Notre Dame Journal of Formal Logic
Volume XVIII, Number 3, July 1977
NDJFAM

SOME APPLICATIONS OF MODEL THEORY TO THE METATHEORY OF PROGRAM SCHEMATA

RICHARD A. DeMILLO

1 *Introduction* Program schemata (also called schemes, or abstract programs) are widely known as devices for treating properties of computer programs which are invariant across a range of interpretations. Since the intent of schemata is to formalize a specific aspect of effective computation, the properties studied are usually those which have been prescribed in other models of computation: e.g., totality, equivalence, decision power. It is perhaps for this reason that the methodology for dealing with schemata has evolved around constructive mathematics and direct demonstration rather than continuous mathematics, transfinite mathematics and indirect proof. Recently, however, it has been pointed out (Kfoury [3], DeMillo [2]) that useful properties of schemata can be established using arguments which rest on nonconstructive foundations; in this case the model theory of first order logic. The outcome of this activity has been to recast some deep questions regarding, for instance, what can and cannot be proved about computer programs into a form which is similar to the corresponding logical questions, where some of the answers are known.

In this note,* we present three such applications of model theory. We allow a free wheeling notion of schemata (allowing, for example, first order oracles of any sort desired) and show that direct limitations exist in the ability to draw inferences about schemata by examining finite entailment and axiomatizability. The third application shows that even the expansive concept of effectiveness allowed here does not admit more relative decision power than the standard models of computation.

2 *Notation* Logical notation follows such standard sources as Bell and Slomson [1]. In particular, such notions as first order language, similarity type, relational structure, and interpretation are assumed in this presentation. A given first order language always talks about

*The work reported herein was sponsored, in part, by NSF Grant GN-655.

Received October 3, 1974

relational structures of the same similarity type, and these are denoted $\mathfrak{A} = \langle \underset{\sim}{A}, \underset{\sim}{F}, \underset{\sim}{R} \rangle$ where $\underset{\sim}{A} \neq \emptyset$, $\underset{\sim}{F}$ is a set of mappings $\underset{\sim}{A}^n \to \underset{\sim}{A}$, and $\underset{\sim}{R}$ is a set of relations $r \subseteq \underset{\sim}{A}^m$ $(m > 0)$. If $f \in \underset{\sim}{F}$ maps $\underset{\sim}{A}^n \to \underset{\sim}{A}$, for $n = 0$, it interprets an individual constant. Lower case Greek letters represent cardinals: ω is the first transfinite ordinal, hence $\omega = N = \{0, 1, 2, \ldots\}$. For any nonempty X, X^ω is the set of all ω-termed sequences on X. Although it will not be essential for later developments, we will give a rather detailed accounting of the satisfiability relation for a first order language $\mathbf{L}$. This keeps the presentation relatively self-contained and leads easily to the corresponding ideas for schemata.

The concept of a schema used here is essentially the concept presented by Kfoury [3], and the reader is referred to that paper for a more detailed justification. Let L be a set of first order formulas, and let T be a set of expressions of the form $v_i \leftarrow t$, where v_i is an individual variable and t is a term. We define $S = (L \times T \times N \times T \times N)$ and say that any $s \in S$ is an instruction. An intuitive reading of $s = \langle \phi, v_i \leftarrow t_1, j, v_k \leftarrow t_2, l \rangle$ is the Algol-like statement

if ϕ *then*
    begin v_i: = t_1; go to j *end*
else
    begin v_k: = t_2; go to l *end.*

We let A_S be any acceptable arithmetization of instructions in S; if $s \in S$, a_s is the value of s in A_S. The set of schemata $\mathsf{P}(L)$ is the set of functions $p: N \to S$ which may be partial on N. That is $\mathsf{Do}(p) \subseteq N$. An effective schema is a schema $p: N \to S$ such that there exists a partial recursive $p': N \to A_S$ satisfying

$$p'(i) = a_{p(i)}$$

for all $i \in N$, whenever either side is defined. A schema p is a flowchart schema iff $\mathsf{Do}(p)$ is finite. Every schema p has a unique START instruction: if n is the least element of $\mathsf{Do}(p)$, then $p(n)$ is the START instruction. If $p(m) = \langle \phi, v_i \leftarrow t_1, j, v_k \leftarrow t_2, l \rangle$ and $j(l)$ is not in $\mathsf{Do}(p)$, then $j(l)$ is said to be an exit of p. For fixed $\mathsf{P}(L)$, we let $\mathsf{P}(L)^{\mathsf{E}}$ and $\mathsf{P}(L)^{\mathsf{F}}$ denote, respectively, the effective and flowchart schemata in $\mathsf{P}(L)$.

3 *Interpretations* The interpretation of a primitive symbol P (individual constant, function symbol, predicate symbol) in a relational structure $\mathfrak{A}$ is written $\underset{\sim}{P}$. Let t be a term and let $x = \langle x_0, x_1, x_2, \ldots x_n, \ldots \rangle \in \underset{\sim}{A}^\omega$. The value of t at x, $[t](x)$ is defined:

(1) if t is an individual variable v_i, $[t](x) = x_i$;
(2) if t is an individual constant a_i, $[t](x) = \underset{\sim}{a}_i$,
(3) if t is a term $f(t_1, \ldots, t_n)$, $[t](x) = \underset{\sim}{f}([t_1](x), \ldots, [t_n](x))$.

For $i \in N$, $y \in \underset{\sim}{A}$ (i/y): $\underset{\sim}{A}^\omega \to \underset{\sim}{A}^\omega$ is defined as follows: for $x \in \underset{\sim}{A}^\omega$

$$((i/y)x)(j) = \begin{cases} x_j, \text{ if } j \neq i, \\ y, \text{ otherwise.} \end{cases}$$

Let L and $\mathfrak{A}$ be fixed, and suppose $x \in \underset{\sim}{A}^{\omega}$, and ϕ is a formula in L. Then x satisfies ϕ, written $\mathfrak{A} \models_x \phi$, iff:

(1) ϕ is atomic $r(t_1, \ldots, t_n)$ and $\langle [t_1](x), \ldots, [t_n](x)\rangle \in \underset{\sim}{r}$;
(2) ϕ is $\phi_0 \vee \phi_1$ and $\mathfrak{A} \models_x \phi_0 \vee \mathfrak{A} \models_x \phi_1$;
(3) ϕ is $\neg\phi_0$ and $\mathfrak{A} \not\models_x \phi_0$;
(4) ϕ is $(\forall v_j)\phi_0$ and $\forall y \in \underset{\sim}{A}\ \mathfrak{A} \models_{(j/y)x} \phi_0$.

Extensions to '$\rightarrow$', '$\wedge$', '$\leftrightarrow$', '$\exists$' follow as usual. If $\mathfrak{A} \models_x \phi$ for all $x \in \underset{\sim}{A}^{\omega}$, ϕ is said to be true in $\mathfrak{A}$, written $\mathfrak{A} \models \phi$. If ϕ contains the free variables $v_{i_1}, \ldots, v_{i_n}$ then $\mathfrak{A} \models_x \phi$ iff $\mathfrak{A} \models \phi[x_{i_1}, \ldots, x_{i_n}]$. If L is a set of formulas, then $\mathfrak{A}$ is said to be a model for L iff $\mathfrak{A} \models \phi$ for each $\phi \in L$.

Now let p be any schema. We define a sequence $\underset{\sim}{p}_x$ for any $x \in \underset{\sim}{A}^{\omega}$ as follows

(1) $\underset{\sim}{p}_x(0) = \langle p(\text{START}), x\rangle$;
(2) if $\underset{\sim}{p}_x(i) = \langle p(n), y\rangle$ where $p(n) = \langle \phi, v_j \leftarrow t_1, k, v_m \leftarrow t_2, l\rangle$, then

$$\underset{\sim}{p}_x(i+1) = \begin{cases} \langle p(k), (j/[t_1](y))y\rangle \text{ if } \mathfrak{A} \models_y \phi \\ \langle p(l), (m/[t_2](y))y\rangle \text{ if } \mathfrak{A} \not\models_y \phi \end{cases};$$

(3) if $\underset{\sim}{p}_x(i) = \langle$undefined, $y\rangle$, write $\underset{\sim}{p}_x(i) = \langle *, y\rangle$ and let $\underset{\sim}{p}_x(i+1)$ be undefined.

Following Kfoury [3], we consider a set of properties $\Gamma = \{\Phi_0, \Phi_1, \ldots,\}$ such that a schema p is Γ satisfiable iff for some $x \in \underset{\sim}{A}^{\omega}$, and all $\Phi_i \in \Gamma$ $\underset{\sim}{p}_x$ satisfies Φ_i. In this case we write $(\mathfrak{A}, \Gamma) \models_x p$. Analogously, if $(\mathfrak{A}, \Gamma) \models_x p$ for all $x \in \underset{\sim}{A}^{\omega}$, we write $(\mathfrak{A}, \Gamma) \models p$.

For any property set Γ, $M(p) = \{\mathfrak{A} \mid (\mathfrak{A}, \Gamma) \models p\}$. For technical reasons we relativize this definition to a certain "universal" set $\underset{\sim}{M}$. Hence $M(p) = \{\mathfrak{A} \in \underset{\sim}{M} \mid (\mathfrak{A}, \Gamma) \models p\}$. As described in Kfoury [3], certain choices of Γ appear to be reasonable; we introduce admissible property sets to recover this notion. Γ is admissible iff:

(1) for some $p \in P(L)$ $M(p) = \underset{\sim}{M}$,
(2) for some $p \in P(L)$ $M(p) = \emptyset$,
(3) any $p, p' \in P(L)$, there exist schemata $p|p'$ and $p||p'$ such that

$$M(p|p') = M(p) \cup M(p')$$
$$M(p||p') = M(p) \cap M(p').$$

By analogy with first order models we let, for X a set of schemata, $M(X) = \cap \{M(p) \mid p \in X\}$.

Let $\Gamma = \{\Phi\}$, then for any $p \in P(L)$, $\mathfrak{A} \in \underset{\sim}{M}$, $x \in \underset{\sim}{A}^{\omega}$, $\underset{\sim}{p}_x$ satisfies Φ iff $\underset{\sim}{p}_x$ is a finite sequence. Then the notion of admissibility has special significance, which we present without proof.

Theorem *If $p', p \in P(L)$ is an effective schema and $\Gamma = \{\Phi\}$, then M satisfies conditions* (1)-(3) *for admissibility.*

Henceforth, we let $\Gamma = \{\Phi\}$. If $(\mathfrak{A}, \Gamma) \models p$, p is said to be total in Φ. If $M(p) = \underset{\sim}{M}$, p is said to be universally total.

4 *A duality concept* The schemata $p|p'$ and $p||p'$ have a certain physical interpretation, given an environment in which to execute the effective schemata p and p'. Consider that in order to execute $p||p'$ for the flowchart schemata p and p' it is sufficient to choose one schema, say p, and to uniformly substitute for each variable v_j of p a variable v' not occurring in p', keeping a record of these substitutions by the expressions $v' \leftarrow v_j$. To execute one first executes these assignments, effectively separating the variables of p and p'; then, alternatively, the instructions of p and p' are executed until one of the execution sequences satisfies Γ, upon which execution terminates. This simulation corresponds to nondeterministic programs. In similar fashion, the execution of $p|p'$ can be simulated by processing p and p' in parallel.

5 *Model constructions* The model theory of $\mathsf{P}(L)^{\mathsf{E}}$ differs radically from the model theory of L in the methods available for constructing models. It is partially because of this fact that the subject carries some interest. We review here two negative results and one positive result which show the points of departure and similarity.

(i) Incompactness (DeMillo, [2]). For appropriate L, $\mathsf{P}(L)^{\mathsf{E}}$ contains an incompact set of programs. That is, for some $X \subset \mathsf{P}(L)$, $M(Y) \neq \emptyset$ for every finite $Y \subset X$, but $M(X) = \emptyset$.
(ii) Upward Löwenheim-Skolem (Kfoury, [3] and DeMillo, [2]). For appropriate L, there is a schema $p \in \mathsf{P}(L)^{\mathsf{F}}$ such that $M(p)$ contains a countable model but no uncountable model.
(iii) Downward Löwenheim-Skolem (Kfoury, [3]). For appropriate L and for every $X \subseteq \mathsf{P}(L)^{\mathsf{E}}$ if $\mathfrak{A} \in M(X)$ is infinite, then for every infinite $\gamma < \mathsf{Card}\ (\underset{\sim}{A})$ there is some $\mathfrak{B} \in M(X)$ such that $\mathsf{Card}\ (\underset{\sim}{B}) = \gamma$.

6 *Inferring properties of effective schemata* The results of this section are clearly metatheoretic. We assume that there is a semantic notion of entailment available which characterizes mathematical inferences which hold for schemata and necessarily limit any syntax which mediates such inferences. Since such results are limitative, they are also negative. For any $X \subseteq \mathsf{P}(L)$, $p \in \mathsf{P}(L)$ we write $X \Vdash p$ and say that X semantically entails p iff $M(X) \subseteq M(p)$. $\mathsf{P}(L)$ is said to have finitary semantic entailment (**FSE**) when $X \Vdash p$ implies $Y \Vdash p$ for some finite $Y \subseteq X$. Let $\mathsf{P}(L)^{\mathsf{E}}$ be fixed, and suppose that L contains a symbol ($\eqsim$) always interpreted as equality, a unary function symbol f, and individual constants a_0, a_1.

Theorem $\mathsf{P}(L)^{\mathsf{E}}$ *does not have* **FSE**.

Proof: Let $X = \{p, p_0, p_1, \ldots\}$, where (using obvious abbreviations)

$$p_\omega = \begin{cases} \text{START: } v_1 \leftarrow a_0\text{; go to 1} \\ \text{1: if } v_1 \eqsim a_1 \text{ then [exit] else } [v_1 \leftarrow f(v_1)\text{; go to 1}] \end{cases}$$

$$p_i = \begin{cases} \text{START: } v_1 \leftarrow a_0\text{; go to 1} \\ \text{1: if } a_1 \eqsim f^i(v_1) \text{ then [go to 1] else [exit].} \end{cases}$$

In each p_i the term $f^i(v_1)$ abbreviates v_1, if $i = 0$ and $f(f^{i-1}(v_1))$, if $i > 0$.

Assume **FSE**. Notice that $M(X) = \emptyset$. Hence, for any p such that $M(p) = \emptyset$, $\emptyset = M(X) \subseteq M(p) = \emptyset$. By **FSE** there is a finite $Y \subseteq X$ such that $M(Y) \subseteq M(p)$; that is $Y \Vdash p$. We choose $\mathfrak{A}$ so that $\underset{\sim}{A} = N$, $\underset{\sim}{f}$ is the successor function, $\underset{\sim}{a}_0 = 0$ and $\underset{\sim}{a}_1 = \sup\{i \mid p_i \in Y \wedge i \neq \omega\} + 1$. Then since every natural number is some n'th sucessor of 0, $M(Y) \neq 0$, which contradicts $Y \Vdash p$. Q.E.D.

Corollary $\mathsf{P}(L)^{\mathsf{F}}$ *does not have* **FSE**.

The set of schemata X in the proof of the previous theorem is essentially the set which contradicts compactness. Let $X \subseteq \mathsf{P}(L)^{\mathsf{E}}$. Then define $\mathsf{Cl}(X) = \{p \mid X \Vdash p\}$. We say that X is a deductive system iff $\mathsf{Cl}(X) = X$; systems will be denoted by α, β, γ, . . . (see Robinson [4] for the corresponding concept for L). The following facts concerning systems are well known:

(1) $\{X \mid X$ is a system$\}$ is a lattice with unit and zero under the operations

$$\alpha \cdot \beta = \alpha \cap \beta$$
$$\alpha + \beta = \bigcap \{\gamma \mid \alpha \cup \beta \subseteq \gamma\}.$$

(2) $\alpha \subseteq \beta$ iff $M(\beta) \subseteq M(\alpha)$.
(3) $M(\alpha) \cup M(\beta) \subseteq M(\alpha \cap \beta)$.

A system α is finitely axiomatizable (**FA**) iff there is a finite $Y \subseteq \alpha$ such that $\mathsf{Cl}(Y) = \alpha$. $\mathsf{P}(L)^{\mathsf{E}}$ is **FA** iff every system is **FA**.

(4) β is not **FA** iff $\beta = \bigcup\{\alpha_i \mid i \in \omega\}$, where for all i, $\alpha_i \subseteq \alpha_{i+1}$ and $M(\alpha_i) \not\subseteq M(\alpha_{i+1})$. (See Robinson [4], p. 36.)

Fact (3) is useful in relating the operations +, · to the syntactic operations $|$, $||$.

Lemma $\mathsf{Cl}(p) + \mathsf{Cl}(p') \subseteq \mathsf{Cl}(p \,||\, p')$ *and* $\mathsf{Cl}(p) \cdot \mathsf{Cl}(p') = \mathsf{Cl}(p \mid p')$.

Proof: Use (3). Q.E.D.

Theorem *For sufficiently strong* L, $\mathsf{P}(L)^{\mathsf{E}}$ *and* $\mathsf{P}(L)^{\mathsf{F}}$ *are not* **FA**.

Proof: Let $L = \{\phi_0, \phi_1, \ldots\}$ be such that for all finite $J \subseteq N$, if $j \in J$ there exist $\mathfrak{A}$, $\mathfrak{B} \in \underset{\sim}{M}$ such that

$$\mathfrak{A} \models \bigwedge_{i \in J} \phi_i \wedge \phi_j \text{ and } \mathfrak{B} \models \bigwedge_{i \in J} \phi_i \wedge \neg\phi_j.$$

For each natural number i let

$$p_i = \text{START: if } \phi_i \text{ then [exit] else [go to START]}.$$

Define a sequence of systems α_0, α_1, . . . as follows:

$$\alpha_0 = \mathsf{Cl}(p_0)$$
$$\alpha_{i+1} = \alpha_i + \mathsf{Cl}(p_{i+1}).$$

Obviously $\alpha_i \subseteq \alpha_{i+1}$. To verify the second property of fact (4) above, let, for each i, $\beta_i = \mathsf{Cl}(p_0 || p_1 || \ldots || p_i)$. Thus $\alpha_i \subseteq \beta_i$, and there is some $\mathfrak{A} \in \underset{\sim}{M}$ such that

$$\mathfrak{A} \models \bigwedge_{j \leq i} \phi_i \wedge \neg\phi_{i+1}.$$

Therefore $\mathfrak{A} \in M(\beta_i) \subseteq M(\alpha_i)$, but $\mathfrak{A} \notin M(\alpha_{i+1})$. Take $\beta = \bigcup \alpha_i$ to complete the proof. Q.E.D.

7 *Semantically preserving effectiveness* A common question to ask about such liberally "effective" concepts as schemata, is how much of the intuitive notion of effectiveness they preserve. Of course, this question has been settled by syntactic arguments, but the purpose of this section is to recast one of these standard results in purely semantic terms. It so happens that this is possible only insofar as the incompactness and non **FSE** properties can be proved semantically. Nevertheless, we will be able to solve a certain generalization of the Halting Problem (negatively, of course) without explicit reference to the **RE** set which is not recursive.

Consider the algebra of sets over $\underset{\sim}{M}$ obtained from $\{M(p) \mid p \in \mathsf{P}(L)\}$. Schemata from $\mathsf{P}(L)$ (or $\mathsf{P}(L)^{\mathsf{E}}$) are said to be non-Turing if a schema can be formulated which ultimately decides Γ in each $\mathfrak{A} \in \underset{\sim}{M}$. That is, if for each p there is some $\bar{p}$ for which $M(\bar{p}) = \underset{\sim}{M} \sim M(p)$. The proof that $\mathsf{P}(L)^{\mathsf{E}}$ is Turing rests on set theoretic properties of filters. We assume that the concept of a filter over $\underset{\sim}{M}$ is known (see Bell and Slomson [1]). An ultrafilter is a maximal filter. Two facts relating to ultrafilters are useful. First, if a set of elements of the algebra is such that any finite subset has a non-zero infimum, then the set is a base for a filter F. Second, if F is a filter, it can be extended to an ultrafilter. An ultrafilter is said to converge to $\mathfrak{A} \in \underset{\sim}{M}$ iff $F = \{K \mid \mathfrak{A} \in K\}$.

Theorem $\mathsf{P}(L)^{\mathsf{E}}$ is Turing.

Proof: We suppose that $\mathsf{P}(L)^{\mathsf{E}}$ is non-Turing. First assume that every ultrafilter on $\underset{\sim}{M}$ converges to some $\mathfrak{A}$. Since $\mathsf{P}(L)^{\mathsf{E}}$ does not have **FSE**, let $X_i \Vdash\!\!\!\!\not\vdash p$ for all finite $X_i \subseteq X$, where $X \Vdash\!\!\!\!\vdash p$. We define $H(X_i) = M(X_i) \sim M(p)$. Since each $H(X_i) \neq \emptyset$ and $\bigcap \{H(X_{ji}) \mid i \leqslant n\} = H\left(\bigcup \{X_{ji} \mid i \leqslant n\}\right)$, the $H(X_i)$ are a base for some filter F. By hypothesis, there is some $\mathfrak{A}$ to which F converges. If $p' \in X$, then $H(p') = M(p') \sim M(p)$ is in F, so $M(p')$ is in F. Hence, for any $p' \in X$, $(\mathfrak{A}, \Gamma) \models p'$. But since $M(p) \cap H(p') = \emptyset$ when $M(p) \in F$, $M(p) \notin F$. But this implies $X \Vdash\!\!\!\!\not\vdash p$. By definition, $M(p \,||\, p') = M(p) \cap M(p')$. Let $\bar{p}$ be such that $M(\bar{p}) = \underset{\sim}{M} \sim M(p)$. Then for any ultrafilter F, either $M(\bar{p}) \in F$, $M(p) \in F$, but not both. In addition $M(p) \cap M(p') \in F$ iff $M(p) \in F$ and $M(p') \in F$. Hence, $M(\bar{p}) \in F$ iff $M(p) \notin F$ and $M(p \,||\, p') \in F$ iff $M(p) \in F$ and $M(p') \in F$. Then for some $\mathfrak{A} \in M$ $(\mathfrak{A}, \Gamma) \models p$ for all $M(p) \in F$ and $(\mathfrak{A}, \Gamma) \models \bar{p}$ for all $M(p) \notin F$. But this implies that F converges to $\mathfrak{A}$. Q.E.D.

REFERENCES

[1] Bell, J. L., and A. B. Slomson, *Models and Ultraproducts*, North-Holland, Amsterdam (1969).

[2] DeMillo, R. A., "Non-definability of certain semantic properties of programs," *Notre Dame Journal of Formal Logic*, vol. XVI (1975), pp. 583-590.

[3] Kfoury, D., "Comparing algebraic structures up to algorithmic equivalence," in *Automata, Languages and Programming*, M. Nivat, editor, North-Holland, Amsterdam (1973), pp. 253-257.

[4] Robinson, A., *Introduction to Model Theory and to the Metamathematics of Algebra*, North-Holland Co., Amsterdam (1965).

University of Wisconsin-Milwaukee
Milwaukee, Wisconsin