THE JOURNAL OF SYMBOLIC LOGIC
Volume 38, Number 1, March 1973

THE UNDECIDABILITY OF INTUITIONISTIC THEORIES OF ALGEBRAICALLY CLOSED FIELDS AND REAL CLOSED FIELDS

DOV M. GABBAY

§0. Introduction. Let T be a set of axioms for a classical theory T^C (e.g. abelian groups, linear order, unary function, algebraically closed fields, etc.). Suppose we regard T as a set of axioms for an intuitionistic theory T^H (more precisely, we regard T as axioms in Heyting's predicate calculus HPC).

Question. Is T^H decidable (or, more generally, if X is any intermediate logic, is T^X decidable)? In [1] we gave sufficient conditions for the undecidability of T^H. These conditions depend on the formulas of T (different axiomatization of the same T^C may give rise to different T^H) and on the classical model theoretic properties of T^C (the method did not work for model complete theories, e.g. those of the title of the paper). For details see [1]. In [2] we gave some decidability results for some theories: The problem of the decidability of theories T^H for a classically model complete T^C remained open. An undecidability result in this direction, for dense linear order was obtained by Smorynski [4]. The cases of algebraically closed fields and real closed fields and divisible abelian groups are treated in this paper. Other various decidability results of the intuitionistic theories were obtained by several authors, see [1], [2], [4] for details.

One more remark before we start. There are several possible formulations for an intuitionistic theory of, e.g. fields, that correspond to several possible axiomatizations of the classical theory. Other formulations may be given in terms of the apartness relation, such as the one for fields given by Heyting [5]. The formulations that we consider here are of interest as these systems occur in intuitionistic mathematics.[1] We hope that the present methods could be extended to the (more interesting) case of Heyting's systems [5].

§1. Algebraically closed fields.

(1) First formulation is in a language with $+$, $\cdot$, 0, 1 and $=$.

(a) Axioms in AE form saying that $+$ is a commutative group.

(b) $x(yz) = (xy)z$, $x(y + z) = xy + xz$, $xy = yx$.

(c) $\forall x \exists y(x = 0 \vee xy = 1)$.

(d) $0 \neq 1$.

(e) Equality axioms in, "$x = x$, $x = y \to y = x$, $x = y \wedge y = z \to x = z$."

(f) For each $n \geq 0$, the following axiom holds:

$$(\forall x_0 \cdots x_n)\exists z \left(\sum_{i=0}^{n} x_i z^i + z^{n+1} = 0\right).$$

Received January 21, 1972, revised April 10, 1972.

[1] I am grateful to Professor Kreisel for helpful criticism.

The system F_1 of the first formulation is decidable.

(2) The second formulation is in the same language as the first with the axiom (c′) replacing axiom (c) and the other axioms remaining unchanged.

(c′) $\forall x(x \neq 0 \rightarrow \exists y(x \cdot y = 1))$.

The system F_2 of this formulation is undecidable.

THEOREM A. *The system F_1 of the first formulation is decidable.*

PROOF. To prove this first observe the following:

(3) $F_1 \vdash_{\mathrm{HPC}} \forall xy(x = y \vee x \neq y)$, and use the following theorem:

THEOREM M (ESSENTIALLY IN [4]). *Let T be a set of axioms for a classical theory T^C, written in the form $(Q \cdots) \bigwedge (\bigwedge A_i \rightarrow \bigvee B_j)$ where $(Q \cdots)$ is a string of quantifiers and A_i, B_j are atomic. Then T is classically model complete iff the following holds for any formula ϕ. $T_1 \vdash$ intuitionistically ϕ iff $T \vdash$ classically ϕ where $T_1 = T \cup \{(\text{universal closure})\ (A \vee -A) \mid A \text{ atomic}\}$.*

Observation (3) and Theorem M show that F_1 is the same as the classical theory of algebraically closed fields.

THEOREM B. *The system F_2 of the second formulation is undecidable, in fact, a finite extension of it with the axioms*

$$- -(x = y) \rightarrow x = y \quad \textit{and} \quad \forall x \exists y(x \neq 0 \rightarrow xy = 1)$$

is undecidable.

PROOF. Call this extension F. Towards showing that F is undecidable we need various definitions, lemmas and constructions. Our purpose is to faithfully interpret in F the classically undecidable theory of a reflexive and symmetric relation with at least five elements. The proof of faithfulness shall use Kripke models. So let us start with definitions. This method is due to Rabin-Scott [6].

We assume familiarity with Kripke models and semantics (see [3]). A Kripke model is denoted by $(\mathbf{S}, \mathbf{R}, \mathbf{0}, \mathbf{A}_t)$, $\mathbf{0} \in \mathbf{S}$, $t \in \mathbf{S}$, where $\mathbf{S}$ is the set of possible worlds, $\mathbf{R}$ is the reflexive and transitive accessibility relation, $\mathbf{0}$ is the base (actual) world and $\mathbf{A}_t$, for $t \in \mathbf{S}$, is the classical model (of the given language) associated with t, A_t denotes the domain of $\mathbf{A}_t$. The truth value of a formula $\phi(a_1, \cdots, a_n)$ at a point $t \in \mathbf{S}$, under the indicated assignment $a_i \in A_t$, is denoted by $[\phi(a_1, \cdots, a_n)]_t$.

Construction (4). Let $(M, <)$ be a model of a reflexive and symmetric relation $<$. Let us assume that $\overline{\overline{M}} > 4$. We construct a Kripke model called the Kripke model *associated* with $(M, <)$. Let

$$\begin{aligned} \mathbf{S}_0 &= \{\{x, y\} \mid -(x < y), x, y \text{ in } M\}, \\ \mathbf{S} &= \{\mathbf{0}\} \cup \mathbf{S}_0 \cup M, \\ \mathbf{R} &= \{\mathbf{0}\} \times \mathbf{S} \cup \{(x, x) \mid x \in \mathbf{S}\} \cup \{(\{x, y\}, x) \mid \{x, y\} \in \mathbf{S}_0\}. \end{aligned}$$

Let $A_t = K^M$, where K is some *fixed* algebraically closed field. Define $+$, $\cdot$ on K^M to be *pointwise* for all $t \in \mathbf{S}$. Let $\bar{0} \in A_t$ be the vector with $0 \in K$ in all coordinates and let $\bar{1}$ be the constant vector $1 \in K$. Define $=$ on A_t as follows: For $f, g \in K^M$ let $[f = g]_{\mathbf{0}} = 1$ iff $\forall m \in M(f(m) = g(m))$. Let $[f = g]_{\{x,y\}} = 1$ iff $f(x) = g(x)$ and $f(y) = g(y)$. Let $[f = g]_x = 1$ iff $f(x) = g(x)$.

LEMMA 5. *The model $(\mathbf{S}, \mathbf{R}, \mathbf{0}, \mathbf{A}_t)$ thus defined is a model of the system F_2.*

PROOF. Axioms (a), (b), (e) and (f) hold because $+$ and $\cdot$ were defined pointwise. $\bar{0} \neq \bar{1}$ holds by definition of $=$. To show that (c′) holds notice that $[f \neq \bar{0}]_{\mathbf{0}} = 1$

iff $\forall m \in M(f(m) \neq 0)$ and $[f \neq \bar{0}]_{\{x,y\}} = 1$ iff both $f(x), f(y) \neq 0$, and so the following g can serve as inverse.

$$g(m) = 0 \qquad \text{if } f(m) = 0,$$
$$= f(m)^{-1} \quad \text{if } f(m) \neq 0.$$

The reader can also verify if $[f = g]_{\mathbf{0}} = 0$, then, for some $m \in M, f(m) \neq g(m)$ and so $[f = g]_m = 0$, which means that $[- -(f = g)]_{\mathbf{0}} = 0$. Similar verification for $t = \{m, n\}$ shows that $\forall xy(- -x = y \rightarrow x = y)$ must hold at $\mathbf{0}$.

Now consider the following formulas:

$$\text{(6)} \quad E =_{\text{def}} (\forall x, u_1, u_2, u_3)\left[\left(x^2 = x \wedge \bigwedge_{i=1}^{3} u_i^2 = u_i \wedge u_1 + u_2 + u_3 = x\right) \rightarrow \left(\bigvee_{i \neq j} (u_i + u_j = x)\right)\right].$$

$$\text{(7)} \quad \begin{aligned} D(x) =_{\text{def}} \langle x^2 = x \wedge (\forall u, v)[(u^2 = u \wedge v^2 = v \wedge u + v = x) \\ \rightarrow (x = \bar{0} \vee (u = \bar{0} \wedge v = x) \\ \vee (u = x \wedge v = \bar{0}))]\rangle \\ \rightarrow \langle x = \bar{0} \vee x = \bar{1} \vee E\rangle. \end{aligned}$$

Let $M_0 \subseteq K^M$ be the set of all $f \in K^M$ such that, for some $m \in M$, we have $f = f_m$, with

$$f_m(n) = 1 \in K \quad \text{if } n = m,$$
$$= 0 \in K \quad \text{otherwise.}$$

LEMMA 8. (1) $[E]_t = 0$ *iff* $t = \mathbf{0}$.
(2) $[D(f)]_{\mathbf{0}} = 0$ *iff* $f \in M_0$.

PROOF. (1) is easy to see; recall that $\bar{\bar{M}} \geq 5$.

(2) If $f \in M_0$, then at $\mathbf{0}$, the antecedent of $D(f)$ is true and the consequent is false. If $f \notin M_0$, then let us show that $D(f)$ holds. Since E is false only at $\mathbf{0}$, we have to check whether the antecedent can be true at $\mathbf{0}$ and the consequent false. If $x = \bar{0}$ does not hold, then there must be $m \in M$ such that $f(m) \neq 0$. $f(m)$ must be 1 since if $f(m) \neq 1$ then $f^2 = f$ would not hold. Since $f(m) = 1$ and $f \notin M_0$, there must be some $n \neq m$ such that $f(n) \neq 0$ and hence $f(n) = 1$. But then take u and v to be f_m and f_n and then the antecedent will not hold. Thus if $f \notin M_0$, $D(f)$ must hold at $\mathbf{0}$.

Define $\rho(u, v)$ by

$$\text{(9)} \qquad \rho(u, v) =_{\text{def}} [E \wedge (u + v = \bar{1}) \rightarrow u = \bar{1} \vee v = \bar{1}].$$

LEMMA 10. *For* $f_a, f_b \in M_0$, *we have*

$$[\rho(f_a, f_b)]_{\mathbf{0}} = 1 \quad \textit{iff } a < b.$$

PROOF. By construction.

Now let S be a statement of the theory of a reflexive and symmetric relation $<$. S can be written in the form

$$(Q \cdots) \bigwedge (\bigwedge x_i < y_i \rightarrow \bigvee u_j < v_j),$$

where $(Q \cdots)$ is a string of quantifiers. We want to associate with S a statement S^* in the theory F of fields, as follows.

Let $\forall^* x\phi$ and $\exists^* x\phi$ denote, for any formula ϕ, the formulas $\forall x(Dx \vee \phi)$ and $\exists x(\phi \wedge (Dx \to E))$ respectively. Let S^* be the following formula:

$$(\forall u_1, \cdots, u_5)\Big\langle\Big[\forall x(Dx \vee \rho(x, x)) \wedge (Q^* \cdots) \bigwedge (\bigwedge \rho(x_i, y_i) \to \bigvee \rho(u_j, v_j) \vee E)\Big] \to \Big[E \vee \bigvee_{i=1}^{5} D(u_i) \vee \bigvee_{1 \le i \ne j \le 5} u_i = u_j\Big]\Big\rangle,$$

where $(Q^* \cdots)$ is the same string $(Q \cdots)$ of quantifiers with * added to them and interpreted as indicated above.

LEMMA 11. *Let* RS *be the theory of a reflexive and symmetric relation with at least 5 elements. Then*

$$\mathrm{RS} \vdash -S \quad \textit{iff}\ F \vdash S^*.$$

PROOF. Assume that there exists a model $(\mathbf{S}, \mathbf{R}, \mathbf{0}\ \mathbf{A}_t)$ where S^* is false. Then there exists a $t \in \mathbf{S}$ and $u_i \in A_t$ such that the antecedent of the main implication of S^* holds and the consequent does not hold.

Define a model $(M_0, <)$ where S holds as follows:

(12) Let $M_0 = \{a \in A_t \mid [D(a)]_t = 0\}$.

(13) Let $a < b$ iff $[\rho(a, b)]_t = 1$.

Clearly, since $[\forall x(Dx \vee \rho(x, x))]_t = 1$ we get that $<$ is reflexive and looking at ρ we see that $<$ is symmetric. We also have $[S_1^*]_t = 1$ where

$$S_1^* = (Q^* \cdots) \bigwedge (\bigwedge \rho(x_i, y_i) \to \bigvee \rho\, (u_j, v_j)).$$

We claim that S holds at $(M_0, <)$. This follows from the following:

LEMMA 14. *Let* $\psi = \bigwedge (\bigwedge x_i < y_i \to \bigvee u_j < v_j)$ *and let*

$$\psi^* = \bigwedge (\bigwedge \rho(x_i, y_i) \to (\bigvee \rho\, (u_j, v_j) \vee E)).$$

Further let $(Q^* \cdots) = (Q_1^* \cdots)(Q_2^* \cdots)$. *Then for any substitution of elements* a_i *of* M_0 *for the variables of* Q_1^* *we have that* $[(Q_2^* \cdots)\psi^*(a_i)]_t = 1$ *iff* $(Q_2 \cdots)\psi(a_i)$ *holds in* $(M_0, <)$.

PROOF. By induction.

From Lemma 14 we deduce that $(M_0, <)$ is a model of S.

Now to prove the other direction of Lemma 11 assume that S has a model $(M, <)$. We assume that $\overline{\overline{M}} \ge 5$. Construct the model $(\mathbf{S}, \mathbf{R}, \mathbf{0}, \mathbf{A}_t)$ associated with $(M, <)$. We claim

(15) $$[S^*)_0 = 0.$$

In fact, for any five different $u_i \in M_0 \subseteq K^M$, the antecedent of S^* holds and the consequent is false. Clearly $[E]_0 = 0$ and $[\forall x(D(x) \vee \rho(x, x))]_0 = 1$, as we have verified in the course of the construction. Also since $[D(f)]_0 = 0$ iff $f \in M_0$ and since $[\rho(f_a, f_b)]_0 = 1$ iff $a < b$ then Lemma 14 holds and therefore $[S_1^*] = 1$. Thus (15) is proved.

§2. Real closed fields.

(16) The language of the first formulation contains the symbols $+, \cdot, 0, 1, =$ and the unary predicate $P(x)$. The axioms are axioms (a)–(e) of (1) along with the following axioms:

(g) $P(x) \wedge P(y) \to P(x + y)$, $x + y = 0 \to -(P(x) \wedge P(y))$, $P(x) \wedge P(y) \to P(xy)$.

(h) $\forall x \forall y \exists z(x+y=0 \to x=z^2 \vee y=z^2)$, $(\forall x_0, x_1, \cdots, x_{2n})\exists y(\Sigma x_i y^i + y^{2n+1} = 0)$.
(k) $x + y = 0 \to x = 0 \vee P(x) \vee P(y)$.

(17) The language of the second formulation is the same as before. The axioms are (a), (b), (c′), (d), (e), (g), (h), and (k′) where

$$\text{(k}'\text{)} \qquad x + y = 0 \wedge -P(x) \wedge -P(y) \to x = 0.$$

THEOREM C. *The system of the first formulation is decidable.*

PROOF. Observe that the formulas $\forall xy(x = y \vee x \neq y)$ and $\forall x(Px \vee -Px)$ are theorems of this formulation and use Theorem M. Actually this system is equal to the classical theory.

THEOREM D. *The system of the second formulation is undecidable, in fact, a finite extension G of it, with the axiom* $- -(x = y) \to (x = y)$ *and* $\forall x \exists y(x \neq 0 \to xy = 1)$ *is undecidable.*

PROOF. We use the same interpretation that we used in the proof of Theorem B. Let $(M, <)$ be a model of a reflexive and symmetric relation. Let K be a real closed field. Define the associated Kripke model as before. We have to define the additional predicate P in the model. Let $[P(f)]_0 = 1$ iff $\forall m P(f(m))$ holds in K. Let $[P(f)]_{\{m,n\}} = 1$ iff $P(f(m)) \wedge P(f(n))$ holds in K. Let $[P(f)]_m = 1$ iff $P(f(m))$ holds in K. We now have to verify that axioms (g), (h) and (k′) hold. Clearly axioms (g) and (h) hold because $+$, $\cdot$ and P are defined pointwise. It is easy to verify that (k′) also holds.

From now on to complete the proof of Theorem D we proceed as in the case of the proof of Theorem B and show that $G \vdash S^*$ iff $\mathrm{RS} \vdash -S$.

Problem. Suppose we replace axiom (k′) of G by

$$\text{(k}''\text{)} \qquad x + y = 0 \wedge x \neq 0 \to Px \vee Py.$$

Is the resulting system decidable?

§3. Divisible abelian groups. In this section we give a general sufficient condition for undecidability that implies the undecidability of many theories, e.g. the intuitionistic theories of divisible abelian groups, abelian groups, equality, unary function, etc. The condition also applies to the intermediate logic N of constant domains, i.e. HPC + the axiom scheme $\forall x(\phi \vee \psi(x)) \to \phi \vee \forall x\psi(x)$, x not free in ϕ.

THEOREM G. *Let T be a set of axioms in a language with* $=$ *such that the theory T^C fulfills the conditions below, then both T^H and T^N are undecidable.*

(a) *T^C has a model with at least two elements.*

(b) *The class of models of T^C is closed under direct products* (*where the operations and relations are defined pointwise*).

(c) *The axioms of T are either equality axioms* (e) *or of the form*

(1) $(Q \cdots) \bigwedge \bigvee \psi_{i,j}$, *where $\psi_{i,j}$ are atomic, or*

(2) $(\forall x_1, \cdots) \bigwedge (\bigwedge \psi_i \to \bigvee \phi_j)$, *where ψ_i, ϕ_j are atomic.*

COROLLARY. *The following* HPC *or N theories are undecidable*:

(1) *Divisible abelian groups* (*i.e. with* $\forall x \exists y(x = my)$, *for all natural numbers m*).

(2) *Abelian groups.*

(3) *Equality.*
(4) *Unary function (one).*
etc.

In [1], the HPC theory of abelian groups and unary function with decidable equality were shown undecidable. This result implies (2) and (4) above, for HPC. For the case of N, however, we have

THEOREM H. *Let T be a set of axioms in language with equality and function symbols only, then* $T^C = T^N \cup \{\forall xy(x = y \vee x \neq y)\}$.

PROOF OF THEOREM G. Let K be a model of T^C with at least two elements. Let $(M, <)$ be a model of a reflexive and symmetric relation $<$ with $\bar{\bar{M}} \geq 5$. Define a Kripke model as in the proof of Theorem B (i.e. Construction (4), with K being now a model of T^C). Define all the relations and operations in the Kripke model pointwise and define equality as in Construction (4).

LEMMA 19. *The Kripke model thus defined is a model of*

$$T^N \cup \{\forall xy(--(x= y) \rightarrow x = y)\}.$$

PROOF. Follows from conditions (b) and (c) of Theorem G. Show that for any sentence ϕ of the form of (c) and for any Kripke model $(\mathbf{S}, \mathbf{R}, \mathbf{0}, \mathbf{A}_t)$ with constant domains and for any world S we have $[\phi]_s = 0$ implies $\mathbf{A}_{s'} \vDash_{\mathrm{CPC}} -\phi$ for some s' such that $s\,\mathbf{R}\,s'$.

Now since K contains at least two elements let $a, b \in K$, $a \neq b$. Let $u_1 = (a \cdots a)$, $u_2 = (b \cdots b)$, and define

$$C(x, u_1, u_2) =_{\mathrm{def}} \forall v(- -(v = u_1 \vee v = x) \rightarrow v = x) \wedge - -(x = u_1 \vee x = u_2).$$

Clearly, $[C(x, u_1, u_2)]_0 = 1$ iff x has the form $x = (a \cdots a, b, a \cdots a)$ or $x = u_1$. From now on we write $C(x)$, for $C(x, u_1, u_2)$.

$$E =_{\mathrm{def}} (\forall x, y, z)(C(x) \wedge C(y) \wedge C(z) \rightarrow x = u_1 \vee y = u_1 \vee z = u_1 \vee x = y \vee y = z \vee x = z).$$

Clearly $s \neq \mathbf{0}$ iff $[E]_s = 1$.

$$D(x) =_{\mathrm{def}} C(x) \rightarrow E \vee x = u_1.$$

$$\rho(x, y) = \forall t[- -(t = x \vee t = y) \wedge E] \rightarrow t = x \vee t = y.$$

Clearly if $[D(x) \vee D(y)]_0 = 0$, then, by construction of the Kripke model, $[\rho(f_n, f_m)]_0 = 1$ iff $m < n$, where $x = f_m = (a \cdots a, b, a \cdots a)$, ($b$ at the mth place), similarly $y = f_n$.

Let $S = (Q \cdots) \bigwedge (\bigwedge u_i < v_i) \rightarrow \bigvee x_j < y_j)$ be a sentence, as before, of the theory RS. Let

$$S^* = (\forall u_1, u_2, t_1, \cdots, t_5)\Big[u_1 \neq u_2 \wedge \forall x(Dx \vee \rho(x, x)) \wedge (Q^* \cdots) \bigwedge (\bigwedge \rho(u_i, v_i) \rightarrow \bigvee \rho(x_j, y_j) \vee E) \rightarrow E \vee \bigvee_{i=1}^{5} D(t_i) \vee \bigvee_{1 \leq i \neq j \leq 5} t_i = t_j\Big].$$

Again, the following holds:

$$T^H \text{ (or } T^N) \vdash S^* \quad \text{iff } \mathrm{RS} \vdash -S.$$

REFERENCES

[1] D. M. GABBAY, *Sufficient conditions for the undecidability of intuitionistic theories with applications*, this JOURNAL, vol. 37 (1972), pp. 375–384.

[2] ———, *Decidability of some intuitionistic predicate theories*, this JOURNAL, vol. 37 (1972), pp. 579–587.

[3] S. R. KRIPKE, *Semantic analysis for intuitionistic logic*. I, ***Formal systems and recursive functions*** (Crossley and Dummett, Editors), North-Holland, Amsterdam, 1965.

[4] C. SMORYNSKI, *Some recent results on elementary intuitionistic theories* (unpublished).

[5] A. HEYTING, *Axiomatic method and intuitionism*, ***Essays on the foundation of Mathematics,*** Magnes Press, Jerusalem 1961.

[6] M. O. RABIN, *A simple method of undecidability proof and some applications*, ***Logic, methodology and the philosophy of science,*** North-Holland, Amsterdam, 1965, pp. 58–68.

STANFORD UNIVERSITY
STANFORD, CALIFORNIA 94305