NONCONVERGENCE, UNDECIDABILITY, AND INTRACTABILITY IN ASYMPTOTIC PROBLEMS

Kevin J. COMPTON*
EECS Department, University of Michigan, Ann Arbor, MI 48109, USA

C. Ward HENSON†
Mathematics Department, University of Illinois, Urbana, IL 61801, USA

Saharon SHELAH‡
EECS Department and Mathematics Department, University of Michigan, Ann. Arbor, MI 48109, USA (Current address: Mathematics Dept., Hebrew Univ., Jerusalem, Israel)

Communicated by Y. Gurevich
Received July 1986

Results delimiting the logical and effective content of asymptotic combinatorics are presented. For the class of binary relations with an underlying linear order, and the class of binary functions, there are properties, given by first-order sentences, without asymptotic probabilities; every first-order asymptotic problem (i.e., set of first-order sentences with asymptotic probabilities bounded by a given rational number between zero and one) for these two classes is undecidable. For the class of pairs of unary functions or permutations, there are monadic second-order properties without asymptotic probabilities; every monadic second-order asymptotic problem for this class is undecidable. No first-order asymptotic problem for the class of unary functions is elementary recursive.

0. Introduction

The classification of decidable and undecidable theories is one of the great achievements of modern logic (see Ershov et. al. [8] and Rabin [20]). This enterprise and subsequent work on the computational complexity of theories (see Ferrante and Rackoff [10]) revealed the effective content of the axiomatic approach in mathematics — an approach which characterizes much of algebra and geometry. More recently, researchers have begun to scrutinize the logical and effective content of other areas of mathematics. This investigation carries forward that work in the area of asymptotic combinatorics.

Asymptotic combinatorics studies the probabilities of properties holding in random finite structures. The probabilities considered are the limit values as the size of the structures increases (hence the term *asymptotic*). Let C be a class

* Research partially supported by NSF grant DCR 84-18524.
† Research partially supported by NSF grant DMS 83-02550.
‡ Research partially supported by NSF grant MCS 81-01560.

(closed under isomorphism) of finite structures for a finite language and C_n the set of structures in C with universe $n = \{0, 1, \ldots, n-1\}$ (in combinatorics these are called the *labeled* structures in C). Let φ be a sentence (of some logic) in a language for this class. Define $\mu_n^C(\varphi) = \mu_n(\varphi)$ to be the fraction of structures in C_n that satisfy φ. We seek to determine when $\mu_n(\varphi)$ will converge as n increases to ∞ (call the limit $\mu(\varphi)$ when it exists), when $\mu(\varphi)$ is computable, and how difficult it is to compute. Our results establish how complicated C must be for nonconvergence, undecidability, and intractability to occur.

Our first main theorem answers a question of Lynch [17].

Theorem 1. *Let C_n be the class of structures $\langle n, \leqslant, R\rangle$, where $\leqslant$ is the usual order and R is an arbitrary binary relation on n. Then there is a first-order φ in the language for this class such that $\mu_n(\varphi)$ does not converge.*

We prove this theorem in Section 1.

Glebskii, Kogan, Liogonkii, and Talanov [11] and, independently, Fagin [9 showed that if C is the set of all structures for a relational language, then $\mu_n(\varphi$ converges for all first-order φ; in fact, $\mu(\varphi)$ is either 0 or 1. Lynch [17] obtains a a consequence of a more general theorem that if one binary relation is specifie as the usual successor relation on n, then $\mu_n(\varphi)$ still converges for first-order φ Theorem 1 establishes that Lynch's result cannot be strengthened to linear orde rather than successor relation. Ehrenfeucht has shown that $\mu_n(\varphi)$ does converg for all first-order φ in the case of a linear order and arbitrary unary relations (se Lynch [17]) so our result is the best possible.

Kaufmann and Shelah [14] showed that if C is the set of all structures for relational language with at least one nonunary relation symbol, then there is monadic second-order φ such that $\mu_n(\varphi)$ does not converge. However, Blas Gurevich, and Kozen [2] showed that $\mu_n(\varphi)$ converges to either 0 or 1 in this cas for all φ in least fixed-point logic.

Our second main theorem answers another question of Lynch [18].

Theorem 2. *Let C_n be the class of structures $\langle n, F\rangle$, where F is a binary functio on n. Then there is a first-order φ in the language for this class such that $\mu_n($ does not converge.*

We prove this theorem in Section 2. It is closely related to our third ma theorem.

Theorem 3. *Let C_n be the set of structures $\langle n, F, G\rangle$, where F and G each ran over either unary functions or permutations on n. Then there is a monac second-order sentence φ in the language for this class such that $\mu_n(\varphi)$ does n converge.*

We prove this theorem in Section 3.

Lynch [18] proved that if C_n is the class of structures $\langle n, F_1, \ldots, F_p\rangle$, where each F_i ranges over either unary functions or permutations on n, then $\mu_n(\varphi)$ converges for all first-order φ. A theorem in Compton [4] implies that $\mu_n(\varphi)$ converges for all monadic second-order φ when C_n is the set of structures $\langle n, F\rangle$ with F a permutation on n. The theorem does not apply when F is an arbitrary unary function, but in a later paper Compton [3] showed that the Cesàro probability

$$\frac{1}{n}\sum_{k<n} \mu_k(\varphi)$$

does converge for all monadic second-order φ. In a forthcoming paper Compton and Shelah [7] show that $\mu_n(\varphi)$ converges for all monadic second-order φ in this case.

Theorems 1, 2, and 3, together with the papers cited, give a fairly complete picture for convergence in relational or functional classes. What about undecidability and intractability?

Define an *asymptotic problem* for a class C of structures to be a set of sentences defined by one of the following forms

$$\{\varphi : \mu(\varphi) \geqslant r\} \text{ or } \{\varphi : \mu(\varphi) < r\}, \quad 0 < r \leqslant 1,$$
$$\{\varphi : \mu(\varphi) > r\} \text{ or } \{\varphi : \mu(\varphi) \leqslant r\}, \quad 0 \leqslant r < 1.$$

The sentences φ are from some specified logic and r is a rational number. Rationality of r is not crucial: we could require instead that r be algebraic or a recursive real. Nor is the use of $\mu(\varphi) = \lim_{n\to\infty} \mu_n(\varphi)$ crucial: we could use $\liminf \mu_n(\varphi)$, $\limsup \mu_n(\varphi)$, Cesàro limit, or any other reasonable method for assigning probabilities to sentences. Our next main theorem is insensitive to any of these variations in the definition.

Theorem 4. *Suppose C is either the set of structures $\langle n, \leqslant, R\rangle$, where $\leqslant$ is the usual order and R a binary relation on n, or $\langle n, F\rangle$ where F is a binary function on n. Then every first-order asymptotic problem for C is undecidable.*

Suppose C is the class of structures $\langle n, F, G\rangle$, where F and G each range over unary functions or permutations on n. Then every monadic second-order asymptotic problem for C is undecidable.

We prove this result in Section 4. In fact we prove a stronger result. For each of the classes mentioned in Theorem 4, the set of sentences (either first-order or monadic second-order, as indicated in the statement of the theorem) such that $\mu(\varphi) = 1$ and the set of sentences such that $\mu(\varphi) = 0$ are recursively inseparable. That is, there is no recursive set containing one of these sets and disjoint from the other.

Fagin [9] noted that the set of first-order sentences φ with $\mu(\varphi)=1$ is a complete, decidable theory when C is the class of all structures for a relational language. Grandjean [13] proved that this set and, hence, its complement within the set of first-order sentences are PSPACE-complete. These are the only two asymptotic problems for this class. This result shows that determination of truth in almost all relational structures has fairly low complexity. Compare with the well-known undecidability for determination of truth in all finite structures when the language contains a nonunary relation symbol (see Trachtenbrot [24] and Vaught [25]). Blass, Gurevich, and Kozen [2] show that the set of sentences φ in least fixed-point logic such that $\mu(\varphi)=1$ is EXPTIME-complete when C is the class of all structures for some relational language.

Lynch [18] showed that when C is the class of structures $\langle n, F_1, \ldots, F_p\rangle$, where each F_i ranges over either unary functions or permutations on n, then an expression for $\mu(\varphi)$ in terms of 0, 1, e, and the usual arithmetic operations (including exponentiation) is computable for first-order φ. It does not follow that each first-order asymptotic problem for this class is decidable; showing this seems to involve difficult questions about rationality of exponential expressions. However, a close reading of Lynch's proof discloses that the asymptotic problems

$$\{\varphi \text{ first-order: } \mu(\varphi)=1\}, \quad \{\varphi \text{ first-order: } \mu(\varphi)=0\}$$

are decidable. Our last main result shows that these problems are highly intractable if some F_i ranges over unary functions. Thus, there is no significant reduction of complexity in going from all finite unary functions to almost all finite unary functions (the theory of all finite unary functions is decidable but not elementary recursive — see Compton and Henson [16] for a proof of nonelementary recursiveness).

Theorem 5. *Let C be the class of structures $\langle n, F\rangle$, where F is a unary function on n. Then no asymptotic problem for C is elementary recursive.*

We prove this theorem in Section 5. As with Theorem 4, it will follow from a stronger result. For C, the class of unary functions, there is no elementary recursive set separating the set of first-order sentences φ such that $\mu(\varphi)=1$ from the set of first-order sentences φ such that $\mu(\varphi)=0$. Recall that the elementary recursive sets are those recognized by a Turing machine in time bounded by an iterated exponential (see Section 5 for a more formal definition).

We will often say in our arguments that a property holds *almost surely* in a class C. By this we mean that the proportion of structures in C_n having the property approaches 1 as n increases to ∞. The natural logarithm of n is denoted $\ln n$ and logarithm base 2 is denoted $\lg n$. If X is a random variable, $E(X)$ denotes its expected value, $\sigma(X)$ its standard deviation, and $\{X \geqslant r\}$ the set $\{x : X(x) \geqslant r\}$ ($\{X<r\}$ is defined similarly). We denote the falling factorial $n(n-1)\cdots(n-i+1)$ by $(n)_i$.

1. Proof of Theorem 1

We produce a first-order sentence φ such that $\mu_n(\varphi)$ does not converge for the class C of structures $\langle n, \leqslant, R\rangle$.

First specify a formula $\psi(x, y, z)$ that says that in $\langle n, \leqslant, R\rangle$, R restricted to the interval $[y, z)$ *codes arithmetic* on the interval $I_0 = [0, x)$. More specifically, ψ says that $0 < x < y < z$ and $[y, z)$ can be partitioned into intervals $I_1 = [y, w)$ and $I_2 = [w, z)$ such that the following hold.

(a) $R \cap (I_1 \times I_0)$ is an order preserving bijection (call it f in this discussion) from I_1 to I_0.

(b) $R \cap (I_2 \times I_0)$ is a function π_0 and $R \cap (I_2 \times I_1)$ is a function π_1 such that $(\pi_0(t), f(\pi_1(t)))$ enumerates $I_0 \times I_0$ in lexicographic order as t ranges over I_2. To say this with a first-order formula is straightforward. We say that $t \in I_2$ *codes* the pair $(\pi_0(t), f(\pi_1(t))) \in I_0 \times I_0$.

(c) $R \cap (I_0 \times I_2)$ is the inverse of a partial function *add* from I_2 to I_0. If $t \in I_2$ codes $(u, 0) \in I_0 \times I_0$, then $add(t) = u$; if $t \in I_2$ codes $(u, v) \in I_0 \times I_0$ and $add(t) < x - 1$, then $add(t+1) = add(t) + 1$ (by (b) $t + 1$ codes $(u, v+1)$); otherwise $add(t)$ is undefined. Thus, when $t \in I_2$ codes $(u, v) \in I_0 \times I_0$ and $u + v < x$, $add(t) = u + v$.

(d) $R \cap (I_1 \times I_2)$ is the inverse of a partial function *mul* from I_2 to I_1. Use an inductive definition similar to the one in (c) to say that if $t \in I_2$ codes $(u, v) \in I_0 \times I_0$ and $u \cdot v < x$, then $f(mul(t)) = u \cdot v$.

Note that whenever $\psi(k, l, m)$ holds with $k, l, m \in n$, $|I_0| = |I_1| = k$ and $|I_2| = k^2$. Hence, $m = l + k + k^2$. Also, $\psi(k, l, m)$ specifies membership or lack of membership in R for $4k^3 + k^2$ pairs, so

$$\mu_n(\psi(k, l, l + k + k^2)) = 2^{-4k^3 - k^2}$$

when $k \leqslant l < n - k - k^2$. Given n, choose $k = k(n)$ such that

$$2^{4k^3+k^2} < n/\ln n < n \ln n \leqslant 2^{4(k+1)^3+(k+1)^2}.$$

For this definition to make sense we must assume that there is no value of the form $2^{4k^3+k^2}$ between $n/\ln n$ and $n \ln n$. This assumption is true for infinitely many n and we restrict our attention to such n.

Let $p = k + k^2$. For $0 \leqslant i < (n-k)/p$, the probabilities

$$\mu_n(\neg\psi(k, k + ip, k + (i+1)p)) = 1 - 2^{-4k^3-k^2}$$

are independent so

$$\begin{aligned}\mu_n(\forall y, z \neg\psi(k, y, z)) &\leqslant (1 - 2^{-4k^3-k^2})^{(n-k)/p} \\ &\leqslant \exp(-2^{-4k^3-k^2}(n-k)/p)\end{aligned}$$

But $2^{-4k^3-k^2} > \ln n/n$ so this approaches 0 as n increases. Thus, $\mu_n(\exists y, z\, \psi(k, y, z))$ converges to 1.

Suppose that $m \geqslant k+1$. Then

$$\mu_n(\exists y, z\ \psi(m, y, z)) \leqslant n 2^{-4m^3-m^2}$$

since there are fewer than n intervals that can code arithmetic on $[0, m)$. Thus,

$$\begin{aligned}\mu_n(\exists x > k\ \exists y, z\ \psi(x, y, z)) &\leqslant n \sum_{m>k} 2^{-4m^3-m^2}\\ &\leqslant n\, 2^{-4(k+1)^3-(k+1)^2} \sum_{i \geqslant 0} 2^{-i}\\ &\leqslant 2/\ln n.\end{aligned}$$

We have established that $k(n)$ is almost surely the largest x such that some interval $[y, z)$ codes arithmetic on $[0, x)$ (when $k(n)$ is defined). Note that as n increases $k(n)$ assumes all large values. Let φ be a sentence that asserts the largest x such that some interval $[y, z)$ codes arithmetic on $[0, x)$ is even. When k is even $\mu_n(\varphi)$ approaches 1; when k is odd, $\mu_n(\varphi)$ approaches 0. □

2. Proof of Theorem 2

We first prove a lemma.

Lemma 2.1. *Let C_n be the set of structures $\langle n, f\rangle$ where f is a unary function on n. Define random variables $X_{jn} = |\{x \in n : |f^{-1}(x)| = j\}|$ on (C_n, μ_n). If $m = m(n) =$* $\mathrm{o}(\ln n/\ln\ln n)$, *then*

$$\begin{aligned}M_{jn} &= E(X_{jn}) = n/(\mathrm{e}j!) + \mathrm{O}(1),\\ D_{jn} &= \sigma(X_{jn}) \leqslant (n(1/(\mathrm{e}j!))(1-(1/(\mathrm{e}j!)))^{\frac{1}{2}} + \mathrm{o}(1/n)\end{aligned}$$

uniformly for $j \leqslant m$, and

$$\lim_{n\to\infty} \mu_n\Bigl(\bigcap_{j \leqslant m} \{X_{jn} \geqslant M_{jn} - D_{jn} \ln n\}\Bigr) = 1.$$

Proof. Our proof follows Kolchin, Sevast'yanov, and Chistyakov [15] but requires a more careful analysis since theirs is for m constant. By II.1(3) and II.1(5) of [15]

$$E(X_{jn}) = \frac{(n)_j}{j!}\frac{(n-1)^{n-j}}{n^n} n,$$

$$E(X_{jn}^2) = E(X_{jn}) + \frac{(n)_{2j}}{j!^2}\frac{(n-2)^{n-2j}}{n^n} n(n-1).$$

Write $(n)_{ij} = n^{ij}1(1-1/n)(1-2/n)\cdots(1-(ij-1)/n)$ and $(n-i)^{n-ij} = n^{n-ij}(1-i/n)^{n-ij}$. Use the estimate

$$1-\frac{r}{n} = \exp\left(\ln\left(1-\frac{r}{n}\right)\right) = \exp\left(-\frac{r}{n}-\frac{r^2}{2n^2}+O\left(\frac{r^3}{n^3}\right)\right)$$

to show

$$\begin{aligned} E(X_{jn}) &= n\exp(-1-(j^2-3j+1)/(2n)+O(j^3/n^2))/j!,\\ E(X_{jn})^2 &= n^2\exp(-2-(j^2-3j+1)/n+O(j^3/n^2))/j!^2,\\ E(X_{jn}^2) &= E(X_{jn})+n(n-1)\exp(-2-(2j^2-5j+2)/n+O(j^3/n^2))/j!^2. \end{aligned}$$

Thus,

$$E(X_{jn}) = (n/(ej!))(1-(j^2-3j+1)/(2n)+O(j^4/n^2))$$

which establishes the first part of the lemma. Also,

$$\begin{aligned} E(X_{jn})^2 &= (n/(ej!))^2(1-(j^2-3j+1)/n+O(j^4/n^2)),\\ E(X_{jn}^2) &= E(X_{jn})+(n(n-1)/(ej!)^2)(1-(2j^2-5j+2)/n+O(j^4/n^2)). \end{aligned}$$

Therefore,

$$\begin{aligned} \sigma(X_{jn}) &= (E(X_{jn}^2)-E(X_{jn})^2)^{\frac{1}{2}}\\ &= ((n/(ej!))(1-(j^2-2j+2)/(ej!)+O(j^4/n))^{\frac{1}{2}} \end{aligned}$$

Uniformly for $j \leqslant m$. This establishes the second part of the lemma.

Equations II.2(13)–(14) of [15] show that

$$\mu_n(X_{jn}=k) = \binom{n}{k}\frac{n!}{2\pi i(j!)^k n^n}\int\frac{(e^z-z^j/j!)^{n-k}}{z^{n-kj}}\frac{dz}{z}$$

where the integral is taken around a circle with center at the origin. Fortunately, we do not need to find an asymptotic expression for the integral to complete the theorem; a crude estimate will do. Observe that the Taylor expansion of $e^z - z^j/j!$ has only non-negative coefficients so for $|z| = 1$, $|e^z - z^j/j!| \leqslant e - 1/j!$. Using this bound for the integrand, we have

$$\mu_n(X_{jn}=k) \leqslant \frac{n!\,e^n}{n^n}\binom{n}{k}\left(\frac{1}{ej!}\right)^k\left(1-\frac{1}{ej!}\right)^{n-k}$$

and consequently

$$\mu_n(X_{jn} < M_{jn} - D_{jn}\ln n) \leqslant 3n^{\frac{1}{2}}\sum_{k<M-D\ln n}\binom{n}{k}\left(\frac{1}{ej!}\right)^k\left(1-\frac{1}{ej!}\right)^{n-k}$$

where $M = n/(ej!)$, $D^2 = n(1/(ej!))(1-1/(ej!))$. The problem thereby reduces to an estimate for a Bernoulli trial distribution. We use Bernstein's inequality (see

Renyi [21, p. 387]). If $p = 1/(\mathrm{e}j!)$, $q = 1-p$, then

$$\sum_{k \leqslant M-\varepsilon D} \binom{n}{k} p^k q^{n-k} \leqslant \exp\left(-\frac{\varepsilon^2}{2(1+\varepsilon/(2D))^2}\right)$$

for $\varepsilon > 0$. Now for large n and $j \leqslant m = \mathrm{o}(\ln n/\ln\ln n)$, $\mathrm{e}j! \leqslant n^{\frac{1}{2}}$ so $D \geqslant n^{\frac{1}{2}}/2$. Put $\varepsilon = \ln n$ to obtain

$$\mu_n(X_{jn} < M_{jn} - D_{jn}\ln n) \leqslant 3n^{\frac{1}{2}} \exp\left(-\frac{n(\ln n)^2}{2(n^{\frac{1}{2}} + \ln n)^2}\right).$$

We have, taking the union over $j < m$, that

$$\lim_{n\to\infty} \mu_n\left(\bigcup_{j<m} \{X_{jn} < M_{jn} - D_{jn}\ln n\}\right) = 0$$

This establishes the third part of the lemma. □

We proceed with the proof of Theorem 2. Consider a structure $\langle n, F\rangle$ where F is a binary function on n. Let $f(x) = F(x, x)$ and $X_{jn} = |\{x \in n : |f^{-1}(x)| = j\}|$. By the lemma, $X_{jn} \geqslant M_{jn} - D_{jn}\ln n$ almost surely for all $j \leqslant m = \mathrm{o}(\ln n/\ln\ln n)$. Define $A = \{x \in n : |f^{-1}(x)| = 0\}$ and the binary relation $R = \{(x, y) : F(x, y) \in A\}$. By definition R is irreflexive, but for pairs (x, y) with $x \neq y$, the probabilities that $(x, y) \in R$ are independent and equal to $\lambda = |A|/n$. By the lemma and Chebyshev's inequality $|\lambda - 1/\mathrm{e}| \leqslant \ln n/n^{\frac{1}{2}}$ almost surely. We may regard R as a random directed graph on n such that the edge probability for each pair of points is between

$$\lambda_0 = 1/\mathrm{e} - \ln n/n^{\frac{1}{2}} \quad\text{and}\quad \lambda_1 = 1/\mathrm{e} + \ln n/n^{\frac{1}{2}}.$$

Let $S_x = f^{-1}(x)$. The sets S_x, $x \in n$, partition n and the number of partition classes S with $|S| = j \leqslant m$ is almost surely greater than $M_{jn} - D_{jn}\ln n$. Furthermore, the partition $\{S_x : x \in n\}$ and binary relation R are independent.

Say that a partition class S *codes arithmetic* on $I_0 \in S$ if the following hold.

(a) There is a unique $p \in S$ such that p has no directed edges to any element of S. Let I be the set of elements in S with a directed edge to p, I_1 the subset of I consisting of elements with no directed edge from any element in I, $I_0 = I - I_1$, $I_2 = S - I - \{p\}$.

(b) $R \restriction I_0$ is an irreflexive linear order $<$ (from this define a reflexive linear order $\leqslant$).

(c) I_0, I_1, and I_2 satisfy conditions (a)–(d) in the proof of Theorem 1 except that the function given by $R \cap (I_1 \times I_0)$ is not required to be order preserving (this would not make sense because I_1 has no order specified on it) and functions π_0, π_1 are not required to order pairs in $I_0 \times I_0$ lexicographically (for the same reason: I_2 has no order specified on it). However, we still require that $(\pi_0(t), f(\pi_1(t)))$ enumerates each pair in $I_0 \times I_0$ precisely once as t ranges over I_2. We must define *add* and *mul* without reference to an order on I_2, but this poses no problem.

(d) If $j \in I_2$ and *add*(j) is not defined, then there is an edge from j to the element of I_2 that codes $(0, 0)$; if *mul*(j) is not defined, then there is an edge from j to the element of I_2 coding $(0, 1)$. This condition simplifies enumeration of edges in S.

(e) There are no edges in S other than those specified above.

A careful enumeration shows that if $|I_0| = k$, then $|S| = m = m(k) = (k+1)^2$ and the number of directed edges in S is $i = i(k) = (9k^2 + 5k)/2$. Moreover, any S satisfying (a)–(e) has no automorphisms so the probability that a particular S of cardinality m satisfies (a)–(e) is $M!\,\lambda^i(1-\lambda)^{l-i}$, where $l = l(k) = m^2 - m$.

Given n, choose $k = k(n)$ such that

$$\begin{aligned} e^{i(k)}(e/(e-1))^{l(k)-i(k)} &\leqslant n/\ln n < n \ln n \\ &\leqslant e^{i(k+1)}(e/(e-1))^{l(k+1)-i(k+1)}. \end{aligned}$$

As in the proof of Theorem 1, $k(n)$ may be undefined for some values of n, but it is defined for infinitely many n, and k assumes all large values as n increases. Notice that $k(n) = O((\ln n)^{\frac{1}{4}})$, from which it follows that

$$\lambda^{-i(k)}(1-\lambda)^{-l(k)+i(k)} \sim e^{i(k)}(e/e-1)^{l(k)-i(k)}$$

for $\lambda_0 \leqslant \lambda \leqslant \lambda_1$. Thus, by further restricting the values of n for which $k(n)$ is defined, we may assume

$$\begin{aligned} \lambda_1^{-i(k)}(1-\lambda_1)^{-l(k)+i(k)} &\leqslant n/\ln n < n \ln n \\ &< \lambda_0^{-i(k+1)}(1-\lambda_0)^{-l(k+1)+i(k+1)}. \end{aligned}$$

Again, $k(n)$ will assume all large values as n increases.

The probability that no partition class S of cardinality $m = m(k)$ codes arithmetic on an interval of size k is bounded above by

$$(1 - m!\,\lambda_1^i(1-\lambda_1)^{l-i})^{M_{mn} - D_{mn} \ln n}$$

since there are almost surely at least $M_{mn} - D_{mn} \ln n$ partition classes of cardinality m. But $M_{mn} - D_{mn} \ln n \sim n/(em!)$ and $\lambda_1^i(1-\lambda_1)^{l-i} > \ln n/n$ so the expression above approaches 0 as n increases. We have shown that there is almost surely a partition class that codes arithmetic on an interval of length k.

We now show that there is almost surely not a partition class that codes arithmetic on an interval of length greater than k. If there were such a partition class it would have size at least $n = m(k+1)$. Let us estimate

$$|\{x \in n : |S_x| \geqslant m(k+1)\}| = n - |\{x \in n : |S_x| < m(k+1)\}|,$$

Since $m(k+1) = O((\ln n)^{\frac{1}{2}})$, we know by Lemma 2.1 that

$$\lim_{n \to \infty} \mu_n\Big(\bigcap_{j < m(k+1)} \{X_{jn} \geqslant M_{jn} - D_{jn} \ln n\}\Big) = 1$$

so almost surely

$$
\begin{aligned}
|\{x \in n : |S_x| < m(k+1)\}| &= \sum_{j<m(k+1)} X_{jn} \\
&\geqslant \sum_{j<m(k+1)} (M_{jn} - D_{jn} \ln n) \\
&= (n/\mathrm{e}) \sum_{j<m(k+1)} 1/j! + \mathrm{O}((n \ln n)^{\frac{1}{2}}).
\end{aligned}
$$

Subtract this from $n = (n/\mathrm{e}) \sum_{j\geqslant 0} 1/j!$ to obtain

$$|\{x \in n : |S_x| \geqslant m(k+1)\}| \leqslant (n/\mathrm{e}) \sum_{j\geqslant m(k+1)} 1/j! + \mathrm{O}((n \ln n)^{\frac{1}{2}}).$$

The sum in this expression is bounded above by $2/m(k+1)!$. The probability that a particular partition class S_x of cardinality at least $m(k+1)$ codes arithmetic on an interval is at most

$$m(k+1)!\, \lambda_0^{i(k+1)}(1-\lambda_0)^{l(k+1)-i(k+1)}.$$

We chose k in a way that insures this quantity is at most $m(k+1)!/(n \ln n)$. Therefore, the probability that there is a partition class S_x that codes arithmetic with $|S_x| \geqslant m(k+1)$ is at most

$$2/(\mathrm{e} \ln n) + \mathrm{O}(m(k+1)!/(n \ln n)^{\frac{1}{2}}).$$

This probability approaches 0 as n increases. We conclude that there is almost surely not a partition class that codes arithmetic on an interval of cardinality greater than k.

Now if we can almost surely compare sizes of intervals with arithmetic coded on them with a first-order formula, we can specify a first-order sentence φ that says the largest interval with arithmetic coded on it will have even length. When k is even $\mu_n(\varphi)$ approaches 1; when k is odd $\mu_n(\varphi)$ approaches 0.

Let S and S' be partition classes coding arithmetic on I_0 and I_0' respectively. A partition class T *compares* S and S' if $|T| = \min(|I_0|, |I_0'|)$, and $R \cap (T \times I_0)$ and $R \cap (T \times I_0')$ are one-to-one functions from T onto initial segments of I_0 and I_0'. Let $r = \min(|I_0|, |I_0'|)$. We may assume that $|I_0|, |I_0'| \leqslant k$ so the probability that a particular T of cardinality r compares S and S' is

$$
\begin{aligned}
r!^2 \lambda^{2r}(1-\lambda)^{(|I_0|+|I_0'|-2)r} &\geqslant r!^2 \lambda^{2k}(1-\lambda)^{2k^2-2k} \\
&\geqslant r!^2 \lambda_1^{2k}(1-\lambda_1)^{2k^2-2k}.
\end{aligned}
$$

Note that $2k < i(k)/2$ and $2k^2 - 2k < (l(k) - i(k))/2$ for large n, so the probability that T compares S and S' is more than

$$r!^2 \lambda^{i(k)/2}(1-\lambda_1)^{(l(k)-i(k))/2} \geqslant r!^2 (\ln n/n)^{\frac{1}{2}}$$

according to our choice of k. But almost surely there are at least $M_{rn} - D_{rn} \ln n = n/(\mathrm{e}r!) + \mathrm{O}(1)$ partition classes T with $|T| = r$. The probability that none of them compare S and S' is less than

$$(1 - r!^2(\ln n/n)^{\frac{1}{2}})^{n/(er!)+O(1)} \leqslant \exp(-(n \ln n)^{\frac{1}{2}}).$$

There are certainly fewer than n partition classes that code arithmetic so the number of comparisons needed between these classes is less than $\binom{n}{2}$. But $\lim_{n\to\infty} \binom{n}{2}\exp(-(n \ln n)^{\frac{1}{2}}) = 0$ so almost surely every pair of partition classes coding arithmetic is comparable. □

3. Proof of Theorem 3

We first present three lemmas.

Lemma 3.1. *Let $i, j < n$, $i + j \leqslant n$. Suppose that $X, Y \subseteq n$, $|X| = i$, $|Y| = j$, X and Y are chosen randomly, and p is the probability that $X \cap Y = \emptyset$. Then*

$$\exp\left(-\frac{ij}{n-i-j+1}\right) \leqslant p \leqslant \exp\left(-\frac{ij}{n}\right).$$

Proof. Suppose $X \subseteq n$ has been chosen. There are $\binom{n}{j}$ subsets $Y \subseteq n$. Of this number $\binom{n-i}{j}$ are subsets of $n - X$. Thus, the probability that X and Y are disjoint is

$$\binom{n-i}{j} \Big/ \binom{n}{j} = (n-i)_j/(n)_j = \prod_{0 \leqslant k < j} \frac{n-i-k}{n-k} = \prod_{0 \leqslant k < j} \left(1 - \frac{i}{n-k}\right).$$

Use the inequalities $\exp(-t/(1-t)) \leqslant 1 - t \leqslant \exp(-t)$ to show

$$\exp\left(-\sum_{0 \leqslant k < j} \frac{i}{n-i-k}\right) \leqslant p \leqslant \exp\left(-\sum_{0 \leqslant k < j} \frac{i}{n-k}\right).$$

Bound the leftmost expression from below by replacing every term in the sum with the last term. Bound the rightmost expression from above by replacing every term in the sum by the first term. The resulting inequality is the desired conclusion. □

Lemma 3.2 (Goncharov [12]). *Let C_n be the set of structures $\langle n, F \rangle$, where F is a permutation on n. Define random variables X_{jn} on (C_n, μ_n) equal to the number of F-cycles of size at most j. Then*

$$E(X_{jn}) \sim \ln j, \qquad \sigma(X_{jn}) \sim (\ln j)^{\frac{1}{2}}$$

uniformly for $j \leqslant n$. Hence, if $j = n^r$, $0 \leqslant r \leqslant 1$, then

$$E(X_{jn}) \sim r \ln n \quad \text{and} \quad \sigma(X_{jn}) \sim (r \ln n)^{\frac{1}{2}}.$$

The proof of this lemma may be found in Gonchorov [12] or Shepp and Lloyd

[23]. We will need a similar lemma for unary functions. If F is a unary function on n, we say $x, y \in n$ are in the same *F-component* if there exist k and l such that $F^k(x) = F^l(y)$.

Lemma 3.3. *Let C_n be the set of structures $\langle n, F\rangle$, where F is a unary function on n. Define random variables X_{jn} on (C_n, μ_n) equal to the number of F-components of size at most $j \leqslant n$. Then*

$$E(X_{jn}) \sim (\ln j)/2, \qquad \sigma(X_{jn}) \sim (\ln j)^{\frac{1}{2}}/2$$

uniformly for $j \leqslant n$. Hence, if $j = n^r$, $0 \leqslant r \leqslant 1$, then

$$E(X_{jn}) \sim (r \ln n)/2, \quad \sigma(X_{jn}) \sim (r \ln n)^{\frac{1}{2}}/2.$$

Kruskal [16] was the first to determine $E(X_{nn})$, the expected number of components. Lemma 3.3 is not proved explicitly in the literature, but it is not difficult to obtain expressions for $E(X_{jn})$ and $\sigma(X_{hn})$ by the kind of argument Riordan [22] uses to obtain an expression for $E(X_{nn})$, then approximate the sums occurring in these expressions.

We proceed with the proof of Theorem 3. Let C_n be the set of structures $\langle n, F, G\rangle$ where F and G are both permutations on n. Our proof is easily modified for the cases where one or both of F and G are unary functions; the changes involve reference to components rather than cycles, use of Lemma 3.3 rather than Lemma 3.2, and slight modifications in the construction that follows.

Fix $\langle n, F, G\rangle$. Define $X \subseteq n$ to be a *matching* if every pair of distinct elements $x, y \in X$ belong to distinct F-cycles and distinct G-cycles. We associate with $\langle n, F, G\rangle$ a bipartite graph Γ that has as vertices the F-cycles and G-cycles of $\langle n, F, G\rangle$, with edges connecting precisely those cycles with nonempty intersection. Thus, an element in the intersection of an F-cycle and G-cycle represents an edge, and a matching $X \subseteq n$ represents a matching in Γ (i.e., a set of edges such that no two have a vertex in common).

We first show that there is a monadic second-order sentence $\psi(X)$ true precisely when X is a *maximum matching* (i.e., a matching of maximal cardinality). Then we show that for $\varepsilon > 0$, the cardinality m of a maximum matching is almost surely between $(\frac{1}{2} - \varepsilon) \ln n$ and $(1 + \varepsilon) \ln n$. Next we show that quantification over binary relations on a maximum matching is almost surely interpretable in monadic second-order logic (using parameters). Hence, we can almost surely say, for a given maximum matching X, that there is a linear order $\leqslant$ on X and functions π_0 and π_1 on X such that $(\pi_0(x), \pi_1(x))$ enumerates the first m pairs of $X \times X$ in lexicographic order as x ranges over X. Now it is an easy matter to define addition, multiplication, and exponentiation on the initial interval of X of length $j = m^{\frac{1}{2}}$. We know j is almost surely between

$$j_0 = ((\tfrac{1}{2} - \varepsilon) \ln n)^{\frac{1}{2}} \quad \text{and} \quad j_1 = ((1 + \varepsilon) \ln n)^{\frac{1}{2}}.$$

But since we have exponentiation we can write a monadic second-order sentence φ saying $k = \lg j$ is even. By taking small ε and suitable n we can insure that $\ln j_0 = \ln j_1$. For such n, the value of k is the same in almost all structures of C_n, so we regard $k = k(n)$ as a function of n. As in previous theorems, k assumes all large values as n increases. Thus, $\mu_n(\varphi)$ does not converge.

The formula $\psi(X)$ says that X is a matching and there is no augmenting path for X. An *augmenting path* for a matching in Γ is a path between two vertices such that every other edge on the path belongs to the matching, but such that the two end vertices are not incident with any edge in the matching. A well-known theorem, first used by Berge [1] and Norman and Rabin [19] as the basis for an algorithm to find maximum matchings, states that a matching is maximum if and only if it has no augmenting paths. Remember that we represent an edge in Γ by an element in the intersection of an F-cycle and G-cycle. Therefore, it is not difficult to write a monadic second-order formula that says that $Y \subseteq n$ represents a path in Γ and that Y is an augmenting path for a matching X.

Let S be a collection of F-cycles and T a collection of G-cycles. We say S and T *intersect completely* whenever every F-cycle in S intersects every G-cycle in T. Observe that if S and T intersect completely, there is a matching (actually, several) between S and T of size $\min(|S|, |T|)$ this matching may be regarded as an embedding of the smaller of S and T into the larger.

Define S^p to be the set of F-cycles of length at least n^p for $0 \leqslant p \leqslant 1$, and T^p similarly for G-cycles.

We claim that if $0 < p, q < 1$ and $p + q > 1$, then S^p and T^q intersect completely. First observe that by Lemma 3.2, $|S^p|, |T^q| \leqslant (1 + \varepsilon) \ln n$ almost surely. By Lemma 3.1, the probability that a particular F-cycle in S^p is disjoint from a particular G-cycle in T^q is at most $\exp(-n^{p+q-1})$. The probability that S^p and T^q do not intersect completely is less than $((1 + \varepsilon) \ln n)^2 \exp(-n^{p+q-1})$, which approaches 0 as n increases.

Setting $p = q = \frac{1}{2} + \varepsilon$, $\varepsilon > 0$, we have that a maximum matching has size greater than $(\frac{1}{2} - \varepsilon) \ln n$, almost surely (this bound could be improved to $(1 - \varepsilon) \ln n$ with a little more work, but this is not necessary for our purposes). Since the number of F-cycles (or G-cycles) is almost surely less than $(1 + \varepsilon) \ln n$, this gives an upper bound on the size of a maximum matching.

It remains to show that quantification over binary relations on a maximum matching X is almost surely interpretable in monadic second-order logic. We show that X can almost surely be partitioned into sets X_i, $0 \leqslant i \leqslant 3$, such that there are one-to-one functions $f_i : X_i \rightarrow S^{\frac{2}{3}}$ and $g_i : X_i \rightarrow T^{\frac{2}{3}}$ which are definable by monadic second-order formulas (with parameters). We know that $S^{\frac{2}{3}}$ and $T^{\frac{2}{3}}$ intersect completely, so $f_i(X_i)$ and $g_j(X_j)$ intersect completely. Every subset of $X_i \times X_j$ corresponds to a subset of $f_i(X_i) \times g_j(X_j)$ which, in turn, can be represented by a subset $Y_{ij} \subseteq n$. Thus, a binary relation $R \subseteq X \times X$ is represented by a sequence of sets $Y_{ij} \subseteq n$, $0 \leqslant i, j \leqslant 3$. We can quantify over the sets Y_{ij} and hence over the sets $R \subseteq X \times X$.

Let

$X_0 = \{x \in X : x$ is an element of an F-cycle in $S^{\frac{7}{10}}\}$,
$X_1 = \{x \in X - X_0 : x$ is an element of an F-cycle in $S^{\frac{4}{10}}\}$,
$X_2 = \{x \in X - X_0 - X_1 : x$ is an element of a G-cycle in $T^{\frac{7}{10}}\}$,
$X_3 = \{x \in X - X_0 - X_1 - X_2 : x$ is an element of a G-cycle in $T^{\frac{4}{10}}\}$.

By Lemma 3.2, $|X_i| < \frac{3}{10} \ln n$. By definition, the sets X_i, $0 \leqslant i < 3$, are disjoint. We must show that their union is X. To do this it is enough to show that every element of X lies either on an F-cycle in $S^{\frac{4}{10}}$ or on a G-cycle in $T^{\frac{4}{10}}$. We claim that, in fact, this is almost surely the case for every element of n. We show that if $0 < p, q < 1$ and $p + q < 1$, then almost surely every F-cycle of length less than n^p and every G-cycle of length less than n^q are disjoint. Lemma 3.1 tells us that the probability that a particular F-cycle and particular G-cycle satisfying these bounds are disjoint is greater than $\exp(-n^{p+q}/(n - n^p - n^q + 1))$ this quantity is greater than $\exp(-2n^{p+q-1})$ for large n. Therefore, the probability that they intersect is less than $1 - \exp(-2n^{p+q-1}) < 2n^{p+q-1}$. Almost surely there are at most $((1+\varepsilon)\ln n)^2$ F-cycle–G-cycle pairs. But $2((1+\varepsilon)\ln n)^2 n^{p+q-1}$ approaches 0 as n increases. Therefore, almost surely every F-cycle of length less than n^p and G-cycle of length less than n^q are disjoint. Take $p = q = \frac{4}{10}$ to establish the claim.

It remains to show that $f_i : X_i \to S^{\frac{2}{3}}$ and $g_i : X_i \to T^{\frac{2}{3}}$, $0 \leqslant i \leqslant 3$, can be defined.

Each element of X_0 lies on an F-cycle in $S^{\frac{7}{10}} \subseteq S^{\frac{2}{3}}$. Let f_0 map each $x \in X_0$ to the F-cycle that contains it. Thus, $f_0(X_0) \subseteq S^{\frac{2}{3}}$. But $S^{\frac{2}{3}}$ and $T^{\frac{2}{3}}$ intersect completely so $f_0(X_0)$ and $T^{\frac{2}{3}}$ intersect completely. Recall that $|X_0| < \frac{3}{10} \ln n$ and $|T^{\frac{2}{3}}| < \frac{1}{3} \ln n$. Therefore, a matching between $f_0(X_0)$ and $T^{\frac{2}{3}}$ represents an embedding of $f_0(X_0)$ into $T^{\frac{2}{3}}$. Let g_0 be the composition of f_0 and this embedding, so $g_0 : X_0 \to T^{\frac{2}{3}}$ is one-to-one.

This argument shows that if one of f_i or g_i has been defined then the other can be defined.

Now elements of X_1 all lie on F-cycles in $S^{\frac{4}{10}}$. But $S^{\frac{4}{10}}$ and $T^{\frac{2}{3}}$ intersect completely, so there is a matching between the set of F-cycles containing elements in X_1 and $T^{\frac{2}{3}}$. This matching represents a one-to-one function $g_1 : X_1 \to T^{\frac{2}{3}}$. Once g_1 has been defined, f_1 may be defined.

We define f_2, g_2, f_3, g_3 in the same way as f_0, g_0, f_1, g_1 by interchanging the roles of F-cycles and G-cycles.

We quantify over relations $R \subseteq X \times X$ by saying that there exist sets X_i, $0 \leqslant i \leqslant 3$, and one-to-one functions f_i, g_i, $0 \leqslant i \leqslant 3$, represented by certain matchings as described above, such that $f_i(X_i)$ and $g_j(X_j)$ intersect completely, $0 \leqslant i, j \leqslant 3$. Quantification over relations $R \subseteq X \times X$ is thereby reduced to quantification over subsets of n.

The theorem follows now from earlier remarks. □

Remark. The constructions in proofs of Theorems 1, 2, and 3 are more elaborate than required just to show nonconvergence. By coding arithmetic in these constructions we provide the means to specify sentences φ (in the appropriate language) so that $\mu_n(\varphi)$ behaves very erratically. In fact, no reasonable definition for asymptotic probability will be defined for all sentences from the logic in question. Moreover, it is possible to give arguments similar to the one in Kaufmann and Shelah [14] to show that every set of points in the unit interval given by a recursive tree is the set of accumulation points of $\mu_n(\varphi)$ for some sentence φ (see [14] for details). This is much different from the situation in classes investigated by Lynch [17] where for each φ, $\mu_n(\varphi)$ has only finitely many accumulation points. Since the argument of Kaufmann and Shelah requires monadic quantification, we must, in the cases covered by Theorems 1 and 2, restrict to smaller initial segments of arithmetic on which monadic quantification can be defined.

4. Proof of Theorem 4

Theorem 4 follows from the proofs of Theorems 1, 2, and 3, and Lemma 4.1 below. We need some preliminary definitions.

A first-order theory Σ is *finitely inseparable* if there is no recursive set that separates *fsat*(Σ), the set of first-order sentences true in some finite model of Σ, from *inv*, the set of inconsistent first-order sentences for this language. That is, there is no recursive set Δ such that *fsat*$(\Sigma) \subseteq \Delta$ and *inv* $\cap \Delta = \emptyset$. We will say that a class D of finite structures is *finitely inseparable* if it is the class of finite models of a finitely inseparable theory, or, equivalently, if the set of first-order sentences true in every structure in D is finitely inseparable (the usual definition is for theories only, but our results are easier to state for classes of structures). Vaught [25], extending an earlier result of Trachtenbrot [24], showed that the class of all finite structures for a language with a nonunary relation symbol is finitely inseparable. It is easy to see that the class of finite initial segments of arithmetic (which are structures for the language with relation symbols interpreted by the partial operations of successor, addition, and multiplication) is finitely inseparable. This can be shown directly or as a consequence of Vaught's result.

Let D be a nonempty class of finite structures for a language consisting of relation symbols R_i with arities $\alpha(i)$, $i<m$. Let C be a class of structures for some language L. We say that D is *almost surely definable* (for a specified logic) in C if there are formulas $\delta(x, \boldsymbol{u})$, $\rho_i(x_1, \ldots, x_{\alpha(i)}, \boldsymbol{u})$, $i<m$, in L (from the specified logic) such that for each $M \in D$

$$\lim_{n\to\infty} \mu_n(\exists \boldsymbol{u}\ (\langle \delta(x, \boldsymbol{u}), \rho_i(\boldsymbol{x}, \boldsymbol{u})\rangle_{i<m} \cong M)) = 1$$

Here $\langle \delta(x, \boldsymbol{u}), \rho_i(\boldsymbol{x}, \boldsymbol{u})\rangle_{i<m}$ denotes the structure with universe $\delta = \{x \in n : \delta(x, \boldsymbol{u}) \text{ is true}\}$ and relations $\{\boldsymbol{x} \in n^{\alpha(i)}\} : \rho_i(\boldsymbol{x}, \boldsymbol{u}) \text{ is true}\}$, restricted to δ, interpreting R_i, $i<m$.

The following theorem is proved implicitly in Compton [5].

Lemma 4.1. *If a finitely inseparable class D is almost surely definable in C, then every asymptotic problem for C is undecidable.*

Proof. Given a sentence φ in the language for D, form φ' by relativizing quantifiers to $\delta(x, \boldsymbol{u})$, replacing relation symbols $R_i(\boldsymbol{x})$ by formulas $\rho_i(\boldsymbol{x}, \boldsymbol{u})$, and existentially quantifying the new free variables $\boldsymbol{u}$ ($\delta(x, \boldsymbol{u})$ and $\rho_i(\boldsymbol{x}, \boldsymbol{u})$ are as in the definition of almost sure definability). If φ is true in some finite model $M \in D$, then $\mu(\varphi') = 1$ because M is almost surely isomorphic to some structure $\langle \delta(x, \boldsymbol{u}), \rho_i(\boldsymbol{x}, \boldsymbol{u})\rangle_{i<m}$. If φ is inconsistent, then $\mu(\varphi') = 0$. Now every asymptotic problem for C (or its complement) separates $\{\varphi' : \mu(\varphi') = 1\}$ from $\{\varphi' : \mu(\varphi') = 0\}$. If an asymptotic problem for C were decidable, it could be used to recursively separate the sentences true in D from the inconsistent sentences.

Inspecting the proofs of Theorems 1, 2, and 3 we see that in each case arbitrarily large finite initial segments of arithmetic are almost surely definable (first-order definable in Theorems 1 and 2, and monadic second-order definable in Theorem 3). By adding a parameter and restricting to the initial subinterval with the parameter as greatest element, we see that every finite initial segment of arithmetic is almost surely definable. By the lemma, every asymptotic problem is undecidable. □

5. Proof of Theorem 5

The proof of Theorem 5 relies on an idea similar to the one in the proof of Theorem 4. The difference is that rather than showing almost sure definability of a finitely inseparable class, we use a slightly different reduction to a set of sentences with high computational complexity.

Define

$$\exp_0(n) = n, \qquad \exp_{r+1}(n) = 2^{\exp_r(n)}, \quad \text{and} \quad \exp_\infty(n) = \exp_n(1).$$

Clearly, for $c > 0$, $\exp_\infty(cn)$ eventually dominates each $\exp_r(n)$. A set is elementary recursive if, for some r, it is recognized by an $\exp_r(n)$ time-bounded Turing machine. (Here r is a non-negative integer.)

The following is a theorem from Compton and Henson [6].

Lemma 5.1. Let *treesat*$_n$ be the set of first-order sentences in the language of trees (i.e., containing just a binary relation symbol interpreting the parent–child relation) true in some finite tree of height at most h. Let *inv* be the set of inconsistent sentences in this language. If $h \geqslant 3$, there is a $c > 0$ such that no set in NTIME($\exp_{h-2}(cn)$) contains *treesat*$_h$ and is disjoint from *inv*.

Let C_n be the set of structures $\langle n, F\rangle$, where F is a unary function on n. For a given h let $\delta_h(x, u)$ be a formula that says $F^i(x) = u$ for some non-negative $i \leqslant h$. Let $\rho(x, y, u)$ be the formula $(F(y) = x \wedge y \neq u)$. Clearly $\langle \delta_h(x, u), \rho(x, y, u)\rangle$ is a tree of height at most h for each $u \in n$ (we regard $\rho(x, y, u)$ restricted to $\{x \in n : \delta(x, u)\}$ as relating parent–child pair (x, y)). Theorem 4.4 of Lynch [18] implies that for every finite tree M

$$\lim_{n\to\infty} \mu_n(\exists u\,[\langle \delta_n(x, u), \rho(x, y, u)\rangle \cong M]) = 1.$$

Now given a sentence φ of length n in the language of trees, form φ' by relativizing quantifiers $\forall x$ and $\exists x$ to $\delta_h(x, u)$, replacing $P(x, y)$ (the parent–child relation symbol applied to x and y) with $\rho(x, y, u)$, and existentially quantifying the new free variable u. Obviously, $|\varphi'| = O(|\varphi|)$ and the mapping that takes φ to φ' is linear time computable. If φ is true in a finite tree M of height h, then $\mu(\varphi) = 1$ because M is almost surely isomorphic to some tree $\langle \delta_h(x, u), \rho(x, y, u)\rangle$. If φ is inconsistent, then $\mu(\varphi') = 0$. Now if for every $c > 0$ there was a set in NTIME($\exp_{h-2}(cn)$) containing $\{\varphi' : \mu(\varphi') = 1\}$ and disjoint from $\{\varphi' : \mu(\varphi') = 0\}$, we would violate Lemma 5.1. Thus, no asymptotic problem for C is elementary recursive. In fact, using techniques from Compton and Henson [6] it is possible to show that there is a $c > 0$ such that no set in NTIME($\exp_\infty(cn)$) contains $\{\varphi : \mu(\varphi') = 1\}$ and is disjoint from $\{\varphi' : \mu(\varphi') = 0\}$. □

6. Conclusion

The techniques we have introduced here play the same role for asymptotic combinatorics as classical undecidability methods play for algebraic theories. We demonstrate nonconvergence, undecidability, and intractability by showing almost sure definability of certain simple classes. We note that although nonconvergence and undecidability of asymptotic problems are closely related, they are not coincident. Compton [5] shows that one may have convergence but undecidable asymptotic problems. The cases considered here lie close to the convergent-nonconvergent and decidable-undecidable borderlines. Other borderline cases (such as structures consisting of a pair of equivalence relations, or unary function plus linear order, or binary relation plus unary function, etc.) can very likely be resolved by these methods.

References

[1] C. Berge, Two theorems in graph theory, Proc. Nat. Acad. Sci. U.S.A. 43 (1957) 842–844.

[2] A. Blass, Y. Gurevich and D. Kozen, A zero–one law for logic with a fixed-point operator, Inform. and Control 67 (1986) 70–90.

[3] K. Compton, Application of a Tauberian theorem to finite model theory, Arch. Math. Logik Grundlag. 25 (1985) 91–98.

[4] K. Compton, A logical approach to asymptotic combinatorics II: Monadic second order properties, to appear.

[5] K. Compton, An undecidable problem in finite combinatorics, J. Symbolic Logic 49 (1984) 842–850.

[6] K. Compton and C.W. Henson, A simple method for proving lower bounds on the complexity of logical theories, Ann. Pure Appl. Logic, to appear.

[7] K. Compton and S. Shelah, A convergence theorem for unary functions, in preparation.

[8] Y. Ershov, I. Lavrov, A. Taimanov and M. Taitslin, Elementary theories, Russian Math. Surveys 20 (1965) 35–105.

[9] R. Fagin, Probabilities on finite models, J. Symbolic Logic 41 (1976) 50–58.

[10] J. Ferrante and C. Rackoff, The Computational Complexity of Logical Theories, Lecture Notes in Math. 718 (Springer, Berlin, 1979).

[11] Y. Glebskii, D. Kogan, M. Liogonkii and V. Talanov, Range and degree of realizability of formulas in the restricted predicate calculus, Kibernetika (Kiev) 2 (1969) 17–28. English translation: Cybernetics 5 (1972) 142–154.

[12] V. Goncharov, Sur la distribution des cycles dans les permutations, Dokl. Akad. Nauk SSSR 35 (1942) 267–269.

[13] E. Grandjean, Complexity of the first-order theory of almost all finite structures, Inform. and Control 57 (1983) 180–204.

[14] M. Kaufmann and S. Shelah, Random models of finite power and monadic logic, Discrete Math. 54 (1985) 285–293.

[15] V. Kolchin, B. Sevast'yanov and V. Chistyakov, Random Allocations (Winston, Washington, 1978).

[16] M. Kruskal, The expected number of components under a random mapping function, Amer. Math. Monthly 61 (1954) 392–397.

[17] J. Lynch, Almost sure theories, Ann. Math. Logic 18 (1980) 91–135.

[18] J. Lynch, First-order probabilities of random unary functions, Trans. Amer. Math. Soc. 287 (1985) 543–568.

[19] R. Norman and M. Rabin, An algorithm for a minimum cover of a graph, Proc. Amer. Math. Soc. 10 (1959) 315–319.

[20] M. Rabin, Decidable theories, in: J. Barwise, ed., Handbook of Mathematical Logic (North-Holland, Amsterdam, 1977).

[21] A. Renyi, Probability Theory (North-Holland, Amsterdam, 1970).

[22] J. Riordan, Enumeration of linear graphs for mappings of finite sets, Ann. Math. Stat. 33 (1962) 178–185.

[23] L. Shepp and S. Lloyd, Ordered cycle lengths in random permutations, Trans. Amer. Math. Soc. 121 (1966) 340–357.

[24] B. Trachtenbrot, Impossibility of an algorithm for the decision problem in finite classes, Dokl. Akad. Nauk SSSR 70 (1950) 569–572. English translation: AMS Transl. Ser. (2) 23 (1963) 1–5.

[25] R. Vaught, On a theorem of Cobham concerning undecidable theories, Logic Methodology and Philosophy of Science (Proc. of the 1960 International Congress), Stanford University Press, Stanford, 1962) 19–25.