MIT/LCS/TM-95

CHARACTERIZING SECOND ORDER LOGIC WITH FIRST ORDER QUANTIFIERS

David Harel

February 1978

MIT/LCS/TM-95

Characterizing Second Order Logic with First Order Quantifiers

David Harel

February 1978

This research was supported by the National Science Foundation under contract no. MCS76-18461.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

LABORATORY FOR COMPUTER SCIENCE

CAMBRIDGE MASSACHUSETTS 02139

Key Words: First order logic
Henkin prefix
Partially ordered quantifiers
Second order logic

Characterizing Second Order Logic with First Order Quantifiers

by

David Harel

Laboratory for Computer Science

MIT, March 1977

Abstract.

A language Q is defined and given semantics, the formulae of which are quantifier-free first-order matrices prefixed by combinations of finite partially ordered first-order quantifiers. It is shown that Q is equivalent in expressive power to second order logic by establishing the equivalence of alternating second order quantifiers and forming conjunctions of partially ordered first-order quantifiers.

Introduction

In [1] and [2] it is shown that the language consisting of formulae of the form QM, where Q is a partially ordered quantifier prefix (Henkin prefix, abbreviated poq) and M is a quantifier-free matrix, is equal in expressive power to Σ_1^1 (notation from Rogers[3]). Extending the language to allow the attachment of poq's to formulae as an additional formation rule (together with, say, $\wedge$ and $\neg$), yields Δ_2^1 (see [1]). This extension seems, however, to destroy the natural character of the semantics of poq's which existed in the case QM. We view the semantics differently in the extended case, giving rise to an extension $\mathcal{Q}$ consisting of formulae of the form PM, where the prefix P is a well formed formula over poq's (using $\wedge$ and $\neg$), and M is a quantifier-free formula. The semantics of formulae of $\mathcal{Q}$ is given in terms of conventional second order logic, and it is shown that in fact $\mathcal{Q}$ is equal in expressive power to full second order logic, by establishing a correspondence between alternating second order quantifiers and forming the conjunction of alternating poq's. This result supplies an alternative characteristic of second order logic using only (partially ordered) first-order quantifiers.

Definitions

We assume throughout that a fixed second order langage L is given, and we freely use $x, x_1, x_2, \ldots y, \ldots, u, \ldots, v, \ldots$ to stand for variables, and $f, f_1, f_2, \ldots, g, h, \ldots$ to stand for function symbols.

We define the language Q as follows:

A partially ordered quantifier prefix (poq) is a tuple of the form

(*) $(x_1, \ldots, x_n; y_1, \ldots, y_m; \beta)$

where β is a function which associates with each y_i for $1 \leq i \leq m$, a tuple, the elements of which are disjoint and are in $\{x_1, \ldots, x_n\}$. Intuitively for a poq Q, we will be using <Q> to mean that the x's are universaly quantified and the y's existentially, but that each y_i depends only on $\beta(y_i)$.

A prefix is defined recursively as follows: <Q> is a prefix for any poq Q, and $\neg P_1$ and $P_1 \wedge P_2$ are prefixes for any prefixes P_1 and P_2.

A matrix is a quantifier-free formula of L.

A well formed formula of Q is a formula of the form PM, where P is a prefix and M a matrix.

We abbreviate $\neg$<Q> to [Q], and $\neg(\neg P_1 \wedge \neg P_2)$ to $(P_1 \vee P_2)$.

We now set ourselves to define the semantics of wff's of Q by gathering that part of a prefix P which essentially quantifies on second order variables, on the left, and attaching the other (first order) part of P to the matrix M. For the reader familiar with the standard semantics given in [1] and [2], this step can be seen to be a natural one, once he is willing to admit that the x_i's in (*) are artificial constructs which serve to help define the existential second order character of a poq.

The second order part of P (sop(P)) and Skolem form of P and w (sf(P,w)) are defined recursively for any prefix P and wff w in L as follows:

If Q is a poq of the form (*) then

$$\underline{sop}(<Q>) = \exists f_1^Q, \ldots, \exists f_m^Q$$

where the f_i^Q are new function symbols.

$$\underline{sop}(\neg P) = \underline{dual}(\underline{sop}(P))$$

where $\underline{dual}(\exists f\pi) = \forall f\underline{dual}(\pi)$ and $\underline{dual}(\forall f\pi) = \exists f\underline{dual}(\pi)$ for any second order prefix π, and dual of the empty prefix is defined to be empty.

$$\underline{sop}(P_1 \wedge P_2) = \underline{sop}(P_1) \circ \underline{sop}(P_2)$$

where $\pi_1 \circ \pi_2$ is defined for any two disjoint second order prefixes as their merge, with $\exists$ preceeding $\forall$. Thus $\exists f_1 \forall f_2 \forall f_3 \exists f_4 \circ \forall f_5 \exists f_6 \exists f_7$ is e.g. $\exists f_1 \forall f_2 \forall f_3 \forall f_5 \exists f_4 \exists f_6 \exists f_7$ or $\exists f_1 \forall f_3 \forall f_2 \forall f_5 \exists f_7 \exists f_4 \exists f_6$ etc.
In order to make this definition unique we fix some ordering on the function symbols of L and merge within each run of the same type of quantifier, according to that order. Thus, if in the above example the f's are ordered by ascending indices, then the first alternative will be chosen. Note that $\underline{sop}(P_1 \vee P_2)$ is the dual merge of $\underline{sop}(P_1)$ and $\underline{sop}(P_2)$, that is, with $\forall$ preceeding $\exists$.

$$\underline{sf}(<Q>, w) = \forall x_1, \ldots, \forall x_n (w^Q)$$

where w^Q is w with $f_i^Q(\beta(y_i))$ substituted for every free occurence of y_i in w.

$$\underline{sf}(\neg P, w) = \neg\underline{sf}(P, w)$$

$$\underline{sf}(P_1 \wedge P_2, w) = \underline{sf}(P_1, \underline{sf}(P_2, w))$$

Given a model I for L we say that I satisfies PM (written $I \models PM$) iff $I \models \underline{sop}(P)\underline{sf}(P,M)$.

A prefix P will be called a Σ_i^1 prefix and denoted by $P^{<i>}$, if $\underline{sop}(P)$ is a Σ_i^1 quantifier-prefix in the usual sense (see [3]); similarly, a Π_i^1 prefix will be denoted by $P^{[i]}$.

Results

In order to simplify the exposition of the following, we use the following notational convenience. For sets of formulae S and T of $\mathcal{Q}$ and L respectively, we write $S \equiv T$ to express the fact that for any $PM \in S$ there exists $w \in T$ such that $\models w \equiv \underline{sop}(P)\underline{sf}(P,M)$, and vice versa.

The following theorem establishes a tight link between alternating second order quantifiers in L, and forming conjunctions of alternating poq's in $\mathcal{Q}$.

Theorem - For $i \geq 0$,

(a) $(\langle Q\rangle \wedge P^{[i]})M \equiv \Sigma^1_{i+1}$,

(b) $([Q] \vee P^{\langle i\rangle})M \equiv \Pi^1_{i+1}$.

Proof - Surely, given a prefix P' of the form $\langle Q\rangle \wedge P^{[i]}$, by definition $\underline{sop}(P')$ is a Σ^1_{i+1} prefix and $\underline{sf}(P',M)$ has no second order quantifiers. Negation gives this direction for (b).

We concentrate on the $\Leftarrow$ direction. For $i=0$ (a) simplifies to $\langle Q\rangle M \equiv \Sigma^1_1$, which is shown in Walkoe[2] and Enderton[1], and negation gives (b).

Assume (a) and (b) hold for $i-1$ where $i>0$. Given a Σ^1_{i+1} formula in prenex form, w: $\exists f_1,\ldots,\exists f_k \alpha R$, with matrix R and Π^1_i prefix α. Use the inductive hypothesis to come up with $([Q'] \vee P'^{\langle i-1\rangle})M'$ equivalent to αR. Denoting by $P^{[i]}$ the prefix $[Q'] \vee P'^{\langle i-1\rangle}$, we use a generalization of Walkoe's technique in essence, to construct $\langle Q\rangle$ and M such that $(\langle Q\rangle \wedge P^{[i]})M$ is equivalent to w:

Let there be n_j appearances of f_j in M', for $1 \leq j \leq k$, and let the arity of f_j be m_j. Define Q to be the poq

$(u^1_{1,1}, u^1_{1,2}, \ldots, u^1_{1,m_1}, u^1_{2,1}, \ldots, u^1_{n_1,m_1}, u^2_{1,1}, \ldots, u^k_{n_k,m_k}$;
$v^1_1, \ldots, v^1_{n_1}, v^2_1, \ldots, v^k_{n_k}$; $\beta)$ with $\beta(v^j_h) = (u^j_{h,1}, \ldots, u^j_{h,m_j})$,

where all the various v's and u's stand for new variables not appearing in $P^{[i]}M$. $\langle Q\rangle$ can be comprehended more easily by visualizing it as

$$\left(\begin{array}{l}
\forall u^1_{1,1}\ldots\forall u^1_{1,m_1}\exists v^1_1 \\
\forall u^1_{2,1}\ldots\forall u^1_{2,m_1}\exists v^1_2 \\
\quad\ldots\qquad\ldots \\
\forall u^1_{n_1,1}\ldots\forall u^1_{n_1,m_1}\exists v^1_{n_1} \\
\quad\ldots\qquad\ldots \\
\quad\ldots\qquad\ldots \\
\forall u^k_{1,1}\ldots\forall u^k_{1,m_k}\exists v^k_1 \\
\quad\ldots\qquad\ldots \\
\forall u^k_{n_k,1}\ldots\forall u^k_{n_k,m_k}\exists v^k_{n_k}
\end{array}\right)$$

We now transform M' into a matrix M of the form $R\wedge(S\rightarrow M'')$ by the following process: R is taken to be the formula

$$\bigwedge_{j=1}^{k}\left(\bigwedge_{h=1}^{n_j-1}\left(\left(\bigwedge_{p=1}^{m_j} u^j_{h,p}=u^j_{h+1,p}\right)\rightarrow v^j_h=v^j_{h+1}\right)\right)$$

which essentially states that all the "lines" of $\langle Q\rangle$ which correspond to some f_j define the same function.

We now consider the appearances of the f_j's in M', working "from within". These $q=n_1+\ldots+n_k$ appearances can be ordered by dependency, starting with those in which some f_j is applied to f-free terms. Define $M''_\emptyset$ as M' and $S_\emptyset$ as <u>true</u>. Assume the r'th appearance in the above order is $f_j(t_1,\ldots,t_{m_j})$, then M''_r is defined to be

M''_{r-1} with the appropriate v^j_h substituted for this appearance, and

S_r is $S_{r-1}\wedge\bigwedge_{s=1}^{m_j}(u^j_{h,s}=t_s)$.

Take M" to be M''_q, and S to be S_q.

This process completes the construction of $(\langle Q\rangle\wedge P^{[i]})M$. We now sketch the argument which serves to prove that $\models w\equiv\underline{sop}(P)\underline{sf}(P,M)$ with P: $\langle Q\rangle\wedge P^{[i]}$

and M: $R\wedge(S\to M'')$. By definition,
$\underline{sop}(P)=\underline{sop}(\langle Q\rangle)\circ\underline{sop}(P^{[i]})=\exists g_1\ldots\exists g_q\underline{sop}(P^{[i]})$
for some new function symbols g_j, and
$\underline{sf}(P,M)=\underline{sf}(\langle Q\rangle,\underline{sf}(P^{[i]},R\wedge(S\to M'')))=\forall u^1_{1,1}\ldots\forall u^k_{n_k,m_k}(\underline{sf}(P^{[i]},R\wedge(S\to M''))^Q)$.
For the sake of the following remarks we abbreviate $\exists f_1\ldots\exists f_k$ to $\exists f$, $\exists g_1\ldots\exists g_q$ to $\exists g$ and $\forall u^1_{1,1}\ldots\forall u^k_{n_k,m_k}$ to $\forall u$.
Surely $\forall u(\underline{sf}(P^{[i]},R\wedge(S\to M''))^Q)$ is logically equivalent to $\forall u(R^Q)\wedge\forall u(\underline{sf}(P^{[i]},S\to M'')^Q)$. Careful application of the definitions involved establishes the additional fact that $\forall u(\underline{sf}(P^{[i]},S\to M'')^Q)$ is in fact logically equivalent to $\underline{sf}(P^{[i]},(M')^g_f)$ where $(M')^g_f$ is M' with the corresponding new function symbols $g_1\ldots g_q$ replacing the q appearances of the symbols $f_1\ldots f_k$.

Using the inductive hypothesis, all we have left to show is the equivalence of

w_1: $\exists f\underline{sop}(P^{[i]})\underline{sf}(P^{[i]},M')$ and

w_2: $\exists g\underline{sop}(P^{[i]})(\forall u(R^Q)\wedge\underline{sf}(P^{[i]},(M')^g_f))$.

Indeed, $I\models w_1$ asserts the existence of an assignment of k functions to the symbols $f_1\ldots f_k$ satisfying $\underline{sop}(P^{[i]})\underline{sf}(P^{[i]},M')$.
To obtain $I\models w_2$, simply assign to $g_1\ldots g_{n_1}$ the function assigned to f_1; to $g_{n_1+1}\ldots g_{n_1+n_2}$ the function assigned to f_2; etc.
Trivially $\forall u(R^Q)$ is satisfied, and hence $I\models w_2$.
Conversely, if $I\models w_2$, $\forall u(R^Q)$ forces the assignment to $g_1\ldots g_q$ to be such that $g_1\ldots g_{n_1}$ are assigned the same function; $g_{n_1+1}\ldots g_{n_1+n_2}$ are assigned the same function; etc.
This assignment of k functions to the g's, when transformed appropriately to the f_j's yields $I\models w_1$. ▮

As an example of the technique of the proof of the theorem, take w to be $\exists f_1\exists f_2\alpha R$, and M' to be of the form $M'(f_1(g(x),f_2(y)),f_2(f_1(f_2(z),x)))$, involving these two terms and possibly other f_i-free terms. Using new variable symbols v_j and u_j, we take $\langle Q\rangle$ to be $\langle u_1,\ldots,u_7;v_1,\ldots,v_4;\beta\rangle$, with $\beta(v_1)=\{u_1,u_2\}$, $\beta(v_2)=\{u_3,u_4\}$ and $\beta(v_j)=\{u_{j+2}\}$ for $3\le j\le 5$, more vividly displayed as

$$\begin{pmatrix} \forall u_1 \forall u_2 \exists v_1 \\ \forall u_3 \forall u_4 \exists v_2 \\ \forall u_5 \exists v_3 \\ \forall u_6 \exists v_4 \\ \forall u_7 \exists v_5, \end{pmatrix}$$

and M as

$$((u_1=u_3 \& u_2=u_4) \to v_1=v_2 \;\&\; u_5=u_6 \to v_3=v_4 \;\&\; u_6=u_7 \to v_4=v_5) \;\&$$
$$(y=u_5 \& z=u_6 \& g(x)=u_1 \& x=u_4 \& v_3=u_2 \& v_4=u_3 \& v_2=u_7) \to R(v_1,v_5).$$

<u>Corollary</u> - $\mathcal{Q} \equiv L$.

<u>Proof</u> - The previous theorem establishes the equivalence in expressive power, of L and a subset of the wff's of $\mathcal{Q}$. Conversely, by the definition of I ⊨ PM, every wff of $\mathcal{Q}$ is equivalent to a formula of L. ∎

<u>Acknowledgments</u>

The author is indebted to W.J. Walkoe for pointing out a flaw in a previous version. The idea for this paper was motivated by work with V.R. Pratt related to program semantics. Discussions with A.R. Meyer and a detailed reading of a previous version by A. Shamir proved very helpful. This research was partially supported by the National Science Foundation under contract No. MCS76-18461.

<u>References</u>

[1] H.B.Enderton, "Finite Partially Ordered Quantifiers", Zeitschr. J. Math. Logik und Grundlagen d. Math, Bd.16, S.393-397, 1970.

[2] W.J.Walkoe, "Finite Partially Ordered Quantification", The Journal of Symbolic Logic, Vol.35, No.4, Dec.1970.

[3] H. Rogers, "Theory of Recursive Functions and Effective Computability", McGraw-Hill, 1967.