, i.e. the intersection of all maximal ideals containing x; it can be defined as $y \in J(x) \iff \widetilde{\mathbb{Z}} \models (\forall r)(\exists y)(1 = y(1 - rx))\}$.

Define an equivalence relation on $\widetilde{\mathbb{Z}}$: xEy iff $J(x) = J(y)$. We can view the quotient, the set I of radical ideals of $\widetilde{\mathbb{Z}}$, as an imaginary sort.

We define operations $\cup, \cap$ on I: $A \cup B = \sqrt{(AB)}$, $A \cap B = \sqrt{A + B}$.

(We saw earlier another way of interpreting the Boolean algebra, in $\underline{\Gamma}$.)

We remark that there is no difficulty extending $T^*_{bool,\infty}$ so as to include archimedean absolute values, with a similar model companion. However, $\mathbb{Q}^a$ is not a model; and more seriously, the model companion remains purely local, carrying no global constraints or information.

4. Undecidability

Assume we have a first order structure where all valuations and absolute values can be discussed. In particular we can define

$$M = \{x : (\forall v) v(x) \geq 0\}$$

$$R = \{x : (\forall v) v(2) \geq 0 \implies v(x) \geq 0\}$$

The interpretation in $\mathbb{Q}^a$ of M, R is: roots of unity, algebraic integers.

Proposition 4.1. *Let $K = \mathbb{Q}^a$, viewed as a Boolean valued field-with-absolute-valued, with respect to all valuations and absolute values. Then K is undecidable. In fact $\mathbb{N}$ is a definable subset of K.*

The proof is an adaptation of Julia's Robinson undecidability theorem for the totally real algebraic integers. Before beginning the proof, recall that the *archimedean* absolute values of $\bar{\mathbb{Q}}$ have the form $|x| = |\sigma(x)|_{\mathbb{C}}$ where $\sigma : \bar{\mathbb{Q}} \to \mathbb{Q}$ is an automorphism , and $|\cdot|_{\mathbb{C}}$ is the usual complex absolute value. Indeed if $|\cdot|$ is an archimedean absolute value, then the *completion* is a complete normed field, and must be isomorphic to $\mathbb{C}$. Hence $|x| = |\sigma(x)|_{\mathbb{C}}$ where $\sigma : \bar{\mathbb{Q}} \to \mathbb{C}$ is an embedding , and $|\cdot|_{\mathbb{C}}$ is the usual complex absolute value. Viewing $\bar{\mathbb{Q}}$ as a subfield of $\mathbb{C}$, we have $\sigma(\bar{\mathbb{Q}}) = \bar{\mathbb{Q}}$, i.e. σ is an automorphism of $\bar{\mathbb{Q}}$.

We will also use that if $a \in R$, then $|a| \geq 1$ for some archimedean $|\cdot|$. Indeed otherwise, $v(a) \geq 0$ for all v, so by product formula $v(a) = 0$ for all v, in particular $|a| = 1$ for all (hence some) archimedean $|\cdot|$.

Proof. **Claim .** There exists a uniformly definable family of finite subsets of M, containing arbitrarily large finite sets.

Proof. Let $S = \{x \in K : (\forall v)(|2|_v > 1 \implies |x|_v > 1)\}$. This is the set of algebraic numbers a such that $|a| > 1$ for every *archimedean* absolute value of $\bar{\mathbb{Q}}$. Thus $x \in S$ iff $|\sigma(x)|_{\mathbb{C}} > 1$ for all Galois conjugates $\sigma(x)$ of x. In particular, $\{2, 3, 4, \ldots\} \subset S$. Let $\mu(x)$ be the minimal value of $|\sigma(x)|_{\mathbb{C}}$ over the finitely many Galois conjugates of x; then $\mu(x) > 1$ for $x \in S$.

For $s \in S$, let $M(s) = \{x \in M : (\forall v)(v(x-1) \geq v(1/s))\}$.

For archimedean v, the condition $(v(x-1) \geq v(1/s))$ holds for all $x \in M$ away from a ball around 1, of radius $|1/s|_v$. If $a \in M$, then a is a primitive d'th root of 1 for some $d > 1$; the Galois conjugates of a are the primitive d'th roots of 1; if the condition holds for *all* archimedean v, then every Galois conjugate of a lies outside the ball around 1 of radius $1/\mu(s)$; in particular, $exp(2\pi i/d)$ lies outside this ball; clearly this is the case for only finitely many d. Hence $M(s)$ is finite.

Consider integers $m > 1$. We have $m \in S$. For non-archimedian v, we have $v(x-1) \geq 0 = v(1/m)$ so the condition $(v(x-1) \geq v(1/s))$ is satisfied for all $x \in M$. For archimedean v, it holds for all $x \in M$ away from a ball around 1, of radius $|1/m|$. So $\cup_m M(m) = M$. □

Let $\alpha_1, \ldots, \alpha_k$ be distinct elements of M. Let $m = 4kN(\Pi_{i<j\leq k}(\alpha_i - \alpha_j))$. Here N is the norm to $\mathbb{Q}$. So $m \in \mathbb{Z}$, $m > 4k$, and the elements $1 + m\alpha_i$ are relatively prime in R.

By the Chinese remainder theorem there exists $t \in R$ with

$$t = i \quad mod \quad 1 + m\alpha_i$$

Note that i is the unique element with $t = i\ mod\ (1 + m\alpha_i)$ and $3|i| \leq |m|$ a.e. Indeed suppose $t = i' \mod (1+m\alpha_i)$ and $3|i'| \leq |m|$ a.e.. Then $i - i' = a(1+m\alpha_i)$ for some $a \in R$; we can choose an archimedean absolute value with $|a| \geq 1$; then $|i - i'| \geq |1 + m\alpha_i| \geq m - 1$, a contradiction.

This shows that the finite set $\{1, \ldots, k\}$ form part of a uniformly definable family of sets F, each in definable bijection with some set $M(s)$, $s \in S$ - hence itself finite. So $a \in \mathbb{N}$ iff for all $w \in F$, c, if $0 \in w$ and $(\forall x)(x \in w \implies x + 1 \in w \vee x = c\})$, then $a \in w$.

□

4.2. Let K be a field with a family of non-archimedean valuations. Define: $k = \{x : [v(x) \geq 0] = 1\}$.

k is a subring of K.

In the presence of any version of the product formula, $v(x) \geq 0$ implies $v(x) = 0$ so $v(x^{-1}) = 0$. Thus k is a *subfield* of K.

4.3. **The function field case.** Let F be any field. We will see that in the integral closure of $F[t]$ in $F(t)^{alg}$ - and with a predicate for F - we can uniformly define finite subsets of F. Moreover, this will not be improved in a model companion.

Let M be a field with additional structure, containing a field F and a transcendental element t, and allowing discussion of "all F-valuations".

We can define the *constant* ring C by the formula:

$$(\forall v)(v(x) \geq 0)$$

This formula defines a subring of M. In the presence of the product formula (and this will be our only use of it here), $0 \notin x \in C$ implies: $(\forall v)(v(x) = 0)$; and so $x^{-1}C$. Thus $C = k$ is a field, containing F.

We can also define a ring R (whose $k(t)^{alg}$-points form the integral closure of $k[t]$):

$$(\forall v)(v(t) \geq 0 \implies v(x) \geq 0)$$

Note that $t \in R \setminus C$. Thus for some v, $v(t) < 0$. So $v(t-\alpha) < 0$ for any $\alpha \in k$. Hence $t - \alpha$ is not invertible in R.

Lemma 4.4. *Let R be an integral domain, k an infinite subfield, $t \in R$ such that $t - \alpha$ is not invertible for $\alpha \in k$. Then $(R, k, +, \cdot)$ is undecidable.*

Proof. Given $r \in R$, let $Z(r) = \{\alpha \in k : r \in (t-\alpha)R\}$. Let $f \in k[t]$ be a polynomial. If $f \in (t-\alpha)R$ and $f, (t-\alpha)$ are relatively prime in $k[t]$, $af + b(t-\alpha) = 1$, then $1 \in (t-\alpha)R$, contradicting the assumption. Thus $Z(f)$ is the set of roots of f in k. Hence $\{Z(r) : r \in R\}$ is a uniformly definable family F of sets including all finite subset of k.

If k contains $\mathbb{Z}$, one easily sees that $\mathbb{N}$ is definable in R. In general, by saturating, we may assume k has algebraically independent element a, b, b'. Let $C_n = \{1, a, \ldots, a^n\}$; let $D_n = \{x + by + b'z : x, y, z \in C_n\}$; let PD_n be the set of all subsets of D_n. Let E_n be the structure (C_n, D_n, PD_n), with the partial 'successor' function $x \mapsto ax$ on C_n, the 'membership' relation on $D_n \times PD_n$, and the graph of $x + by + b'z$ on $C_n^3 \times D_n$. Note that $x + by + b'z$ is injective on C_n^3, so identifies D_n with C_n^3. With parameters a, b, b', t, we have a uniformly definable family of structures, including all structures E_n. Taking the union over all a, b, b', t we obtain a uniformly definable family of structures F including all the E_n.

Now it is clear that E_n interprets truncated arithmetic. One can find a sentence σ true in the structures E_n, whose logical consequences are recursively inseparable from the set of their negations. But $\{\phi : (\forall A \in F)(A \models \sigma \implies A \models \phi)$ separates them. Thus $Th((R, k, +, \cdot))$ cannot be decidable. □

4.5. What if we take the space of valuations as a sort with individual elements? We immediately see that $\mathbb{Q}$ is definable, as $\{x : (\forall v, v')(v(x) = v'(x)\}$. From a different angle, while questions using *all* valuations are meaningful, a specific choice of finitely many valuations can be quite arbitrary; for instance, while the isomorphism type of $(\mathbb{Q}^a, v)$ for *one* valuation v of $\mathbb{Q}^a$ is uniquely determined by $v|\mathbb{Q}$, specifying a *second* valuation v' involves a large number of arbitrary choices, e.g. when $v|\mathbb{Q} = v'|\mathbb{Q} = v_\infty$, the choice of primes q such that $\sqrt{q}$ has the same sign under the complex embeddings corresponding to v, v'.

Problem 4.6. It is not known if the theory of the integral closure of $\mathbb{C}[t]$ in $\mathbb{C}(t)^{alg}$ is decidable. [3] Let us show the first place that behaves differently. Let $K = \mathbb{C}(t)^{alg}$. Let v_α be the valuation of $\mathbb{C}(t)$ at $\alpha \in \mathbb{C}$. Let X be the space of valuations of $\mathbb{C}(t)^a$ lying above some v_α (but not above v_∞!). View K as a Boolean-valued expansion of the theory of fields, as above; $[\phi] = \{v \in X : K_v \models \phi$. Define $\underline{\Gamma}$ as above to be the group of continuous maps with compact support from X into $\mathbb{Q}$. Then $\underline{\Gamma}$ is interpretable; each element of $\underline{\Gamma}$ can be written as a difference of two terms $v(c)^+$. Now as before, the theory of $\underline{\Gamma}$ is just $DOA_{bool,triv}$. But the image of $v : K^* \to \underline{\Gamma}$ is *not* surjective now. The quotient is a quotient of the projective limit of all groups $\mathbb{Q} \otimes J(C)$, with J the Jacobian of C, C running through all curves over $\mathbb{C}$. The quotient factors through the projective limit of all groups $\mathbb{Q} \otimes J(C)$, with J the Jacobian of C, C running through a projective system of 'all' curves over $\mathbb{C}$, covering $\mathbb{P}^1(\mathbb{C})$; it is essentially the quotient of the latter by the subgroup of elements supported above the point $\infty \in \mathbb{P}^1$.

(see [3].) This leads to:

Problem 4.7. Study the theory of $(\underline{\Gamma}, +, \max, v(K^*))$ in the language of partially ordered Abelian groups with distinguished subgroup.

References

[1] A. Prestel, J. Schmid "Existentially closed domains with radical relations" J. Reine Angew. Math. , 407 (1990) pp. 178-201

[2] L. van den Dries, "Elimination theory for the ring of algebraic integers" J. Reine Angew. Math. , 388 (1988), pp. 189-205

[3] L. van den Dries, A. Macintyre, "The logic of Rumely's local-global principle" J. Reine Angew. Math. , 407 (1990) pp. 33-56

[3] (Feb. 2016) It is undecidable.