Internal Note #032
Computational Logic Inc.
July 11, 1988

A Counterexample to the 0-1 Law for Existential Monadic Second-Order Logic

Matt Kaufmann

A Counterexample to the 0-1 Law for Existential Monadic Second-Order Logic

Matt Kaufmann
Computational Logic, Inc.
1717 W. Sixth Street, Suite 290
Austin, TX 78703

For any sentence ϕ of any logic and any **n** > 0, one may define the $\mathbf{n}^{th}$ probability of ϕ to be the fraction of structure for the vocabulary of ϕ with universe **{0,1,...,n-1}** which satisfy ϕ. The the *limit probability* of ϕ is the limit of the $\mathbf{n}^{th}$ probability of ϕ as **n** goes to infinity, which may or may not exist. Fagin [1] and independently Glebskii, Kogan, Liogon'kii, and Talanov [2] proved that the limit probability of a first-order sentence is always 0 or 1. In the paper [3] it was shown that this "0-1 law" fails badly for monadic second-order logic, i.e. that part of second-order logic in which the only second-order quantifiers are over unary relations (though a vocabulary may still contain relation symbols of any finite arity). In this note we show that this law still fails when one further restricts the logic to extend first-order logic only by allowing formulas of the form $(\exists\ \mathbf{P_1})\ \ldots\ (\exists\ \mathbf{P_n})\ \phi$ where ϕ is first-order, which we will refer to as existential monadic second-order logic.

Acknowledgements. I thank Phokion Kolaitis for bringing the question for existential monadic second-order logic to my attention.

Theorem 1. There is a sentence of existential monadic second-order logic which has no limit probability.

Theorem 2. For every rational number **r** in the interval [0,1] there is a sentence of existential monadic second-order logic which has limit probability **r**.

The main lemma for the proofs of these theorems will be the following, whose proof we'll defer for the moment.

Main Lemma. There is a first-order formula $\phi(x,y)$ in a vocabulary which includes a sequence of unary relation symbols $\overline{P}$ such that the following sentence has limit probability 1:

$$(\exists\ \overline{P})\ \text{"}\phi(x,y)\text{ defines a linear order of the universe"}$$

Given the Main Lemma, we may prove the theorems as follows. For the first, we simply use the following sentence, where ϕ is as in the Main Lemma. Notice that it simply says of a finite structure that its universe has an odd number of elements.

$$\begin{array}{l}(\exists\ \overline{P})\ (\exists\ Q)\\ \quad [\ \text{"}\phi(x,y)\text{ defines a linear order of the universe}\\ \qquad \text{such that } Q \text{ contains every other element, including}\\ \qquad \text{the first and last" }]\end{array}$$

Now notice that we can get a sentence of limit probability 1/2 simply by modifying this sentence to say that **Q** contains every other element of the restriction of this linear order to an arbitrary set **S** (here **S** is a unary relation symbol of the vocabulary), including the first and last elements of **S**. The extension of this idea to complete the proof of the second theorem is simple; given a fraction **p/q**, simply say that for some **Q** contained in **S**, **Q** contains every q^{th} element of **S** starting with the first, and there are exactly p elements left over at the end. We omit the details of showing that the limit probability is indeed **p/q**.

To prove the Main Lemma we start with some notation and definitions regarding the notion of coding subsets.

Definitions. Let **A** and **B** be subsets of a structure $(C;R,...)$, where **R** is binary (and we also use **R** for the symbol that it interprets).

(i) For $b \in B$, we say that **b** **R**-*codes* $\{a \in A:\ \langle a,b\rangle \in R\}$ *with respect to* **A**. (We omit the "with respect to" part when it is clear from context, which is always, and we also say "codes" in place of "**R**-codes" when **R** is clear from context or unimportant to specify.)

(ii) We say that **B** *codes distinct subsets of* **A** if no two elements of **B** code the same subset of **A**.

(iii) We say that **B** *codes the power set of* **A** if **B** codes distinct subsets of **A** and moreover every subset of **A** is coded by an element of **B**.

The following lemma shows that the power set of a small enough set is probably coded.

Lemma 1. If $\mathbf{S} \subseteq \mathbf{T} \subseteq \mathbf{A}$, where $(\mathbf{A};\mathbf{R},\ldots)$ is a finite structure, and if $|\mathbf{T}| \geq |\mathbf{S}|\,2^{|\mathbf{S}|}$ then with limit probability 1, some subset of **T** codes the power set of **S**.

<u>Proof</u>. It is enough to show that with probability 1, every subset of **S** is coded by an element of **T**. The probability of failure is less than or equal to the sum over all subsets $\mathbf{S'}$ of **S** of the probability that $\mathbf{S'}$ is not coded by an element of **T**. This individual probability is the product over all elements **t** of **T** of the (independent) probabilities that **t** does not code $\mathbf{S'}$, each of which is $(1 - 1/2^{|\mathbf{S}|})$. Thus, the probability of failure is at most

$$2^{|\mathbf{S}|} \cdot (1 - 1/2^{|\mathbf{S}|})^{|\mathbf{S}| \cdot 2^{|\mathbf{S}|}}$$

But the second factor is asymptotic with $1/e^{|\mathbf{S}|}$, so the limit is 0. -|

Lemma 2. Suppose that **S** and **T** are subsets of a structure $(\mathbf{A};\mathbf{R},\mathbf{S},\mathbf{T},\ldots)$ in which which **T** codes distinct subsets of **S** and such that there is a first-order definable total order **<** on **S**. Then there is a first-order definable total order on **T**. In fact, this definition is constructible from the given definition of **<** (independently of the particular choice of **S** and **T**).

<u>Proof</u>. One simply uses the lexicographic order on **T** (viewed as a family of subsets of **S**). That is, define a total order << on **T** as follows: **x** << **y** if and only if $\mathbf{x} \neq \mathbf{y}$ and for **a** equal to the <-least member of the symmetric difference of the sets coded by **x** and **y**, $\mathbf{a} \notin \mathbf{x}$. -|

Lemma 3. Let $\mathbf{R}$ be an arbitrary binary relation on $\{0,1,...,k-1\}$, and let $\mathbf{n}$ be an integer greater than $k^2 \cdot 4^k$. Let $\mathbf{p}$ be the probability that some substructure of a random model of the form $(\{0,...,n-1\};R')$ contains an isomorphic copy of $(\{0,1,...,k-1\},R)$ Then $\mathbf{p}$ approaches 1 as $\mathbf{k}$ approaches infinity (uniformly over such $\mathbf{n}$).

Proof. Imagine that one tries to build the requisite isomorphic embedding as follows. Let $a = k \cdot 4^k$. Partition the universe into $\mathbf{k}$ pieces each of size $\mathbf{a}$ (plus possibly one extra piece containing all elements left over, since $\mathbf{n}$ may exceed $a \cdot k$). At each stage $i < k$, attempt to extend the embedding by mapping $\mathbf{i}$ to some element of the i^{th} piece of the partition. Then the probability of failure is bounded above by the sum over $\mathbf{i}$ of the probabilities that there is no element of the i^{th} piece which lies in the appropriate relation to the $i-1$ elements of the range so far. The i^{th} such probability is $(1 - 1/4^{i-1})^a$. Hence the probability of failure is bounded above by $k(1 - 1/4^k)^a$. Recalling that $a = k \cdot 4^k$, it is easy to see that this bound approaches 0 as $\mathbf{k}$ approaches infinity. -|

Proof of Main Lemma. Fix a structure $(A;R,R_0,R_1,R_2)$, and pick $\mathbf{k}$ greatest such that $|A| \geq 2^k \cdot 2^{2^k}$. By Lemma 3, we may (with limit probability 1) choose $P_0 \subseteq A$ of power $\mathbf{k}$ such that the restriction of $\mathbf{R}$ to P_0 is a total order. (Notice that 2^{2^k} exceeds $k^2 \cdot 4^k$ for sufficiently large $\mathbf{k}$.) Next, by Lemma 1, we may (with limit probability 1) choose $P_1 \subseteq A$ which R_0-codes the power set of P_0, and then $P_2 \subseteq A$ which R_1-codes the power set of P_1. Since $|A| < 2^{k+1} \cdot 2^{2^{k+1}}$, an easy calculuation shows that with limit probability 1, A R_2-codes distinct subsets of P_2. To summarize: If we let P_3 be $\mathbf{A}$, then we have that P_{i+1} R_i-codes distinct subsets of P_i for i = 0, 1, 2. Thus by successive application of Lemma 2, there is a formula in the vocabulary $\{R,R_0,R_1,R_2,P_0,P_1,P_2\}$ (not depending on the particular choices of the *sets* P_i) which defines a total order of the universe, and this is the desired formula $\phi(x,y)$. -|

References

[1] Fagin, R., ‘‘Probabilities on Finite Models’’, *J. Symbolic Logic*, Vol. 41, 1976, pp. 50-58.

[2] Y. V. Glebskii, D. I. Kogan, M. I. Liogon’kii and V. A. Talanov, ‘‘Range and Degree of Realizability of Formulas in the Restricted Predicate Calculus’’, *Cybernetics*, Vol. 5, 1969, pp. 142-154 (translated 1972).

[3] Kaufmann, M. and Shelah, S., ‘‘On Random Models of Finite Power and Monadic Logic’’, *Discrete Mathematics*, Vol. 54, 1985, pp. 285-293.