Monadic Counting Does Not Suffice

Steven Lindell, Haverford College 6/21/95 revised 7/02

Abstract: *This result separates monadic from dyadic counting over finite ordered structures. It is proved by showing that in the absence of any other relations, the former is a decidable theory, while the latter is not.*

Definitions: Let **mVT**(<) denote monadic variable-threshold◊ logic over ordered structures. The *variable-threshold* quantifier $(\exists^{>i}x)\varphi$ which binds x in φ and leaves i free is true just in case there are more than i elements x which make φ true. This monotone, symmetric quantifier is well-defined and unambiguous for all i ($i = 0$ gives first-order), and closed under negation over finite structures in the presence of addition via $\neg(\exists^{>i}x)\varphi \Leftrightarrow (\exists^{>n-1-i}x)\neg\varphi$. Also, note that the semantics of the variable threshold quantifier also make sense on the domain of the natural numbers **N**.

Background: Addition is definable in **mVT**(<) from $i - j = k \Leftrightarrow (\exists^{=k}x)[j < x \leq i]$. Multiplication is easily defined *dyadically* (quantification over pairs) as $i \times j = k \Leftrightarrow (\exists^{=k}\langle u, v\rangle)[u < i \wedge v < j]$. Conversely, it can be shown that monadic threshold quantification suffices in the presence of ×. We show that it does not suffice in the absence of ×.

Theorem: Primality is not definable in **mVT**(<) over the class of structures $\{\langle n, 0, +\rangle : n \in \omega\}$.†

Proof: *(high-level sketch)* We'll show that every sentence φ of **mVT**(<) has an eventually periodic spectrum.‡

1. Construct a formula $\varphi'(n)$ in which all variables x in φ have been bounded by a new free variable n, by adding clauses $x < n$. Observe that $n \models \varphi$ if and only if $\mathbf{N} \models \varphi'(n)$.

2. Proceed to show that φ' admits the same elimination of quantifiers as Presburger arithmetic [Enderton, p.188]. Only two modifications to the proof are required.

3. Set $M = 2^m$, and then convert $(\exists^{>z}x)[\alpha_1 \vee \ldots \vee \alpha_m]$ to: (*cf. ibid* Theorem 31F p. 181)

$$(\forall z_1 \ldots z_{M-1}) \quad [(\bigwedge_{b=1}^{M-1} z_b = |\bigcap_{i=1}^{m} \{\alpha_i : b(i) = 1\}|) \rightarrow (\sum_{b=1}^{M-1} z_b \cdot (-1)^{\#b+1} > z)]$$

   where $\#b$ is the number of ones in the binary representation of b, and $b(i)$ is the i^{th} bit of b. The conclusion expresses the combinatorial inclusion-exclusion principle, which counts a finite number of elements in a set union in terms of set intersections, whereas the hypothesis finds the exact number of elements in each component so that

$$z = |\alpha| \equiv \neg(\exists^{>z}x)\alpha \wedge (\exists^{>z-1}x)\alpha$$

   when α is finite, and is automatically false if any of the components is infinite. The net result is a first-order combination of threshold quantifiers applied only to conjuncts which replaces the original formula.

4. Follow the proof in [Enderton] without further change until the very end (p. 191). Instead of ascertaining if there is a congruential element in the gap between the upper and lower bounds, just express the least-upper and greatest-lower bounds using **min** and **max** (over the fixed number of formulas) and compare the number of elements in the gap (subtract, then express using **div** m, for the fixed m) to the threshold z. This last step introduces a first-order quantifier (in **div** m), which we eliminate using the original proof. Q.E.D.

Corollary: $\times \notin$ **mVT**(<) $\neq$ Logspace.

Reference: [Enderton] A Mathematical Introduction to Logic, 1st edition.

◊ We have chosen this terminology because "threshold" more accurately describes a quantifier, whereas *counting* refers to a term constructor ([cf. M. Otto, Bounded Variable Logics and Counting - A Study in Finite Models, *Lecture Notes in Logic* volume 9, Springer 1997]). The term "variable" emphasizes the fact that the threshold is parameterized, to help eliminate a common source of confusion. Since **VT** subsumes first-order logic, the latter is not mentioned.

† Actually, the proof will show more: *Satisfiability for* **mVT**(<) *is decidable.* Therefore we cannot express multiplication, because even the quantifier-free logic of + and × can express classes of problems (like Diophantine equations) which are undecidable (Hilbert's 10th problem).

‡ As a consequence of showing that **mVT**(<) = **FO**(+) on signatures with no additional relations [Enderton, p.192].