Can. J. Math., Vol. XXXIV, No. 2, 1982, pp. 500–505

TWO UNDECIDABILITY RESULTS USING MODIFIED BOOLEAN POWERS

STANLEY BURRIS AND JOHN LAWRENCE

In this paper we will give brief proofs of two results on the undecidability of a first-order theory using a construction which we call a modified Boolean power. Modified Boolean powers were introduced by Burris in late 1978, and the first results were announced in [**2**]. Subsequently we succeeded in using this construction to prove the results in this paper, namely Ershov's theorem that every variety of groups containing a finite non-abelian group has an undecidable theory, and Zamjatin's theorem that a variety of rings with unity which is not generated by finitely many finite fields has an undecidable theory. Later McKenzie further modified the construction mentioned above, and combined it with a variant of one of Zamjatin's constructions to prove the sweeping main result of [**3**]. The proofs given here have the advantage (over the original proofs) that they use a single construction.

A *Boolean pair* $(B, B_0, \leqq)$ is a Boolean algebra $(B, \leqq)$ with a distinguished subalgebra $(B_0, \leqq)$. B_0 is *dense* in B if

$$\forall x \in B \forall y \in B[\forall z \in B_0(y \leqq z \rightarrow x \leqq z) \rightarrow x \leqq y].$$

Our starting point is the following result on the first-order theory of Boolean pairs.

THEOREM 1. (McKenzie, [**3**]) *The class $\mathscr{BP}^D$ of Boolean pairs $(B, B_0, \leqq)$ such that B_0 is dense in B has an undecidable theory.*

Given an algebra A, a congruence θ of the algebra A, two fields B, B_0 of subsets of a set I with $B_0 \subseteq B$, define the *modified Boolean power* $A[B, B_0, \theta]^*$ to be the subalgebra of A^I consisting of all $f \in A^I$ such that $|f(I)| < \omega, f^{-1}(a) \in B, f^{-1}(a/\theta) \in B_0$ for $a \in A$. For $f, g \in A[B, B_0, \theta]^*$ let us define

$$[\![f = g]\!] = \{i \in I: f(i) = g(i)\}$$
$$[\![f \neq g]\!] = \{i \in I: f(i) \neq g(i)\}.$$

In the following we will establish undecidability by showing that for suitable A, θ the class $\mathscr{BP}^D$ can be interpreted into

$$\{A[B, B_0, \theta]^*: (B, B_0, \subseteq) \in \mathscr{BP}^D\}.$$

Received February 3, 1981. The work of the first author was supported by NSERC Grant A7256 while that of the second was supported by NSERC Grant A4540.

https://doi.org/10.4153/CJM-1982-033-6 Published online by Cambridge University Press

1. Rings with unity.

LEMMA 1. *Let R be a directly indecomposable non-simple ring with unity. Choose a congruence θ of R with $\triangle < \theta < \nabla$. Then $\mathscr{B}\mathscr{P}^D$ can be interpreted into*

$$\{R[B, B_0, \theta]^*: (B, B_0, \subseteq) \in \mathscr{B}\mathscr{P}^D\}.$$

Proof. Let us show that the formulas

$$\delta(x): x \approx x$$

$$\delta_0(x): \text{“}x \text{ is a central indempotent”}$$

$$\rho(x, y): \forall z[\delta_0(z) \rightarrow (y \cdot z \approx y \rightarrow x \cdot z \approx x)]$$

$$Eq(x, y): \rho(x, y) \;\&\; \rho(y, x)$$

suffice to interpret $(B, B_0, \subseteq)$ into $A[B, B_0, \theta]^*$.

For $f \in R[B, B_0, \theta]^*$ let $\alpha(f) = [\![f \neq 0]\!]$. Then one can easily verify

$$B = \{\alpha(f): f \in A[B, B_0, \theta]^*\}$$

$$B_0 = \{\alpha(f): f \in A[B, B_0, \theta]^* \text{ and } f \text{ is a central indempotent}\}$$

and for $f, g \in R[B, B_0, \theta]^*$, with $\delta(f)$ and $\delta_0(g)$ holding,

$$\alpha(f) \subseteq \alpha(g) \text{ if and only if } f \cdot g = f.$$

Thus for $f, g \in R[B, B_0, \theta]^*$, $\rho(f, g)$ holds if and only if $\alpha(f) \subseteq \alpha(g)$ as B_0 is dense in B. Consequently we can conclude

$$(B, B_0, \subseteq) \cong (\delta^S, \delta_0{}^S, \rho^S)/Eq^S$$

where $S = R[B, B_0, \theta]^*$.

LEMMA 2. *A semi-simple variety V of rings is generated by finitely many finite fields.*

Proof. First note that the free algebra $F_V(\phi)$ in V is finite, for otherwise it is isomorphic to $\mathbf{Z}$; but $\mathbf{Z}_4 \notin V$. Thus there are only finitely many p (all non-zero) such that there is a field of characteristic p in V. For any prime p the polynomial ring $\mathbf{Z}_p[x]$ is not in V as $\mathbf{Z}_p[x]/\langle x^2 \rangle$ is subdirectly irreducible but not simple.

If F is a field, say of characteristic p, in V then F is finite. For otherwise there is either a transcendental element $a \in F$, hence $\mathbf{Z}_p[x]$ can be embedded in F, or there are elements $a_n \in F$ for $n < \omega$ such that degree $(a_n) \geqq n$, and in this case $\mathbf{Z}_p[x]$ can be embedded in $F^\omega/\mathscr{U}$ for a suitable $\mathscr{U}$. Thus V has, up to isomorphism, only finitely many fields in it, and they are all finite.

Now consider $F_V(x)$. As this is commutative and V is semi-simple it must be a subdirect product of fields. As there are only finitely many fields in V and they are finite it follows that $x^n = x$ holds for some n. But

https://doi.org/10.4153/CJM-1982-033-6 Published online by Cambridge University Press

then $V \models x^n \approx x$, so by a result in [**1**], V is generated by finitely many finite fields.

THEOREM 2. (Zamjatin [**7**]) *A variety of rings with unity has a decidable theory if and only if it is generated by finitely many finite fields.*

Proof. The direction ($\Rightarrow$) follows from Lemma 1 and Lemma 2. The converse is in [**4**].

2. Groups. If V is a variety of groups containing a finite non-abelian group, let G be a minimal non-abelian finite group in V. Then G has the following properties:

(i) G is solvable [[**6**], p. 148] as every proper subgroup is abelian.

(ii) G is two-generated, say by a, b.

(iii) We can assume $\langle b \rangle$, the normal subgroup generated by b, is proper, hence abelian, so $\langle b \rangle \subseteq C_b$, the centralizer of b.

(iv) G is subdirectly irreducible, and the monolith M is the commutator subgroup.

(v) As $M \subseteq \langle b \rangle$, the centralizer C_b is a normal subgroup of G.

(vi) There is a finite m_0 such that for $[c, d] \neq 1$

$$M = \left\{ \prod_{i=1}^{m} h_i^{-1}[c, d]h_i \colon \quad h_i \in G, m \leqq m_0 \right\}.$$

LEMMA 3. *Let G be as described above. Then, with θ the congruence corresponding to the normal subgroup C_b, $\mathcal{BP}^D$ can be interpreted, using one parameter, into*

$$\{G[B, B_0, \theta]^* \colon (B, B_0, \subseteq) \in \mathcal{BP}^D\}.$$

Proof. For $c \in G$ let $\mathbf{c}$ denote the constant function in $G[B, B_0, \theta]^*$ with value c. If $f \in G[B, B_0, \theta]^*$ let $\alpha(f) = [\![f \neq 1]\!]$. Then we have

(*) $\quad B = \{\alpha([f, g]) \colon f, g \in G[B, B_0, \theta]^*\}$

(**) $\quad B_0 = \{\alpha([f, \mathbf{b}]) \colon f \in G[B, B_0, \theta]^*\}.$

To see (*) note that

$$\alpha(f) = \cup_{c \neq 1} f^{-1}(c) \in B$$

for all $f \in G[B, B_0, \theta]^*$. On the other hand given $X \in B$ let $f = \mathbf{a}$ and let g be defined by

$$g(i) = \begin{cases} b & \text{if} \quad i \in X \\ 1 & \text{if} \quad i \notin X. \end{cases}$$

https://doi.org/10.4153/CJM-1982-033-6 Published online by Cambridge University Press

Then $\alpha([f, g]) = X$. For (**) we have

$$\begin{aligned}\alpha([f, \mathbf{b}]) &= [\![[f, \mathbf{b}] \neq 1]\!] \\ &= \{i \in I: f(i) \notin C_b\} \\ &= \bigcup_{c \notin C_b} f^{-1}(c/\theta) \in B_0.\end{aligned}$$

And given $Y \in B_0$ let f be defined by

$$f(i) = \begin{cases} a & \text{if } i \in Y \\ 1 & \text{if } i \notin Y. \end{cases}$$

Then $\alpha([f, \mathbf{b}]) = Y$.

Our next claim is that for $f, h \in G[B, B_0, \theta]^*$ with $h(i) \in M$ for all i, we have

$$(***) \quad \alpha(h) \subseteq \alpha([f, \mathbf{b}])$$

if and only if

$$h = \prod_{\substack{c,d \in G \\ d \notin C_b}} \prod_{j=1}^{m_{cd}} t_{cdj}^{-1}[f, f_{cd}]t_{cdj}$$

for suitable f_{cd}, t_{cdj} with $f_{cd} \in C_{\mathbf{b}}$, and for suitable $m_{cd} \leqq m_0$, where m_0 is as defined in (vi).

The direction $(\Leftarrow)$ follows from

$$\begin{aligned}\alpha(h) = \alpha\left(\prod_{\substack{c,d \in G \\ d \notin C_b}} \prod_{j=1}^{m_{cd}} t_{cdj}^{-1}[f, f_{cd}]t_{cdj} \right) &\subseteq \bigcup_{\substack{c,d \in G \\ d \notin C_b}} \bigcup_{j=1}^{m_{cd}} \alpha(t_{cdj}^{-1}[f, f_{cd}]t_{cdj}) \\ &= \bigcup_{\substack{c,d \in G \\ d \notin C_b}} \alpha([f, f_{cd}]) \subseteq \alpha([f, \mathbf{b}]).\end{aligned}$$

For the converse $(\Rightarrow)$ we have $\alpha(h) \subseteq \alpha([f, \mathbf{b}])$. For $c, d \in G$ let

$$X_{cd} = [\![h = \mathbf{c}]\!] \cap [\![f = \mathbf{d}]\!]$$

$$f_{cd}(i) = \begin{cases} b & \text{for } i \in X_{cd} \\ 1 & \text{otherwise} \end{cases}$$

$$h_{cd}(i) = \begin{cases} c & \text{for } i \in X_{cd} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$f_{cd} \in C_{\mathbf{b}}$$

$$\alpha([f, f_{cd}]) = X_{cd} \quad \text{if} \quad d \notin C_b$$

$$h = \prod_{\substack{c,d \in G \\ d \notin C_b}} h_{cd} \quad (\text{as } h(i) \neq 1 \Rightarrow f(i) \notin C_b).$$

Given $c, d \in G$ with $d \notin C_b$, $c \in M$ there is $m_{cd} \leqq m_0$ by (vi) such that

$$c = \prod_{j=1}^{m_{cd}} e_{cdj}{}^{-1}[d, b]e_{cdj}$$

for suitable e_{cdj}. Letting $t_{cdj} = \mathbf{e}_{cdj}$ it follows that

$$h_{cd} = \prod_{j=1}^{m_{cd}} t_{cdj}{}^{-1}[f, f_{cd}]t_{cdj}$$

so

$$h = \prod_{\substack{c,d\in G\\ d\notin C_b}} \prod_{j=1}^{m_{cd}} t_{cdj}{}^{-1}[f, f_{cd}]t_{cdj}.$$

This establishes the converse.

Now to prove the lemma let us consider the formulas

$$\delta(x)\colon \exists x_1 \exists x_2 (x \approx [x_1, x_2])$$

$$\delta_0(x)\colon \exists x_3 (x \approx [x_3, \mathbf{b}])$$

$$\bar{\rho}(x, y)\colon \delta(x)\ \&\ \exists y_3 \{y = [y_3, \mathbf{b}]\ \&$$

$$\bigvee_{\langle m_{cd} : m_{cd} \leqq m_0 \rangle} \exists \mathbf{u} \exists \mathbf{v} \left(x \approx \prod_{\substack{c,d\in G\\ d\notin C_b}} \prod_{j=1}^{m_{cd}} u_{cdj}{}^{-1}[y_3, v_{cd}]u_{cdj} \mathop{\&}_{\substack{c,d\in G\\ d\notin C_b}} (\mathbf{b}\, v_{cd} \approx v_{cd}\mathbf{b}) \right)$$

$$\rho(x, y)\colon \forall z (\bar{\rho}(y, z) \rightarrow \bar{\rho}(x, z))$$

$$Eq(x, y)\colon \rho(x, y)\ \&\ \rho(y, x).$$

Now we have, with $H = G[B, B_0, \theta]^*$,

$\alpha(\delta^H) = B$ (by (*))

$\alpha(\delta_0{}^H) = B_0$ (by (**))

$\bar{\rho}(f, g)$ holds $\Leftrightarrow f \in \delta^H$, $g \in \delta_0{}^H$ and $\alpha(f) \subseteq \alpha(g)$ (by (***))

$\rho(f, g)$ holds if $f, g \in \delta^H$ and $\alpha(f) \subseteq \alpha(g)$ (as B_0 is dense in B)

$Eq(f, g)$ holds $\Leftrightarrow f, g \in \delta^H$ and $\alpha(f) = \alpha(g)$.

Thus

$$(B, B_0, \subseteq) \cong (\delta^H, \delta_0{}^H, \rho^H)/Eq^H.$$

We immediately have the following.

THEOREM 3 ([**5**]). *If V is a variety of groups with a finite non-abelian member then V has an undecidable theory.*

References

1. R. F. Arens and I. Kaplansky, *Topological representations of algebras*, Trans. Amer. Math. Soc. *63* (1948), 457–481.

https://doi.org/10.4153/CJM-1982-033-6 Published online by Cambridge University Press

2. S. Burris, *An algebraic test for undecidability*, N.A.M.S. *26* (1979).
3. S. Burris and R. McKenzie, *Decidability and Boolean representations*, Memoirs Amer. Math. Soc. *32*, No. 246 (1981).
4. S. Comer, *Elementary properties of structures of sections*, Bol. Soc. Mat. Mexicana *19* (1974), 78–85.
5. Yu. L. Ersov, *Theories of non-abelian varieties of groups*, Proc. of Symposium in Pure Mathematics *25* (A.M.S., Providence, Rhode Island, 1974), 255–264.
6. W. R. Scott, Group theory (Prentice Hall, 1964).
7. A. P. Zamjatin, *Varieties of associative rings whose elementary theory is decidable*, Soviet Math. Doklady *17* (1976), 996–999.

University of Waterloo,
Waterloo, Ontario