Sh:201

Discrete Mathematics 54 (1985) 285–293
North-Holland

ON RANDOM MODELS OF FINITE POWER AND MONADIC LOGIC

Matt KAUFMANN*
Purdue University, West Lafayette, IN 47907, USA

Saharon SHELAH†
Mathematics Institute, Hebrew University, Jerusalem, Israel

Received 21 October 1983
Revised 31 August 1984

For any property ϕ of a model (or graph), let $\mu_n(\phi)$ be the fraction of models of power n which satisfy ϕ, and let $\mu(\phi) = \lim_{n\to\infty} \mu_n(\phi)$ if this limit exists. For first-order properties ϕ, it is known that $\mu(\phi)$ must be 0 or 1. We answer a question of K. Compton by proving in a strong way that this 0–1 law can fail if we allow monadic quantification (that is, quantification over sets) in defining the sentence ϕ. In fact, by producing a monadic sentence which codes arithmetic on n with probability $\mu = 1$, we show that every recursive real is $\mu(\phi)$ for some monadic ϕ.

For any sentence ϕ of any logic, let $\mu_n(\phi)$ be the fraction of models of cardinality n which satisfy ϕ. (A precise definition appears in Definition 1 below.) Then let $\mu(\phi) = \lim_{n\to\infty} \mu_n(\phi)$, if this limit exists. Fagin [2] and independently Glebskii, Kogan, Liogon'kii, and Talanov [4] proved that $\mu(\phi)$ is 0 or 1 for each first-order sentence ϕ without function or constant symbols. A related result for the space of countable models was proved by Gaifman [3]. For other related references the reader may consult Lynch [5] and Compton [1].

In second-order logic one allows quantification over arbitrary relations. For this logic the limit $\mu(\phi)$ need not even exist; for example, if $|A| = n$ then A satisfies "there is a permutation of order 2 without fixed points" iff n is even. This example disappears if we restrict the second-order quantifiers to quantifiers over *sets*. The resulting logic is called *monadic second-order logic*. Note that we allow n-place relation symbols in the vocabulary. If the vocabulary is restricted to unary predicates, then it is known that the 0–1 law holds. The following question of K. Compton appears in [6]: does $\mu(\phi)$ exist and equal 0 or 1 for all monadic second-order ϕ? In this paper we answer this question negatively in a strong way by proving Theorem 2 below. First let us formally give the requisite definition.

* Current address: Austin Research Centre, Burroughs Corporation, Austin, TX 78727, USA.
† Support from the NSF and the United States–Israel Binational Science Foundation is gratefully acknowledged.

Notation. We identify each natural number n with the set of its predecessors, i.e. $n = \{0, 1, \ldots, n-1\}$.

Definition 1. Let L be a finite vocabulary. (Usually L will consist of a single binary relation symbol R.) Let S_n be the space of all L-structures with universe $\{0, 1, \ldots, n-1\} = n$. Then set $\mu_n(\phi) = |\{\mathfrak{A} \in S_n : \mathfrak{A} \models \phi\}|/|S_n|$. If $\lim_{n\to\infty} \mu_n(\phi)$ exists, we denote this limit by $\mu(\phi)$.

We are about ready to state the main theorem and its consequence that answers Compton's question. Let $+\restriction n$ denote $\{\langle x, y, z\rangle \in n \times n \times n : x + y = z\}$; similarly for $\times \restriction n$. Notice that in first-order logic one may assert (of a finite model) that $\langle n, \phi(x, y, z, \ldots), \psi(x, y, z, \ldots)\rangle \cong \langle n, +\restriction n, \times\ n\rangle$, where n is the cardinality of the model but this sentence does not depend on n. Let us abbreviate this sentence by "$\langle \phi, \psi\rangle \cong \langle +, \times\rangle$".

Theorem 1. *There are monadic second-order formulas* $\phi_+(x, y, z, \bar{P}, R)$ *and* $\phi_\times(x, y, z, \bar{P}, R)$, *where* R *is a binary relation symbol and* $\bar{P}$ *is a sequence of unary relation symbols, such that the following sentence has probability* $\mu = 1$:

$$\exists \bar{P}(\langle \phi_+(x, y, z, \bar{P}, R), \phi_\times(x, y, z, \bar{P}, R)\rangle \cong \langle +, \times\rangle)$$

(*where this abbreviation is defined above*).

The following result implies that there are sentences of monadic second-order logic which have no limit and sentences with any recursive real as the limit.

Theorem 2. *Let* T *be any recursively enumerable tree of finite sequences of zeros and ones, without terminal nodes. Then there is a sentence* ϕ *of monadic second-order logic such that the set of subsequential limits from* $\langle \mu_n(\phi) : n \in \mathbb{N}\rangle$ *equals the set of reals of the form* $\sum\{2^{-i-1} : b(i) = 1\}$ *for* b *ranging over the branches of* T, *i.e.* $b \restriction n \in T$ *for all* $n \in \mathbb{N}$.

The solution given by Theorem 2 is due to Shelah. Before giving the proofs of Theorems 1 and 2, we outline a simpler but less powerful example, due (independently of Shelah) to Kaufmann and J. Schmerl, which hints at the power of monadic second-order logic.

Suppose $\mathfrak{A} = (A, R, \ldots)$ is a finite structure with $R \subseteq A^2$. If $X \subseteq A$, say X is *R-suitable* if for all $x, y \in X$ there is $a \in A$ such that $(\forall z \in X)(Rza \leftrightarrow z = x \vee z = y)$. Let $n(R)$ be the largest k such that every subset of A of power k is R-suitable. Then there is a monadic second-order formula $\phi_R^{\leq}(X)$ which says that X has power at most $n(R)$. $\phi_R^{\leq}(X)$ is $\forall Z[$"$|X| <_R |Z|$"$\vee($"$|Z| <_R |X|$"$\wedge$"Z is R-suitable"$)]$, where "$|X| \leq_R |Z|$" is

$$\exists X_1 \exists X_2 \exists X_3 \exists Z_1 \exists Z_2 \exists Z_3 [X = X_1 \cup X_2 \cup X_3$$
$$\wedge\ Z \supseteq Z_1 \cup Z_2 \cup Z_3 \wedge \bigwedge_{1\leq i\leq 3} \exists P((\forall x \in X_i)(\exists!\, u \in P) Rxu$$
$$\wedge (\forall u \in P)(\exists!\, x \in X_i) Rxu \wedge (\forall z \in Z_i)(\exists!\, u \in P) Rzu \wedge (\forall u \in P)(\exists z \in Z_i) Rzu)],$$

and "$|X| <_R |Z|$" is similar except that $Z \supsetneq Z_1 \cup Z_2 \cup Z_3$. Let $\phi_R(X)$ say that $|X| = n(R)$, i.e. $\phi_R^{\leq}(X) \wedge \exists y \neg \phi_R^{\leq}(X \cup \{y\})$. Now consider a vocabulary with 2 binary relations R and S. We claim that the following sentence does not have probability 1: $\exists X(\phi_R(X) \wedge \phi_S(X))$, i.e. $n(R) = n(S)$. This will be seen to follow from the following observations.

(1) Let i_j = least i such that $\mu_j(n(R) = i)$ is a maximum (for fixed j). Then $\mu(n(R) = n(S)) = 1$ iff $\lim_{j\to\infty} \mu_j(n(R) = i_j) = 1$.

(2) For all k, $\mu(n(R) \geq k) = 1$.

(3) If $\mu_j(n(R) \leq i) > 1 - \varepsilon$ then $\mu_{j+1}(n(R) \leq i) > (1-\varepsilon)(1 - 2^{-(i+1)})$.

(1) is easy to prove, and (2) is an easy consequence of the fact that a first-order sentence ϕ holds in the countable universal homogeneous model iff $\mu(\phi) = 1$ (cf. Fagin [2]). To verify (3), given a random model of power $j+1$, pick a random submodel of power j. Assuming $\mu_j(n(R) \leq i) > 1 - \varepsilon$, with probability $> 1 - \varepsilon$ this submodel has a counterexample $\langle X; a, b \in X \rangle$ to $(i+1)$-suitability. The probability that the element c outside the submodel 'restores' X (i.e. $Rac \wedge Rbc \wedge (\forall x \in X)(Rxc \rightarrow x = a \vee x = b)$) is $2^{-(i+1)}$, and (3) follows. Now by (1) and (2), if $\mu(n(R) = n(S)) = 1$ then for all k there exist arbitrarily large j such that $i_{j+1} > i_j > k$. Setting $i = i_j$ this contradicts (3). Therefore $\mu_n(n(R) = n(S)) \not\rightarrow 1$.

Finally, since $\mu(n(R) = n(S)) \neq 1$ (if indeed this limit exists at all), then since $\mu_n(n(R) > n(S)) = \mu_n(n(S) > n(R))$ for all n, we see that $\mu(n(R) > n(S))$ is neither 0 nor 1. We do not know if $\mu(n(R) = n(S))$ exists. There is also a monadic second-order sentence ψ asserting that $n(R)$ is an even number. While it seems likely that $\mu(\psi) = \frac{1}{2}$, we do not even know whether $\mu(\psi)$ exists.

We turn now to:

Proof of Theorem 1. Fix n, and let k be the unique integer satisfying $2^{3k} \leq n < 2^{3(k+1)}$. Also fix $B = \{0, 1, \ldots, k-1\}$ and $C = \{0, 1, \ldots, 10k-1\}$; then $B \subseteq C$. We will code arithmetic on 2^k by coding all subsets of B, and then viewing these codes as binary expansions of numbers less than 2^k. Then we will view elements of n (recall $n = \{0, 1, \ldots, n-1\}$) as coding distinct subsets of C, and use this idea together with the arithmetic on 2^k to code arithmetic on n. We begin by proving three claims which say that with probability 1, we can do such coding.

(1) Let ψ_0 say that for all $A \subseteq B$, there is α such that $A = \{l \in B: lR\alpha\}$. Then $\mu(\psi_0) = 1$.

Proof. For each $A \subseteq B$ and $\alpha < n$ the probability of "$A = \{l \in B: lR\alpha\}$" is 2^{-k}. These are independent events as α varies over elements of n. Hence the probability that $(\forall \alpha \in n)\ (A \neq \{l \in B: lR\alpha\})$ is $(1 - 2^{-k})^n \sim e^{-n/2^k} \leq e^{-2^{2k}}$, so the probability that this occurs for some $A \subseteq B$ is $\leq 2^k e^{-2^{2k}} \leq e^{-\sqrt{n}}$.

(2) Let ψ_1 say that for all distinct $\alpha, \beta \in C$, $\{l \in B: lR\alpha\} \neq \{l \in B: lR\beta\}$. Then $\mu(\psi_1) = 1$.

Proof. For each pair $\alpha \neq \beta$ the probability that $\{l \in B: lR\alpha\} = \{l \in B: lR\beta\}$ is 2^{-k}. So the probability that this holds for some $\alpha, \beta \in C$ is at most $|C|^2 2^{-k} = 100k^2 2^{-k} < n^{-1/4}$ for sufficiently large n.

(3) Let ψ_2 say that for all $\alpha<\beta<n$, $\{l\in C: lR\alpha\}\neq\{l\in C: lR\beta\}$. Then $\mu(\psi_2)=1$.

Proof. $\mu_n(\neg\psi_2)\leq n^2\,2^{-|C|}\leq 2^{6(k+1)}\,2^{-10k}=2^{-4k+6}\to 0$, and (3) follows.

By (1), (2), and (3) we may assume henceforth that the model $M=(n,R)$ satisfies $\psi_0\wedge\psi_1\wedge\psi_2$. No more probability arguments will appear. *Rather, we will expand M by adding various unary predicates so that addition and multiplication restricted to n are definable in the expanded structure by certain formulas ϕ and ψ (respectively).* This of course yields the theorem. For a technical reason we also assume $10k<[\sqrt{2^k}]$.

Our first step is to expand M to a structure M_0 (adding only unary predicates) so that there is a linear order on B definable in M_0. In fact, as $B=\{0,1,\ldots,k-1\}$ we would like the natural order on B to be definable in such an expansion M_0, and this is easily arranged as follows. For each $i<k$ choose $\alpha_i<n$ such that $\{0,1,\ldots,i\}=\{j<k: jR\alpha_i\}$; this is possible as $M\models\psi_0$. Then let $S=\{\alpha_i: i<k\}$. Clearly, for $i,j<k$ we have $i<j$ iff $(\exists\alpha\in S)(iR\alpha\wedge\neg jR\alpha)$.

It will be convenient to allow quantification over two-place relations on B. This practice keeps us in the realm of *monadic* second-order logic, however, as we now show. First notice that since $M\models\psi_0$, for every $\alpha\neq\beta$ from $B(=k)$ there is some $x_{\{\alpha,\beta\}}<n$ such that $\{\alpha,\beta\}=\{l\in B: lRx_{\{\alpha,\beta\}}\}$. For any relation $S\subseteq B^2$, then, we may associate sets $X,Y\subseteq n$ so that $X=\{x_{\{\alpha,\beta\}}:\alpha\leq\beta<k$ and $\alpha S\beta\}$ and $Y=\{x_{\{\alpha,\beta\}}:\beta<\alpha<k$ and $\alpha S\beta\}$. Notice that if $x_{\{\alpha,\beta\}}=x_{\{\gamma,\delta\}}$ then $\alpha=\gamma$ and $\beta=\delta$. It is then clear that S can be recovered from X and Y, so for any monadic $\theta(S,\ldots)$ there is a monadic $\theta'(X,Y,\ldots)$ such that in M_0 (or indeed, in any expansion of M_0), $(\exists S\subseteq B^2)\theta\leftrightarrow(\exists X)(\exists Y)\theta'(X,Y,\ldots)$. Henceforth we will freely use quantification over binary relations on B. In particular, $+$ and $\times$ restricted to $k=B$ are definable in M_0.

Since $M\models\psi_0\wedge\psi_1$ we may extend C to represent all of the subsets of B. Hence we may (monadically) expand M_0 to a structure M_1 which has the following properties:

(4) The predicate "$x\in B$" (i.e. $x<k$) is definable in M_1, as is the usual order on k. Also C is definable in M_1 (recall $C=\{0,1,\ldots,10k-1\}$), as is a set $D\supseteq C$ of power 2^k such that $(\forall\alpha\in D)\,(\forall\beta\in D)\,[\alpha\neq\beta\to\{l\in B: lR\alpha\}\neq\{l\in B: lR\beta\}]$. We may quantify over binary relations on B. In particular, arithmetic on B is definable in M_1.

Now define a function $f:D\to 2^k$ by $f(\alpha)=\sum\{2^i: iR\alpha, i\in B\}$. We claim:

(5) The relation $R_+=\{\langle\alpha,\beta,\gamma\rangle:\alpha,\beta,\gamma\in D$ and $f(\gamma)=f(\alpha)+f(\beta)\}$ is definable in M_1.

For, let $X\subseteq B=k$ be the set of places where there is a carry in the addition $f(\alpha)+f(\beta)$, i.e. where $\sum\{2^j: jR\alpha, j<i\}+\sum\{2^j: jR\beta, j<i\}\geq 2^i$. Choose $\delta\in D$ such that $\{l\in B: lR\delta\}=X$. Now the requirements for $f(\gamma)=f(\alpha)+f(\beta)$ are local. That is, $f(\gamma)=f(\alpha)+f(\beta)$ iff for some δ, the right thing happens at each coordinate;

that is, iff: $iR\gamma \leftrightarrow [(iR\alpha \leftrightarrow iR\beta) \leftrightarrow iR\delta]$ for all $i<k$; $\neg\, 0R\delta$; $(i+1)R\delta \leftrightarrow [(iR\delta \wedge iR\alpha) \vee (iR\delta \wedge iR\beta) \vee (iR\alpha \wedge iR\beta)]$ for all $i<k-1$; and $\neg[((k-1)R\delta \wedge (k-1)R\alpha) \vee ((k-1)R\delta \wedge (k-1)R\beta) \vee ((k-1)R\alpha \wedge (k-1)R\beta)]$ (so that $f(\alpha)+f(\beta)<2^k$). Hence (5) holds. Now we prove

(6) The relation $R_\times = \{\langle \alpha, \beta, \gamma\rangle \in D^3 : f(\alpha)\cdot f(\beta) = f(\gamma)\}$ is definable in M_1.

Given $\alpha, \beta \in D$ with $f(\alpha)\cdot f(\beta)<2^k$, we define γ (uniformly in α and β) such that $f(\alpha)\cdot f(\beta)=f(\gamma)$, as follows. Let $f(\alpha)=\sum \alpha_i 2^i$ and $f(\beta)=\sum \beta_i 2^i$. Consider the matrix $S\subseteq B^2$ formed (roughly) by putting $\sum \alpha_i 2^{i+j}$ in column j if $\beta_j \neq 0$, otherwise putting all zeros in column j. Formally, set $S=\{\langle i,j\rangle \in B^2 : j\leqslant i$ and $(i-j)R\alpha$ and $jR\beta\}$. Now the intuitive idea is that $f(\alpha)\cdot f(\beta)$ is the sum of the columns of S, that is, $\sum\{\sum\{2^i : \langle i,j\rangle\in S\} : j<k\}$. So let $T\subseteq B^2$ represent the partial sums, that is, the jth column of T should represent the sum of the first j columns of S. Formally, T is characterized by setting $\langle i,0\rangle\in T$ iff $\langle i,0\rangle \in S$, and $\langle i,j+1\rangle\in T$ iff there are δ,η,ν with $\{i<k : iR\delta\}=\{i<k:\langle i,j\rangle\in T\}$, $\{i<k: iR\eta\}=\{i<k:\langle i,j+1\rangle \in S\}$, and $f(\nu)=f(\delta)+f(\eta)$ (which is definable, by (5)). Finally, $f(\alpha)\cdot f(\beta)=f(\gamma)$ iff there are such S and T such that γ codes the last column of T: $(\forall i<k)\ (iR\gamma \leftrightarrow \langle i, k-1\rangle\in T)$. Since by (4) we are allowed quantification over binary relations on B, this concludes the proof of (6).

At this point we turn to the problem of defining arithmetic on n rather than merely on 2^k. As $M\models\psi_2$ we can view n as a subset of $2^{|C|}$. The idea is to code each element of M (i.e. of n) by the number of predecessors it has in M, under the lexicographic order on $2^{|C|}$. We use the arithmetic available on 2^k to carry out this coding. Notice that by replacing M_1 with an isomorphic copy (in which B and C are fixed pointwise by the isomorphism), we may assume by (5) and (6) that:

(7) $D=2^k$, and setting $E=\{l : l^2<2^k\}$, we have 'plus' and 'times' on E definable in M_1. Also we can code binary relations on E in M_1: for $S\subseteq E^2$, consider $\{i\cdot[\sqrt{2^k}]+j : \langle i,j\rangle\in S\}$.

We now prove:

(8) In M_1, we can define the relation "$x\in E \wedge |X|=x$".

To see this, notice that for $x\in E$, we have $|X|=x$ iff there is $S\subseteq x\times 10k$ such that for all $i<x$, $\{l<10k: iSl\}=\{l<10k: lR'\alpha\}$ for some $\alpha\in X$, and conversely, every $\alpha\in X$ has this property for some unique $i<x$. By $M\models\psi_2$ and the last clause of (7), and since $10k\subseteq E$ (as we have assumed $10k<[\sqrt{2^k}]$), this argument proves (8).

At least we are ready to begin to define arithmetic on n, in M_1. Let $m=\max(E)$, and for $\alpha<n$ let $\|\alpha\|$ be the number of elements which precede α in the lexicographic order on 2^{10k}, in the following sense:

$$\|\alpha\| = |\{\beta : \text{for some } l<10k, lR\alpha \wedge \neg lR\beta \wedge (\forall i<l)(iR\alpha \leftrightarrow iR\beta)\}|.$$

Notice that the predicate $\|\beta\|<\|\alpha\|$ is definable in M_2. Thinking in base m, we see that there are unique $p^0_\alpha, p^1_\alpha, \ldots, p^6_\alpha < m$ such that $\|\alpha\| = \sum_{i=0}^6 p^i_\alpha m^i$ (as $m^7 > n$). We claim:

(9) The relations "m^i divides $\|\alpha\|$" (each $i = 1, 2, \ldots, 6$) and "$p^i_\alpha = l$" (each $i = 0, \ldots, 6$) are definable in M_1.

In fact (9) follows easily from (8). For example, m divides $\|\alpha\|$ iff for some $X \subseteq \{\beta : \|\beta\| < \|\alpha\|\} \cup \{\alpha\}$, we have $\alpha \in X$ and $\beta_0 \in X$ where $\|\beta_0\| = 0$, and for all $\beta, \gamma \in X$ with $\beta < \gamma$, if $(\forall\delta)(\|\beta\| < \|\delta\| < \|\gamma\| \to \delta \notin X)$ then $|\{\delta : \|\beta\| \leqslant \|\delta\| < \|\gamma\|\}| = m$. The higher powers are treated similarly. For example, "m^2 divides $\|\alpha\|$" is defined just like "m divides α", except that $|\{\delta : \|\beta\| \leqslant \|\delta\| < \|\gamma\|\}| = m^2$ for successive $\beta < \gamma$ in X: $(\exists Y)$ $(\beta \in Y \wedge \gamma \in Y \wedge (\forall \beta' \in Y)$ $(\forall \gamma' \in Y)$ $[(\forall\delta)$ $(\|\beta'\| < \|\delta\| < \|\gamma'\| \to \delta \notin Y) \to$ $|\{\delta : \|\beta'\| \leqslant \|\delta\| < \|\gamma'\|\}| = m]$. The higher powers m^i are handled similarly, that is, $|\{\delta : \|\beta\| \leqslant \|\delta\| < \|\gamma\|\}| = m^i$ for successive $\beta < \gamma$ in X, and this can be said by subdividing $\{\delta : \|\beta\| \leqslant \|\delta\| < \|\gamma\|\}$ $(i-1)$ times. The predicates "$p^i_\alpha = l$" are handled similarly.

Finally, we can easily define $\{\langle\alpha, \beta, \gamma\rangle : \|\alpha\| + \|\beta\| = \|\gamma\|\}$ in M_1, using (9) and (7). Also, by (9) and the distributive law, it is easy to reduce the problem of defining $\{\langle\alpha, \beta, \gamma\rangle : \|\alpha\| \cdot \|\beta\| = \gamma\}$ in M_1 to the problem of finding, for all $p_1, p_2 < m$, some $i, j < m$ such that $p_1 \cdot p_2 = im + j$. But since we have defined arithmetic up to m^2 in M_1, this is also routine, and the proof is complete. □

Theorem 2 is a rather direct consequence of the following lemma, which we will prove using Theorem 1.

Lemma. *Suppose that f and g are recursive functions such that $f(n) < g(n)$ for all n. Then there is a sentence ϕ of monadic second-order logic and a finite-to-one function h from $\mathbb{N}$ onto $\mathbb{N}$ such that $\lim_{n\to\infty} |\mu_n(\phi) - f(h(n))/g(h(n))| = 0$.*

In particular, given any recursively enumerable tree T of finite sequences of 0's and 1's (as in Theorem 2), we may apply this lemma to recursive functions f and g such that $\langle f(n)/g(n) : n \in \mathbb{N}\rangle$ enumerates T. (Here we are of course identifying a node $s \in T$ with the corresponding fraction $\sum\{2^{-(i+1)} : s(i) = 1\}$.) Then it is clear that for every branch b of T we can choose a subsequence from $\langle\mu_n(\phi) : n < \omega\rangle$ converging to $\sum\{2^{-(i+1)} : b(i) = 1\}$, where ϕ is the sentence given by the lemma. Conversely, if $\langle\mu_n(\phi) : n \in I\rangle$ is a convergent subsequence of $\langle\mu_n(\phi) : n \in \mathbb{N}\rangle$, then $\langle f(h(n))/g(h(n)) : n \in I\rangle$ converges, so since h is finite-to-one, there is a branch b of T such that $\langle f(h(n))/g(h(n)) : n \in I\rangle$ converges to $\sum\{2^{-(i+1)} : i \in b\}$, and Theorem 2 follows.

Proof of Lemma. Recall that a function f is recursive if and only if it is definable in $(\mathbb{N}, +, \cdot, <)$ by a formula $\exists\bar{u}\theta(x, y, \bar{u})$ where θ is Δ_0, i.e. θ has only *bounded* quantifiers (those of the form $\forall v_1 < v_2, \exists v_1 < v_2$). We may assume that the symbols + and · occur in θ as ternary relation symbols. (Notice that this may increase the length of $\bar{u}$.) By replacing $\exists\bar{u}$ with $\exists z\,\exists u_1<z\,\exists u_2<z\cdots\exists u_l<z$, we see that f is definable in $(\mathbb{N},+,\cdot,<)$ by a formula $\exists z\theta(x,y,z)$ where θ is Δ_0 and has $+$ and $\cdot$ as relation symbols. Notice that for all n, if $(n,+\restriction n,\cdot\restriction n,<\restriction n)\models\exists z\theta(i,j,z)$ then $f(i)=j$. Choose a similar formula $\exists z\psi(x,y,z)$ for g. It is convenient to assume further that $\mathbb{N}\models\forall x\forall y\forall z[\theta(x,y,z)\vee\psi(x,y,z)\rightarrow x<z\wedge y<z]\wedge\forall x\forall y_1\forall y_2\forall z\forall w[\theta(x,y_1,z)\wedge\psi(x,y_2,w)\rightarrow z=w]$. The idea is that z is the least number coding witnesses for both θ and ψ. To be precise, simply replace $\theta(x,y,z)$ by $x<z\wedge y<z\wedge(\exists v<z)(\exists y'<z)(\exists w<z)[\theta(x,y,v)\wedge\psi(x,y',w)]$, and then replace this new formula $\theta_0(x,y,z)$ by $\theta_0(x,y,z)\wedge(\forall u<z)\neg\theta_0(x,y,u)$; and change ψ similarly.

Next we define the function h. Given n, let $m=[n^{1/4}]$. First suppose that

(∗) $n=m^4+a+mb+m^2c$ for some $a,b,c<m$ such that $\mathbb{N}\models\theta(a,b,m)\wedge\psi(a,c,m)$;

then set $h(n)=a$. Notice that such a, b, and c are unique, so if (∗) holds then $h(n)$ is well-defined. Moreover, for all a we may choose m such that $\mathbb{N}\models\theta(a,f(a),m)\wedge\psi(a,g(a),m)$, by choice of θ and ψ; so $h(m^4+a+mf(a)+m^2g(a))=a$, hence h is onto. Notice that there are unique b, c, m such that $\theta(a,b,m)\wedge\psi(a,c,m)$, so thus far, h is one–one. It remains to define $h(n)$ if (∗) fails. In that case let $h(n)$ equal the greatest $a<m$ such that $\mathbb{N}\models(\exists y<n)(\exists z<m)(\exists w<m)[\theta(a,y,w)\wedge\psi(a,z,w)]$; if there is no such a (but this can happen for only finitely many n), set $h(n)=0$. It is clear that h is finite-to-one.

Now let Θ be the sentence given by Theorem 1, that is, Θ says $\langle\phi_+(x,y,z,\bar{P},R),\phi_\times(x,y,z,\bar{P},R)\rangle\cong\langle+,\times\rangle$, and $\lim_{n\to\infty}\mu_n(\exists\bar{P}\Theta)=1$. Consider the following property of a model (n,R):

(†) $(n,R)\models\exists\bar{P}\Theta$, $h(n)\neq0$, and $[\log_2(n)+1]<[\sqrt{n}]$.

We will show that it suffices that ϕ have the following property:

(∗) Whenever (†) holds for (n,R), then $(n,R)\models\phi$ iff for some $i<f(h(n))$, $|\{k: kRk\}|\equiv i \pmod{g(h(n))}$.

In order to define ϕ we use the following abbreviation. For $X\subseteq n$ we can write $\mathrm{succ}_X(i,j)$ if $i\in X$, $j\in X$, and $k\notin X$ whenever $i<k<j$. Then ϕ should say:

(i) $(\forall i\in X)(iRi)$;

(ii) $(\forall i)(\forall j)[\mathrm{succ}_X(i,j)\rightarrow|\{k: kRk \text{ and } i\leq k<j\}|=g(h(n))]$;

(iii) $|\{k: kRk \text{ and } \max(X)\leq k\}|<f(h(n))$.

Now let us describe ϕ. First, ϕ says that for some $\bar{P}$, $\Theta(\bar{P})$ holds. Now we want ϕ to assert (i), (ii), and (iii) above; then (∗) follows. Of course (i) presents no problem, and since the formulas θ and ψ from the definitions of f and g are Δ_0 (and by choice of h), $f(h(n))$ and $g(h(n))$ are definable in $(n,\bar{P},R)$. (More precisely, the $f(h(n))$th and $g(h(n))$th elements in the order defined by $\Theta(\bar{P})$ are definable.) So to express (ii) and (iii) we need only express the cardinalities there. Since $h(n)\neq0$, $f(h(n))<[n^{1/4}]$ and $g(h(n))<[n^{1/4}]$, so it suffices to define the relation "$x<[n^{1/4}]\wedge|X|=x$". This is similar to the proof of (8) in the proof of Theorem 1. First notice that we can quantify over binary relations S on $[\sqrt{n}]$, by coding S by $\{x+[\sqrt{n}]y: xSy\}$. Then for $x<[n^{1/4}]$, $|X|=x$ iff $|X|\geqslant x\wedge\neg(|X|\geqslant x+1)$; and for $x\leqslant[n^{1/4}]$, $|X|\geqslant x$ iff for some $S\subseteq x\times[\log_2(n)+1]$, we have $(\forall i<x)(\sum\{2^j: iSj\}\in X)\wedge(\forall i<j<x)(\exists k)(iSk\leftrightarrow\neg jSk)$. Since $[\log_2(n)+1]<[\sqrt{n}]$ if (†) holds, it follows that $(*)$ holds for ϕ.

The next task is to see that $\lim_{n\to\infty}\mu_n$("(†) holds") $=1$. But this is clear from the choice of Θ, together with the fact that h is finite-to-one and $\lim_{n\to\infty}[\log_2(n)+1]/[\sqrt{n}]=0$.

Finally, let μ^i be the probability that $|\{k: kRk\}|\equiv i \pmod m$, where $m=g(h(n))$. We claim:

$$\lim_{n\to\infty}\left(\left(\sum_{k<f(h(n))}\mu^k\right)-\mu_n(\phi)\right)=0.$$

But this is clear from $(*)$, together with the fact that $\lim_{n\to\infty}$("(†) holds")$=1$. Hence the lemma follows from

$$\lim_{n\to\infty}\left(\left(\sum_{k<f(h(n))}\mu^k\right)-\frac{f(h(n))}{g(h(n))}\right)=0.$$

But this in turn follows from

$$(**)\ \text{for } 0\leqslant k<l<m,\qquad |\mu^k-\mu^l|<5\binom{n}{\left[\frac{n}{2}\right]}/2^n.$$

For if $(**)$ holds, then by Stirling's formula there is a constant C (not depending on n) such that $|\mu^k-\mu^l|\leqslant C/\sqrt{n}$ when $0\leqslant k<l<m$, and hence $|\mu^k-1/m|\leqslant C/\sqrt{n}$ for $0\leqslant k<m$. Then it follows that

$$\left|\left(\sum_{k<f(h(n))}\mu^k\right)-\frac{f(h(n))}{g(h(n))}\right|\leqslant\frac{C}{\sqrt{n}}f(h(n))<\frac{C}{\sqrt{n}}n^{1/4},$$

which has limit 0, as claimed.

To prove $(**)$ first notice that for $0\leqslant k<l<m$, $\mu^k=\sum_i\binom{n}{im+k}/2^n$ and $\mu^l=\sum_i\binom{n}{im+l}/2^n$. Now if $a_i=\binom{n}{im+k}/2^n$ and $b_i=\binom{n}{im+l}/2^n$, then we see that $a_0<b_0<a_1<b_1<\cdots<a_p<b_p$, where p is greatest such that $(p+1)m\leqslant[\frac{1}{2}n]$, and also $a_{p+2}>b_{p+2}>a_{p+3}>b_{p+3}>\cdots>a_q>b_q$, where q is greatest such that $qm+l\leqslant n$. Notice that

$$0<\sum_{i=0}^{p}b_i-\sum_{i=0}^{p}a_i\leqslant\sum_{i=0}^{p-1}a_{i+1}+b_p-\sum_{i=0}^{p}a_i=b_p-a_0<b_p,$$

and similarly

$$0<\sum_{i=p+2}^{q}a_i-\sum_{i=p+2}^{q}b_i<a_{p+2}.$$

Sh:201

So we have

$$|\mu^k - \mu^l| < b_p + a_{p+2} + a_{p+1} + b_{p+1} + a_{q+1} \leq 5\binom{n}{\left[\frac{n}{2}\right]}/2^n,$$

since $\binom{n}{[n/2]} \geq \binom{n}{k}$ for all k. □

We close by remarking that by Theorem 1, one has second-order logic on $[\sqrt{n}]$, in the following sense. Suppose Ψ is a second-order sentence, i.e. we allow monadic and binary quantification in Ψ, but Ψ has no non-logical symbols (except equality). Then there is a monadic second-order sentence Φ (with one non-logical symbol R, R a binary relation symbol) such that $\mu[(n, R) \models \Phi \text{ iff } [\sqrt{n}] \models \Psi] = 1$. This is clear by a trick we have already used: binary relations on $[\sqrt{n}]$ can be coded by subsets of n via the map $\langle i, j\rangle \mapsto i + [\sqrt{n}]j$.

Acknowledgments

The first author thanks Jim Schmerl and Kevin Compton for interesting discussions on the subject. The authors also thank Central States Universities, Inc. for supporting the conference [6] in which Compton's question was brought to our attention.

References

[1] K. Compton, A logical approach to asymptotic combinatorics I, Advances in Math., to appear.
[2] R. Fagin, Probabilities on finite models, J. Symbolic Logic 41 (1976) 50–58.
[3] H. Gaifman, Concerning measures in first-order calculi, Israel J. Math. 2 (1964) 1–18.
[4] 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 5 (1969) 142–154 (translated 1972).
[5] J.F. Lynch, Almost sure theories, Ann. Math. Logic 18 (1980) 91–135.
[6] Conference, Decision Problems in Math. and Comp. Sci., Central States Universities, Inc. (1982).