Logical Definability of Counting Functions

Kevin J. Compton
EECS Department
University of Michigan
Ann Arbor, MI 48109-2122
USA
kjc@eecs.umich.edu

Erich Grädel
Mathematische Grundlagen der Informatik
RWTH Aachen
D-52056 Aachen
Germany
graedel@informatik.rwth-aachen.de

Abstract

The relationship between counting functions and logical expressibility is explored. The most well studied class of counting functions is #P, which consists of the functions counting the accepting computation paths of a nondeterministic polynomial-time Turing machine. For a logic L, $\#L$ is the class of functions on finite structures counting the tuples $(\bar{T}, \bar{c})$ satisfying a given formula $\psi(\bar{T}, \bar{c})$ in L. Saluja, Subrahmanyam, and Thakur showed that on classes of ordered structures #FO = #P (where FO denotes first-order logic) and that every function in $\#\Sigma_1$ has a fully polynomial randomized approximation scheme. We give a probabilistic criterion for membership in $\#\Sigma_1$. A consequence is that functions counting the number of cliques, the number of Hamilton cycles, and the number of pairs with distance greater than two in a graph, are not contained in $\#\Sigma_1$. It is shown that on ordered structures $\#\Sigma^1_1$ captures the previously studied class spanP. On unordered structures #FO is a proper subclass of #P and $\#\Sigma^1_1$ is a proper subclass of spanP; in fact, no class $\#L$ contains all polynomial-time computable functions on unordered structures. However, it is shown that on unordered structures every function in #P is identical almost everywhere with some function #FO, and similarly for $\#\Sigma^1_1$ and spanP. Finally, we discuss the closure properties of #FO under arithmetical operations.

1 Introduction

The relationship between computational complexity and the expressive power of logical languages is an important topic in finite model theory. Early results in this area focussed on decision problems and relational queries. Examples include the Büchi-Elgot-Trakhtenbrot theorem [8, 11, 33] characterizing regular languages in terms of monadic second-order logic (probably the first result in the area) and Fagin's theorem [12] characterizing NP in terms of existential second-order logic (often cited as the beginning of finite model theory as a separate research area). Other results followed, notably the Immerman-Vardi [21, 35] characterization of P in terms of least fixed point logic, and Immerman's logical characterizations of other complexity classes, such as the characterizations of logarithmic space complexity classes in terms of transitive closure logics [22]. The most important results in this field are surveyed in [18, 23].

More recent investigations concern logical expressibility in other areas of complexity theory such as *optimization* and *counting*. As with the earlier work, these results reveal the logical structure of complexity, but moreover, they yield insights that could not be achieved without a logical framework. Papadimitriou and Yannakakis [30], for example, set forth a new, logical approach to efficient approximation for NP-optimization problems. Exploiting Fagin's theorem, they present two syntactically defined classes of optimization problems, MAX SNP and MAX NP. Optimal solutions to problems in these classes are approximable to within a constant factor in polynomial-time. Arora et. al. [1] showed that problems hard for MAX SNP cannot have a polynomial-time approximation scheme unless P = NP.

Kolaitis and Thakur [26, 27] systematically investigated logical expressibility of optimization problems. They defined MAX Σ_n (respectively, MAX Π_n) to be the class of problems which, given a finite structure $\mathfrak{A}$, compute the maximum number of tuples $\bar{x}$ in $\mathfrak{A}$ satisfying a Σ_n (respectively, Π_n) formula $\psi(\bar{x}, \bar{S})$ as $\bar{S}$ ranges over predicates on $\mathfrak{A}$. (The classes MAX SNP and MAX NP are the closures of the syntactic classes MAX Σ_0 and MAX Σ_1 under appropriate reductions.) Kolaitis and Thakur showed that the classes MAX Σ_n and MAX Π_n collapse to a strict hierarchy of four levels:

$$\text{MAX } \Sigma_0 \subsetneq \text{MAX } \Sigma_1 \subsetneq \text{MAX } \Pi_1 \subsetneq \text{MAX } \Pi_2 = \text{MAXFO}.$$

In [5] we extended the logical approach to approximability by allowing formulae to contain predicates definable in least fixed point logic and maximization to be taken over constants as well as predicates. We also introduced a new method characterizing rates of growth of average optimal solution sizes thereby showing that a number of important problems do not belong to MAX Σ_1 with fixed point predicates. This method is related to *limit laws* in finite model theory and the *probabilistic method* from combinatorics.

The success of the logical approach to optimization problems motivated research along similar lines on counting functions. A well studied complexity class of such functions is Valiant's class #P consisting of the functions that count the number of accepting computation paths of a given nondeterministic polynomial-time Turing machine [34]. Saluja, Subrahmanyam and Thakur [32] considered the class #FO consisting of all functions which, given a finite structure $\mathfrak{A}$, compute the number of tuples $\bar{T}, \bar{c}$ such that $\mathfrak{A} \models \psi(\bar{T}, \bar{c})$ where ψ is a first-order formula. The class $\#\Sigma_n$ (respectively, $\#\Pi_n$) is defined analogously with respect to formulae in the prefix class Σ_n (respectively, Π_n). Saluja, et al. show that on ordered structures #FO captures #P, and that the classes $\#\Sigma_i$ and $\#\Pi_i$ form a proper hierarchy of five levels.

Theorem 1.1 (Saluja, Subrahmanyam, Thakur) *On ordered structures*

$$\#\Sigma_0 \subsetneq \#\Sigma_1 \subsetneq \#\Pi_1 \subsetneq \#\Sigma_2 \subsetneq \#\Pi_2 = \#\text{FO} = \#\text{P}.$$

In contrast to the situation with optimization problems, the restriction to ordered structures is necessary here. (We will discuss this in detail.) A similar phenomenon occurs with the logical characterizations of decision problems. Linear orders may be introduced in existential second-order logic, so Fagin's theorem applies to arbitrary structures. The other logical characterizations of complexity classes cited in the first paragraph apply only to classes of ordered structures.

As with optimization problems, counting functions are efficiently approximable in the existential case. Here the appropriate notion of approximability is the existence of a fully polynomial randomized approximation scheme (FPTRAS).

Theorem 1.2 (Saluja, Subrahmanyam, Thakur) *Every function in $\#\Sigma_1$ has a FPTRAS.*

In this paper we continue the investigation on the relationship between counting classes and expressibility. We will be concerned with membership in classes such as $\#\Sigma_1$ and #FO and, more generally, with membership in classes $\#L$ where L is an arbitrary logic. We will also explore the differences between these classes on ordered and unordered structures.

In section 3 we give some background on limit laws in logic. In section 4 we use these results to prove a probabilistic criterion for membership in the class $\#\Sigma_1$ (on unordered structures) similar to the one we established in [5] for MAX Σ_1^{FP}. We show that every function in $\#\Sigma_1$ has an expected value of $\Theta(q(n)2^{p(n)})$, where $p(n), q(n)$ are polynomials; moreover, if the function is not identically 0, then its expectation is non-zero. As a consequence, functions with different growth rates, such as functions counting the number of cliques, or the number of Hamilton cycles, or the number of pairs with distance greater than two in a graph, are not contained in $\#\Sigma_1$. This criterion is then extended to the closure of $\#\Sigma_1$ under infinitary reductions.

In section 5 we investigate functions defined by more powerful logics than FO. It turns out that fixed point logic defines the same functions as first-order logic, but going up to existential second-order logic provides more expressive power. On ordered structures $\#\Sigma_1^1$ captures the class spanP. This class was introduced by Köbler, Schöning and Toràn [24] and contains the functions which are definable as the number of different outputs produced by a nondeterministic polynomial-time Turing machine. On unordered structures, $\#\Sigma_1^1$ is a proper subclass of spanP. In fact, we prove that no class of the form $\#L$ contains all polynomial-time computable functions on unordered structures. This holds for arbitrary logics L; the only assumption we make is that logics do not distinguish between isomorphic structures.

Despite this general and unavoidable weakness of logical counting classes we can prove that in a probabilistic sense, #FO and $\#\Sigma_1^1$ come very close to capturing #P and spanP on unordered structures, provided the underlying vocabulary is rich enough (i.e., contains at least one non-unary predicate). Indeed for every function $F \in \#\mathrm{P}$ there exists a function $F' \in \#\mathrm{FO}$ such that $F = F'$ on almost all structures (and similarly for $\#\Sigma_1^1$ and spanP). To prove these results we use a theorem by Babai, Erdös and Selkow that there exist polynomial-time algorithms that compute canonical orderings on almost all graphs.

In the last section we consider closure properties for classes $\#L$. It is known that #P is closed under a number of operations, such as addition, multiplication, binomial coefficients and others. We show that all these closure properties hold also for #FO. On the other hand, there are other operations, such as subtraction, division, minima, medians, etc., under which #P is closed only if certain generally believed assumptions in complexity theory fail. We show without using unproved complexity-theoretic assumptions that #FO is not closed under any of these operations.

2 Preliminaries

2.1 Complexity and definability classes of counting functions

Let M be a nondeterministic polynomial-time Turing machine (abbreviated NPTM). By convention, every accepting computation path of M produces precisely one output, and no rejecting path produces an output. We denote by $\mathrm{acc}(M, x)$ the set of all accepting computation paths of M on input x, and by $\mathrm{out}(M, x)$ the set of all outputs produced by these paths.

Definition 2.1 A function f from a set of words D into $\mathbb{N}$ is in #P if there exists a NPTM M such that $f(x) = |\mathrm{acc}(M, x)|$ for all $x \in D$. A function $f : D \to \mathbb{N}$ is in the class spanP if there is a NPTM M such that $f(x) = |\mathrm{out}(M, x)|$ for all $x \in D$.

In this paper we are mostly interested in functions $F : \mathcal{C} \rightarrow \mathbb{N}$ where $\mathcal{C}$ is a class of finite structures over a fixed vocabulary and where F is invariant under isomorphism, i.e., $F(\mathfrak{A}) = F(\mathfrak{B})$ for $\mathfrak{A} \cong \mathfrak{B}$. Such functions are called *numerical invariants* or just *invariants*.

Definition 2.2 Let $\mathcal{C}$ be a class of finite structures over a fixed vocabulary τ (e.g., the class of all finite graphs). Let L be a class of logical formulae over τ, with additional relation and constant parameters. A function $F : \mathcal{C} \rightarrow \mathbb{N}$ is in $\#L$ if there exists a formula $\psi(\bar{T}, \bar{c})$ in L such that for all structures $\mathfrak{A} \in \mathcal{C}$

$$F(\mathfrak{A}) = |\{(\bar{T}, \bar{c}) : \mathfrak{A} \models \psi(\bar{T}, \bar{c})\}|.$$

In particular, #FO is the class of functions definable in this sense by first-order formulae.

Example. Given an undirected graph $G = (V, E)$, let $\#\mathrm{pm}(G)$ be the number of perfect matchings of G. This function is in #FO since it is definable by the expression

$$\#\mathrm{pm}(G) = |\{M : G \models \varphi(M)\}|$$

where $\varphi(M)$ says that M is a perfect matching:

$$\varphi(M) = \forall x \forall y\, (Mxy \rightarrow (Myx \wedge Exy)) \wedge \forall x \exists y\, Mxy \wedge \forall x \forall y \forall z\, (Mxy \wedge Mxz \rightarrow y = z).$$

We designate the vocabulary of the relation parameters $\bar{T} = T_1, \ldots, T_s$ by σ. Thus, ψ is in fact a sentence over the vocabulary $\tau \cup \sigma \cup \{\bar{c}\}$. For future reference, we suppose that relation symbols $T_1, \ldots, T_s$ have arities $m_1, \ldots, m_s$ and define the polynomial $p_\sigma(n) := \sum_{i=1}^{s} n^{m_i}$. Obviously, there exist precisely $2^{p_\sigma(n)}$ different interpretations of $\bar{T}$ on a given universe of cardinality n.

We say that a class L of logical formulae (over some vocabulary τ) is *closed under positive first-order operations* if it contains all atomic and negated atomic formulae over the vocabulary τ and if for all formulae ψ and φ of L and all element variables x, L contains formulae that are equivalent (on finite structures) to $(\psi \wedge \varphi)$, $(\psi \vee \varphi)$, $\exists x\, \psi$ and $\forall x\, \psi$.[1] If L is closed under positive first-order operations, then every function $F \in \#L$ can be defined by an expression $F(\mathfrak{A}) = |\{T : \mathfrak{A} \models \psi(T)\}|$ where $\psi(T)$ is a formula of L with precisely one relation parameter T and no constant parameter.

2.2 Logics

We give some background on the most important logics that are of interest to finite model theory and descriptive complexity. This section may be skipped by readers who are familiar with these fields.

Several logics will be used in this paper. The most basic one is first-order logic, denoted FO. As usual Σ_m (respectively, Π_m) denotes the classes of all first-order formulae in prenex normal form with m alternating blocks of quantifiers starting with $\exists$ (respectively, $\forall$).

It is well-known that first-order logic is not very expressive. In fact every first-order definable class of structures can be decided with polynomial-size constant-depth circuit, i.e. $\mathrm{FO} \subseteq \mathrm{AC}^0$.

More expressive logics considered in this paper are existential second-order logic Σ_1^1, the least fixed point logic FP, and the infinitary logic $L^{\omega}_{\infty\omega}$.

[1] For some of the logics considered in this paper, such as Σ_1^1, it is not known whether they are closed (up to logical equivalence) under negation on the class of finite structures.

Existential second-order logic and NP. The class of all formulae of the form

$$\exists R_1 \cdots \exists R_t \psi$$

where ψ is first-order, is called *existential second order logic* and is denoted Σ^1_1. This logic is of fundamental importance for complexity theory due to the following celebrated result [12].

Theorem 2.3 (Fagin) *Let $\mathcal{C}$ be a class of finite structures over a fixed vocabulary closed under isomorphisms. Then $\mathcal{C}$ is in* NP *if and only if there exists a sentence $\psi \in \Sigma^1_1$ such that $\mathcal{C} = \{\mathfrak{A} : \mathfrak{A} \models \psi\}$.*

Let us briefly discuss the proof of (the non-trivial direction of) Fagin's Theorem. First suppose that $\mathcal{C}$ is a class of *ordered* finite structures $(\mathfrak{A}, <)$ — where $\mathfrak{A}$ has vocabulary τ and $<$ is a total order on the universe of $\mathfrak{A}$. The ordering allows for a canonical encoding of the structures as binary strings: Represent every predicate $R^{\mathfrak{A}} \subseteq A^k$ by its characteristic string $\chi(R^{\mathfrak{A}})$ whose m-th bit is 1 if and only if the m-th tuple of A^k (with the respect to the lexicographical order on A^k induced by $<$) belongs to $R^{\mathfrak{A}}$.

Fagin proved that from any nondeterministic polynomial-time Turing machine M that decides $\mathcal{C}$ one can construct a first-order sentence $\varphi(<, \bar{T})$ over the vocabulary $\tau \cup \{<, \bar{T}\}$ such that

$$(\mathfrak{A}, <, \bar{T}) \models \exists \bar{T}\, \varphi$$

if and only if the relations $\bar{T}$ describe an accepting computation of M on (the encoding of) $(\mathfrak{A}, <)$. It follows that

$$(\mathfrak{A}, <) \models \exists \bar{T}\, \varphi \qquad \text{iff} \qquad (\mathfrak{A}, <) \in \mathcal{C}.$$

To understand the rôle of the ordering, one should keep in mind that Turing machines operate on strings while logical formulae express properties of structures. When we say that a Turing machine M accepts a class $\mathcal{C}$ of structures we actually mean that M accepts the set of encodings of the structures in $\mathcal{C}$. But to specify an encoding one needs an ordering on the universe.

Nevertheless, the assumption that the structures be ordered can be dispensed with in this case. Indeed, let $\mathcal{C}$ be a class of not necessarily ordered τ-structures accepted by M. In existential second-order logic we can introduce an ordering by existentially quantifying over a binary relation $<$ and using a first-order formula $\alpha(<)$ which expressing that $<$ does indeed define a total order; in fact $\alpha(<)$ is in Π_1. As a consequence we obtain that for all τ-structures $\mathfrak{A}$

$$\mathfrak{A} \in \mathcal{C} \qquad \text{iff} \qquad \mathfrak{A} \models (\exists <)(\exists \bar{T})(\alpha \wedge \varphi).$$

Fixed point logic. The expressive power of first-order logic is limited by the lack of a mechanism for unbounded iteration or recursion. The most notable example of a query that is not first-order expressible is the transitive closure (TC) of a relation. This has motivated the study of more powerful languages that add recursion in one way or another to first-order logic. The most prominent of these are the various forms of *fixed point logics*.

Let τ be a vocabulary, P an r-ary predicate not in τ and $\psi(\bar{x})$ be a formula over the vocabulary $\tau \cup \{P\}$ with only positive occurrences of P and with free variables $\bar{x} = x_1, \ldots, x_r$. Then ψ defines, for every finite τ-structure A with universe $|A|$, an operator ψ^A on the class of r-ary relations over $|A|$ by

$$\psi^A : P \longmapsto \{\bar{a} : (A, P) \models \psi(\bar{a})\}.$$

Since P occurs only positively in ψ, this operator is monotone, i.e. $Q \subseteq P$ implies that $\psi^A(Q) \subseteq \psi^A(P)$. Therefore this operator has a *least fixed point* which may be constructed inductively beginning with the empty relation. Set $\Psi^0 := \emptyset$ and $\Psi^{j+1} := \psi^A(\Psi^j)$. At some stage i, this process reaches a stable predicate $\Psi^i = \Psi^{i+1}$, which is the *least fixed point* of ψ on A, and denoted by Ψ^∞. Since $\Psi^i \subseteq \Psi^{i+1}$, the least fixed point is reached in a polynomial number of iterations, with respect to the cardinality of A.

The fixed point logic FP is defined by adding to the syntax of first order logic the *least fixed point formation rule:* if $\psi(\bar{x})$ is a formula over the vocabulary $\tau \cup \{P\}$ with the properties stated above and $\bar{u}$ is an r-tuple of terms, then

$$[\mathrm{LFP}_{P,\bar{x}}\ \psi](\bar{u})$$

is a formula over the vocabulary τ (to be interpreted as $\Psi^\infty(\bar{u})$).

Example. Here is a fixed point formula that defines the reflexive, transitive closure of the binary predicate E:

$$\mathrm{TC}(u,v) \equiv [\mathrm{LFP}_{T,x,y}\ (x=y) \vee (\exists z)(Exz \wedge Tzy)](u,v).$$

On the class of all finite structures, FP has strictly more expressive power than first-order logic — it can express the transitive closure — but is strictly weaker than PTIME-computability. However, Immerman [21] and Vardi [35] proved that on *ordered structures* the situation is different. There FP characterizes precisely the queries that are computable in polynomial time. On the other hand, on very simple classes of structures, such as structures with empty vocabulary (i.e. sets), FP collapses to first-order logic.

Infinitary logic. Infinitary logics are extensions of first-order logic admitting disjunctions and conjunctions over infinite sets of formulae.

Definition 2.4 The logic $L_{\infty\omega}$ is the smallest class of expressions such that

(i) $L_{\infty\omega}$ contains all first-order formulae;

(ii) if ψ is a formula of $L_{\infty\omega}$, then so is $\neg\psi$;

(iii) if ψ is a formula of $L_{\infty\omega}$ and x_i is a variable, then $\exists x_i\psi$ and $\forall x_i\psi$ are formulae of $L_{\infty\omega}$;

(iv) if Φ is a set of formulae of $L_{\infty\omega}$ then $\bigvee\Phi$ and $\bigwedge\Phi$ are formulae of $L_{\infty\omega}$.

Infinitary formulae may have an infinite number of distinct variables. Further, note that *every* class of finite structures is definable in $L_{\infty\omega}$. Thus, this logic is too powerful to be of much interest in finite model theory.

However, by restricting the number of variables we obtain logics that have turned out to be very important for finite model theory.

For any natural number k, the logic $L^k_{\infty\omega}$ is the class of all formulae in $L_{\infty\omega}$ that contain only the variables $x_1, \ldots, x_k$. Further, $L^\omega_{\infty\omega} = \bigcup_k L^k_{\infty\omega}$.

One of the reasons for the importance of this logic is that it contains many of the logics of interest in descriptive complexity, such as the various forms of fixed point logics. On the other hand the Ehrenfeucht-Fraïssé method that characterizing elementary equivalence generalizes to a very elegant game-theoretic characterisation of the distinctive power of $L^\omega_{\infty\omega}$ in terms of pebble games [3, 20, 31]. Most of the inexpressibility results for fixed point logics are proved using these games, so they establish in fact an inexpressibility result for $L^\omega_{\infty\omega}$.

Atomic types and equality types.

Definition 2.5 Let τ be a relational vocabulary and $x_1, \dots, x_k$ be distinct variables. A maximally consistent set t of τ-atoms and negated τ-atoms (including equalities and inequalities) in $x_1, \dots, x_k$ is called an *atomic τ-type in $x_1 \dots, x_k$*. Since such a set is always finite, we can form in first-order logic the conjunction of the formulae in t; by abuse of notation, we denote this conjunction by $t(x_1, \dots, x_k)$. On every τ-structure $\mathfrak{A}$, the type t defines the set of realizations $t^{\mathfrak{A}} = \{\bar{u} \in A^k : \mathfrak{A} \models t(\bar{u})\}$.

An *equality type* is an atomic type over the empty vocabulary, i.e., a maximally consistent set e of equalities $x_i = x_j$ and inequalities $x_i \neq x_j$, where $1 \leq i < j \leq k$. On every structure $\mathfrak{A}$, an equality type e defines the set $e^{\mathfrak{A}} = \{\bar{u} \in A^k : \mathfrak{A} \models e(\bar{u})\}$.

The number of different equality types of k-tuples is clearly bounded by a number which depends only on k.

Lemma 2.6 *For every equality type e there is a polynomial $G_e(n)$ such that the size of $e^{\mathfrak{A}}$ for each finite $\mathfrak{A}$ is $G_e(|\mathfrak{A}|)$.*

Proof. Let i be the number of distinct components in every tuple $\bar{u}$ satisfying φ_e. Set $G_e(n) = n(n-1)\cdots(n-i+1)$. ∎

Lemma 2.7 *Every quantifier-free first-order formula is equivalent to a disjunction over atomic types.*

Proof. Let $\psi(x_1, \dots, x_k)$ be quantifier-free. Then ψ is equivalent to the disjunction

$$\bigvee_{t \models \psi} t(x_1, \dots, x_k)$$

over all atomic types that imply ψ. ∎

3 Asymptotic probabilities in logic

We review here the results on asymptotic probabilities of logical sentences that we need for analysing $\#\Sigma_1$. A more comprehensive survey of this area is given in [10].

Let τ be a relational vocabulary. For $\mathcal{C}$ being the class of all finite τ-structures or the class of all graphs, let $\Omega(n)$ be the probability space of all structures in $\mathcal{C}$ with universe $\{0, \dots, n-1\}$ with the uniform probability distribution.[2]

Given a τ-sentence ψ of some logic L, we denote by $\mu_n(\psi)$ the probability that $\mathfrak{A} \models \psi$ for a randomly chosen $\mathfrak{A} \in \Omega(n)$. An interesting question is, whether the limit $\mu(\psi) := \lim_{n\to\infty} \mu_n(\psi)$ exists and to determine the possible values of $\mu(\psi)$ as ψ ranges over the sentences in L.

The first result of this kind is the 0-1 law for first-order logic which was proved independently by Glebskiĭ et al. [15] and by Fagin [13].

[2] Not all $\{E\}$-structures are graphs. However, the results on asymptotic probabilities go through for the class of all graphs since it is a *parametric* class, (as are the classes of digraphs or tournaments) cf. [10].

Theorem 3.1 *For every first-order sentence ψ over a relational vocabulary, either $\mu(\psi) = 0$ or $\mu(\psi) = 1$.*

We present an outline of Fagin's proof. Suppose we have atomic types $s(x_1, \ldots, x_k)$ and $t(x_1, \ldots, x_k, x_{k+1})$ such that $s \subset t$. Then we can formulate the *extension axiom*

$$\sigma_{s,t} = \forall x_1 \cdots \forall x_k (s(\bar{x}) \rightarrow \exists x_{k+1} t(\bar{x}, x_{k+1})).$$

It states that every realization of s can be extended to a realization of t. It was observed by Fagin [13] that every extension axiom is almost surely true on random finite structures, and that the rate of convergence is exponential.

Lemma 3.2 *For every extension axiom $\sigma_{s,t}$, and all sufficiently large n*

$$\mu_n(\sigma_{s,t}) \geq 1 - c^{-n}$$

for some constant $c > 1$.

Using a common model-theoretic technique known as a *back and forth* argument, Gaifman [14] showed that the collection T of all extension axioms over a vocabulary τ is an $\aleph_0$*-categorical theory*. This means that up to isomorphism, T has precisely one countably infinite model $\mathfrak{R}$, which is often called the *countable random structure* over the vocabulary τ. (When we deal with graphs $\mathfrak{R}$ is also called the *Rado graph.*) As a consequence the theory T is complete. By compactness it follows that a first order sentence ψ is true in $\mathfrak{R}$ if and only if it is consequence of a finite collection of extension axioms. Thus,

$$\mathfrak{R} \models \psi \text{ iff } \mu(\psi) = 1.$$

This immediately implies the 0-1 law for first-order logic. Moreover it proves that all probability sequences $\mu_n(\psi)$ have exponential rate of convergence.

More precise results can be obtained by analysing the properties of the countable random structure $\mathfrak{R}$. Using again a back and forth argument, one shows that $\mathfrak{R}$ is *homogeneous*: Given any two k-tuples $\bar{a}$ and $\bar{b}$ satisfying the same atomic type, there exists an automorphism of $\mathfrak{R}$ taking $\bar{a}$ to $\bar{b}$. This implies that for any atomic type $s(\bar{x})$ and any first-order formula $\psi(x)$, either

$$\mathfrak{R} \models \forall \bar{x}\, (s(\bar{x}) \rightarrow \psi(\bar{x}))$$

or

$$\mathfrak{R} \models \forall \bar{x}\, (s(\bar{x}) \rightarrow \neg\psi(\bar{x})).$$

Here, we will need a stronger form of Theorem 3.1, involving formulae rather than sentences.

Note that for a formula $\psi(\bar{x})$ and a tuple $\bar{u}$ of natural numbers, the asymptotic probability $\mu(\psi(u))$ need no longer be 0 or 1, even if ψ is atomic. For instance, for the formula $P(0)$, we have $\mu_n(P(0)) = 1/2$ for all n.

However, it turns out that the limit $\mu(\psi(\bar{u}))$ always exists, and that its value depends only on $\psi(\bar{x})$ and on the *equality type* of $\bar{u}$ rather than on $\bar{u}$ itself.

Theorem 3.3 *Let $\psi(\bar{x})$ be a first-order formula with free variables $\bar{x} = x_1, \ldots, x_k$ and let e be an equality type of k-tuples.*

(i) There exists a dyadic rational[3] q_e *such that for every tuple* $\bar{u} \in \mathbb{N}^k$ *satisfying* $e(\bar{u})$, *the probability that a randomly chosen structure* $\mathfrak{A} \in \Omega(n)$ *is a model of* $\psi(\bar{u})$ *converges exponentially fast to* q_e.

(ii) If ψ *is existential and* $q_e = 0$ *then* $e(\bar{x}) \wedge \psi(\bar{x})$ *is logically invalid.*

PROOF. *(i):* Let $X_{\psi,e}$ be the set of atomic types $s(x_1, \ldots, x_k)$ such that

$$\mathfrak{R} \models \forall \bar{x}(s(\bar{x}) \rightarrow (e(\bar{x}) \wedge \psi(\bar{x}))).$$

In particular e is the unique equality type compatible with $s \in X_{\psi,e}$. On the other hand, for a given equality type e, the number of atomic types s in k variables with $e \subset s$ is 2^m for some m. Given a tuple $\bar{u} \in \mathbb{N}^k$ realizing e, the probability that $\bar{u}$ also realizes s on a random structure $\mathfrak{A} \in \Omega(n)$ is $\mu_n(s(\bar{u})) = 2^{-m}$, for all $n > \max u_i$ (for smaller n, this probability is not defined). Let

$$\alpha(\bar{x}) = \bigvee_{s \in X_{\psi,e}} s(\bar{x}).$$

Thus $\mu_n(\alpha(\bar{u})) = |X_{\psi,e}| 2^{-m} =: q_e$ for sufficiently large n.

On the other hand, the fact that in $\mathfrak{R}$, every atomic type $s(\bar{x})$ implies either $\psi(\bar{x})$ or $\neg\psi(\bar{x})$ gives

$$\mathfrak{R} \models \forall \bar{x}\, (e(\bar{x}) \rightarrow (\alpha(x) \leftrightarrow \psi(\bar{x}))).$$

Since all sentences true in $\mathfrak{R}$ are true on finite random structures with probability converging to one exponentially fast, we infer that the sequence $\mu_n(\psi(\bar{u}))$ converges exponentially fast to $\mu(\alpha(\bar{u})) = q_e$.

(ii): Let $\psi(\bar{x}) = \exists \bar{y}\, \varphi(\bar{x}, \bar{y})$ where φ is quantifier-free. Suppose that $e(\bar{x}) \wedge \psi(\bar{x})$ is satisfiable. We will prove that $\mu(\psi(\bar{u})) > 0$ for tuples $\bar{u}$ of equality type e.

There exists a structure $\mathfrak{A}$ and tuples $\bar{u}$ and $\bar{v}$ such that

$$\mathfrak{A} \models e(\bar{u}) \wedge \varphi(\bar{u}, \bar{v}).$$

Let $s(\bar{x})$ and $t(\bar{x}, \bar{y})$ be the atomic types of $\bar{u}$ and $(\bar{u}, \bar{v})$ in $\mathfrak{A}$. The probability that a tuple $\bar{u}$ of equality type e realizes s is $2^{-\ell}$ for some ℓ.

The sentence

$$\forall \bar{x}\, ((s(\bar{x}) \rightarrow \exists \bar{y}\, t(x, y))$$

is a consequence of a finite collection of extension axioms, so it holds almost surely in a random structure. As a consequence, we also get that that

$$\mu(\forall \bar{x}\, (s(\bar{x}) \rightarrow \psi(\bar{x}))) = 1.$$

But this implies that for any tuple $\bar{u}$ of equality type e

$$\mu(\psi(\bar{u})) \geq \mu(s(\bar{u})) = 2^{-\ell} > 0.$$

■

[3] A dyadic rational is a rational number whose denominator is a power of two.

It turns out that 0-1 laws also hold for many important extensions of first-order logic, such as fixed point logic, infinitary logic $L^{\omega}_{\infty\omega}$ and some fragments of existential second-order logic.

In particular, Kolaitis and Vardi [28] established the 0-1 law for $L^{\omega}_{\infty\omega}$ and proved that $L^{\omega}_{\infty\omega}$ admits quantifier elimination on a dense class of models.

Theorem 3.4 *For every formula $\psi(\bar{x})$ in $L^{\omega}_{\infty\omega}$ there exists a quantifier-free formula $\alpha(\bar{x})$ such that*

$$\mathfrak{A} \models \forall\bar{x}(\psi(\bar{x}) \leftrightarrow \alpha(\bar{x}))$$

for all but an exponentially decreasing fraction of structures $\mathfrak{A}$, when the cardinality of $\mathfrak{A}$ tends to infinity.

4 A probabilistic analysis of $\#\Sigma_1$

Given that every function in $\#\Sigma_1$ has a FPTRAS, it is interesting to determine the expressive power of this class. We show that a probabilistic analysis, in the same style as developed in [5] for optimization problems, can be carried out also for $\#\Sigma_1$ and gives interesting non-expressibility results.

Definition 4.1 A second-order formula is *purely existential* if it has the form $\exists\bar{T}\,\exists\bar{y}\,\varphi$ where φ is quantifier-free.

Lemma 4.2 *Every purely existential second-order formula is equivalent to an existential first-order formula.*

We omit the proof which is an easy exercise.

As in the last section, let $\Omega(n)$ be a probability space of τ-structures with universe $\{0,\dots,n-1\}$. Every numerical invariant F on τ-structures can be considered as a random variable on each $\Omega(n)$; we denote its expectation by $E(F)$.

Theorem 4.3 (Probabilistic criterion for $\#\Sigma_1$) *For all $F \in \#\Sigma_1$ there exists a polynomial $p(n)$ such that*

(i) Suppose $F(\mathfrak{A})$ is not polynomially bounded in $|\mathfrak{A}|$. Then for structures $\mathfrak{A}$ such that $F(\mathfrak{A}) \neq 0$, $\log F(\mathfrak{A}) \sim p(|\mathfrak{A}|)$.[4]

(ii) Either F is identically 0 or $E(F) = \Theta(q(n)2^{p(n)})$ for some polynomial $q(n) \neq 0$.

Proof. Let $F \in \#\Sigma_1$ be defined by the expression

$$F(\mathfrak{A}) = |\{(\bar{T},\bar{c}) : \mathfrak{A} \models \exists\bar{y}\,\varphi(\bar{T},\bar{c},\bar{y})\}|$$

where φ is quantifier-free. For each structure $\mathfrak{A}$ and tuple of elements $\bar{c}$ from $\mathfrak{A}$, let

$$H_{\bar{c}}(\mathfrak{A}) = |\{\bar{T} : \mathfrak{A} \models \exists\bar{y}\,\varphi(\bar{T},\bar{c},\bar{y})\}|.$$

Thus, $F(\bar{A}) = \sum_{\bar{c}} H_{\bar{c}}(\mathfrak{A})$. Let $p(n) = p_\sigma(n)$. Recall that there are $2^{p(n)}$ possible interpretations of $\bar{T}$ on $\mathfrak{A}$ when $|\mathfrak{A}| = n$. Suppose that $H_{\bar{c}}(\mathfrak{A}) \neq 0$. Let k be the number of occurrences of $\bar{T}$-atoms in

[4] Here, $f \sim g$ means that $f(\mathfrak{A})/g(\mathfrak{A})$ tends to 1 as the cardinality of $\mathfrak{A}$ goes to infinity.

φ. If we fix an interpretation $\bar{T}$ and witnesses $\bar{y}$ such that $\mathfrak{A} \models \varphi(\bar{T}, \bar{c}, \bar{y})$ then we can change the truth-value of any $\bar{T}$-atom not occurring in $\varphi(\bar{T}, \bar{c}, \bar{y})$ and the formula will still hold in $\mathfrak{A}$. Thus it follows that for all $\bar{c}$, if $H_{\bar{c}}(\mathfrak{A}) \neq 0$, then $H_{\bar{c}}(\mathfrak{A}) \geq 2^{-k} 2^{p(n)}$. Let $S(\mathfrak{A})$ be the number of tuples $\bar{c}$ for which $H_{\bar{c}}(\mathfrak{A}) \neq 0$. Then,

$$S(\mathfrak{A}) 2^{p(n)} \geq F(\mathfrak{A}) \geq S(\mathfrak{A}) 2^{-k} 2^{p(n)}.$$

For $F(\mathfrak{A}) \neq 0$, we have $n^r 2^{p(n)} \geq F(\mathfrak{A}) \geq 2^{-k} 2^{p(n)}$. Since F is not polynomially bounded, $\bar{T}$ cannot be the empty sequence, i.e., $p(n) \neq 0$. By taking logarithms, claim (i) follows.

To prove the second claim we estimate the random variable S on $\Omega(n)$. We write S as the sum $\sum_{\bar{c}} S_{\bar{c}}$ of the indicator random variables

$$S_{\bar{c}}(\mathfrak{A}) = \begin{cases} 1 & \text{if } \mathfrak{A} \models \exists \bar{T}\, \exists \bar{y}\, \psi(\bar{T}, \bar{c}, \bar{y}) \\ 0 & \text{otherwise.} \end{cases}$$

The formula $\exists \bar{T}\, \exists \bar{y}\, \psi(\bar{T}, \bar{c}, \bar{y})$ is purely existential and therefore equivalent to a Σ_1-formula. By Theorem 3.3(i), $E(S_{\bar{c}})$ converges exponentially to some dyadic rational q_e determined by the equality type e of $\bar{c}$. Let $S_e = \sum_{\bar{c} \in e} S_{\bar{c}}$. If $q_e \neq 0$ then $E(S_e)$ is exponentially close to $q_e G_e(n)$, where $G_e(n)$ is the polynomial described by Lemma 2.6. If $q_e = 0$ then, by Theorem 3.3(ii), S_e is identically 0. Therefore, if $q_e = 0$ for all equality types e, then S, and hence also F is identically 0. Otherwise, we infer by linearity of expectation that $E(S) = \sum_e E(S_e)$ which converges exponentially fast to the polynomial $q(n) := \sum_e q_e G_e(n)$. Thus, there exist constants c, d such that

$$c q(n) 2^{p(n)} \geq E(F) \geq d q(n) 2^{p(n)}.$$

If F is defined without constant parameters, i.e., by an expression $F(\mathfrak{A}) = |\{\bar{T} : \mathfrak{A} \models \exists \bar{y}\, \varphi(\bar{T}, \bar{y})\}|$, counting only predicates, then an obvious modification of the argument shows that either $F = 0$ or $E(F) = \Theta(2^{p(n)})$. ∎

Applications. We use the probabilistic criterion to show that certain functions do not belong to $\#\Sigma_1$.

- The function #dist2 assigns to a graph the number of pairs of nodes with distance two. This function, mentioned in [32], obviously is in $\#\Sigma_1$. The related function #dist>2, counting the pairs of distance at least three, is easily seen to be in $\#\Pi_1$. Our criterion shows that #dist>2 $\notin \#\Sigma_1$, because #dist>2 is not identically 0, yet it is known that $E(\#\text{dist}{>}2)$ converges exponentially to 0 (almost all graphs have diameter two).

- Let $\#\text{cl}(G)$ denote the number of cliques in G. Obviously, $\#\text{cl} \in \#\Pi_1$. Since the expected number of k-cliques in a random graph with n vertices is $\binom{n}{k} 2^{-\binom{k}{2}}$ it follows that almost surely $p(n) = o(\#\text{cl})$ for every polynomial p. On the other hand, the maximal clique has almost surely no more than $2 \log n$ nodes [7], so $\#\text{cl} = o(2^n)$ almost surely. It follows that $\#\text{cl} \notin \#\Sigma_1$.

- A similar argument shows that the number of vertex covers is in $\#\Pi_1 - \#\Sigma_1$.

- By using Theorem 4.3*(i)* we can also obtain nonexpressibility results on classes of graphs with a finite number of built-in relations such as, e.g., order. We illustrate the method for #cl. Fix any function $f(n)$ with $\log n = o(f(n))$ and $f(n) = o(n)$ and let G_n be the graph consisting of an $f(n)$-clique and $n - f(n)$ isolated nodes. The number of cliques in G_n is

$$\#\mathrm{cl} = n + 2^{f(n)} - f(n) - 1$$

namely the number of nodes (1-cliques) plus the number of subsets of cardinality at least two of the $f(n)$-clique. Thus, $\#\mathrm{cl}(G_n)$ is not polynomially bounded, but $\log(\#\mathrm{cl}(G_n)) = o(n)$.

Notice that this argument still holds if the vocabulary is expanded. It follows that $\#\mathrm{cl}$ is not in $\#\Sigma_1$ even on classes of graphs with built-in relations. In particular this holds for the class of all ordered graphs.

4.1 Closure under infinitary reductions

Here is another simple application of the probabilistic criterion: The expected number of Hamilton cycles in a random graph with n vertices is $(n-1)!\,2^{-n}$, so $\#\mathrm{ham} \notin \#\Sigma_1$. However, a better result than this is known. Simple monotonicity arguments show that $\#\mathrm{ham} \in \#\Pi_2 - \#\Sigma_2$ [32]. However, our argument can be expanded to give a stronger result for which the previously used techniques do not seem to suffice. Instead of $\#\Sigma_1$ we consider its closure under logical reductions.

Definition 4.4 Let L and K be classes of logical formulae. A formula ψ over a vocabulary τ (possibly with additional parameters $\bar{T}, \bar{c}$) is in L^K if it can be obtained from a formula $\varphi \in L$ over the vocabulary $\tau \cup \{P_1, \dots, P_k\}$ and formulae $\alpha_1(\bar{z}_1), \dots, \alpha_k(\bar{z}_k) \in K$ over the vocabulary τ (without additional parameters!) by substituting $\alpha_i(\bar{x})$ for all occurrences of atoms $P_i(\bar{x})$ in φ, i.e.,

$$\psi(\bar{T}, \bar{c}) = \varphi(\bar{T}, \bar{c}, \alpha_1/P_1, \dots, \alpha_k/P_k).$$

Theorem 4.5 (Extended probabilistic criterion) *Let $K \subseteq L^{\omega}_{\infty\omega}$. Then, for all $F \in \#\Sigma_1^K$ there exists a polynomial $p(n)$ such that either $E(F)$ converges to 0 exponentially fast, or $E(F) = \Theta(q(n)2^{p(n)})$ for some polynomial $q(n) \neq 0$.*

Proof. By Theorem 3.4 we have that for every formula $\alpha(\bar{x}) \in L^{\omega}_{\infty\omega}$ there exists a quantifier-free first-order formula $\beta(\bar{x})$ such that $\mathfrak{A} \models \forall \bar{x}\,(\alpha \leftrightarrow \beta)$ for all but an exponentially decreasing fraction of structures $\mathfrak{A}$. So probabilistically, the predicates from K can be eliminated, i.e., every formula in Σ_1^K is equivalent to a formula from Σ_1 almost surely. ■

In particular, the extended criterion applies to $\#\Sigma_1^{\mathrm{FP}}$ since fixed point logic is contained in $L^{\omega}_{\infty\omega}$. As a consequence $\#\mathrm{ham}$ is not even in $\#\Sigma_1^{\mathrm{FP}}$. The same applies to the number of cliques and the number of vertex covers.

Remark. We note that it is important that we closed $\#\Sigma_1$ under *logical* reductions, and not under reduction defined by resource bounded Turing machines (such as, e.g., any kind of polynomial-time reductions), since the latter do not preserve asymptotic probabilities.

5 The power of logical counting classes

We now investigate the power of $\#\mathrm{FO}$ and classes $\#L$ for logics L that extend FO. We first consider functions definable by existential second-order logic Σ^1_1, and relate it to the class spanP.

Theorem 5.1 *On ordered finite structures,*

$$\mathrm{spanP} = \#\Sigma_1^1 = \#\Sigma_1^1(\Pi_2).$$

Here, $\Sigma_1^1(\Pi_2)$ means the class of all Σ_1^1-formulae whose first-order part is in Π_2. The proof is a straightforward modification of the proof of Fagin's theorem [12]. It is known that $\#\mathrm{P} = \mathrm{spanP}$ if and only if $\mathrm{UP} = \mathrm{NP}$. Thus, we cannot separate $\#\mathrm{FO}$ from $\#\Sigma_1^1$ on ordered structures, short of proving that $\mathrm{P} \neq \mathrm{NP}$. The matter is different on arbitrary finite structures, where model-theoretic methods suffice to separate the two classes.

Theorem 5.2 *On arbitrary finite structures,*

$$\#\mathrm{FO} \subsetneq \#\Sigma_1^1.$$

PROOF. The characteristic function $\chi_{\mathcal{C}}$ of any set of finite structures $\mathcal{C} \in \mathrm{NP}$ is in $\#\Sigma_1^1$. Indeed, by Fagin's Theorem there exists a formula $\psi \in \Sigma_1^1$ such that $\mathcal{C} = \{\mathfrak{A} : \mathfrak{A} \models \psi\}$. Choose a monadic predicate variable T not occurring in ψ. Then

$$\chi_{\mathcal{C}}(\mathfrak{A}) = |\{T : \mathfrak{A} \models \psi \wedge \forall x\, Tx\}|.$$

On the other hand, let $\mathcal{C} =$ EVEN, i.e., the set of finite structures over the empty vocabulary with universes of even cardinality. Assume, towards a contradiction, that

$$\chi_{\mathcal{C}}(\mathfrak{A}) = |\{T : \mathfrak{A} \models \varphi(T)\}|$$

where $\varphi(T)$ is first-order. This means that on every structure $\mathfrak{A}$ of even cardinality there exists precisely one T such that $\mathfrak{A} \models \varphi(T)$. On such a structure, every permutation π of the universe is an automorphism, so $\mathfrak{A} \models \varphi(\pi T)$ as well (where $\pi T = \{\bar{x} : \pi\bar{x} \in T\}$). Thus T must be fixed by all permutations of the universe. The only predicates that have this property are unions of equality types (because the group of all permutations operates transitively on each equality type). Since the number of equality types is bounded by a constant, so is the number of unions of these equality types, and moreover, each such union u is definable by a quantifier-free formula $\alpha_u(x_1, \ldots, x_k)$. We then construct, for each u, the formula $\varphi(\alpha_u/T)$ by replacing all occurrences of atoms $T(\bar{z})$ in φ by $\alpha_u(\bar{z})$.

It follows that the formula $\exists T \varphi(T)$, whose models—according to our assumptions—are precisely the structures of even cardinality, is equivalent to the first-order formula $\bigvee_u \varphi(\alpha_u/T)$. But this contradicts the well-known fact that EVEN is not first-order expressible. ■

Corollary 5.3 *On arbitrary finite structures,*

$$\#\mathrm{FO} \subsetneq \#\mathrm{P}.$$

Theorem 5.2 is not limited to first-order logic, but applies to any logic L which does not express EVEN. In particular this is the case for every logic that admits a 0-1 law.

Corollary 5.4 *On arbitrary finite structures*

$$\#\Sigma_1^1 - \#L^\omega_{\infty\omega} \neq \emptyset.$$

On unordered finite structures, least fixed point logic FP is intermediate between first-order and existential second-order logic: FO $\subsetneq$ FP $\subsetneq \Sigma^1_1$. However, for defining counting functions, FP is no more powerful than first-order logic.

Theorem 5.5 *#FP = #FO.*

PROOF. This is a consequence of the fact that every FP-definable query is *implicitly* definable in first-order logic [25]. In particular, this implies the following: Let $F \in$ #FP be defined by the expression

$$F(\mathfrak{A}) = |\{(\bar{P}, \bar{c}) : \mathfrak{A} \models \psi(\bar{P}, \bar{c})\}|$$

where $\psi(\bar{P}, \bar{c}) \in$ FP. Then there exists a first-order formula $\varphi(\bar{Q}, \bar{P}, \bar{c})$ with a new sequence $\bar{Q} = Q_0, \ldots, Q_r$ of predicate variables, such that for all expansions $(\mathfrak{A}, \bar{P}, \bar{c})$ of $\mathfrak{A}$, there is precisely one sequence of relations $\bar{Q}$ with

$$\mathfrak{A} \models \varphi(\bar{Q}, \bar{P}, \bar{c})$$

and moreover, for that sequence $\bar{Q}$, it holds that

$$\mathfrak{A} \models \psi(P, \bar{c}) \text{ iff } \mathfrak{A} \models \forall x Q_0 x.$$

It follows that for all $\mathfrak{A}$,

$$F(\mathfrak{A}) = |\{(\bar{Q}, \bar{P}, \bar{c}) : \mathfrak{A} \models \varphi(\bar{Q}, \bar{P}, \bar{c}) \wedge \forall x Q_0 x\}|.$$

∎

Does FO collapse to $\#\Pi_2$ unordered structures? The proof given in [32] for the ordered case does not extend to the unordered case, since it depends on encodings of Turing machine computations. A straightforward use of Skolem functions also does not work because Skolem functions are not unique. However, a more sophisticated application of a Skolem function argument (taking at each step the union of the graphs of all applicable Skolem functions) shows that every function in #FO is indeed definable in $\#\Pi_2$. To summarize, we can complement Theorem 1.1 by

Theorem 5.6 *On arbitrary finite structures,*

$$\#\Sigma_0 \subsetneq \#\Sigma_1 \subsetneq \#\Pi_1 \subsetneq \#\Sigma_2 \subsetneq \#\Pi_2 = \#\mathrm{FO} \subsetneq \#\mathrm{P}.$$

Next we discuss the problem of whether $\#\Sigma^1_1$ captures spanP on unordered structures. The analogy to NP suggests that this might be the case, since in Σ^1_1 an ordering can be introduced by existential quantification. But the straightforward extension of the proof of Theorem 5.1 does not work, since different linear orderings of the input structure will in general produce different encodings of the output.

In fact it turns out that $\#\Sigma^1_1$ does not capture spanP on unordered structures. Even worse, we will prove that some very simple functions are not definable even by the most sophisticated logics. We need some facts on group actions of the symmetric group.

Recall that a *group action* of a group $(G, \cdot)$ on a set S is an operation $\circ : G \times S \to S$ (usually written in infix notation) such that for all $g, h \in G$ and $a \in S$, $g \circ (h \circ a) = (g \cdot h) \circ a$, and for the identity element *id* of G, $id \circ a = a$. We will write ga rather than $g \circ a$ whenever the action can be inferred from context. If G is a subgoup of S_n (the symmetric group on $\mathbf{n} = \{0, 1, \ldots, n-1\}$), there is a natural group action of G on n. A group action is *k-transitive* if whenever $a_1, \ldots, a_k$ is a sequence of distinct elements in S and similarly for $b_1, \ldots, b_k$, there is a $g \in G$ such that $ga_i = b_i$ for $i = 1, \ldots, k$.

Lemma 5.7 *If $k \leq n$ then the natural group action of S_n on $\mathbf{n}$ is k-transitive. If $k+2 \leq n$ then the natural group action of A_n (the alternating subgroup of S_n) is k-transitive.*

PROOF. Let $a_1, \ldots, a_k$ be a sequence of distinct elements of n, and similarly for $b_1, \ldots, b_k$. Extend both these sequences to complete listings $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ of all the elements of $\mathbf{n}$. The mapping g taking each a_i to b_i is an element of S_n satisfying the condition in the definition of k-transitivity. If $k+2 \leq n$, form h in the same way as g but with b_{n-1} and b_n interchanged in the second sequence. Then either g or h is an element of A_n satisfying the condition in the definition of k-transitivity. ■

Let e be the equality type of k pairwise unequal variables and $\mathbf{n}$ be the structure with universe n over the empty vocabulary . Then the natural group action of S_n on $e^{\mathbf{n}}$ takes the pair consisting of g and $(a_1, \ldots, a_k)$ to $(ga_1, \ldots, ga_k)$. We define by extension the natural group action of S_n on the power set of $e^{\mathbf{n}}$. By the previous lemma and a little elementary group theory we have the following proposition.

Proposition 5.8 *Suppose e is the equality type of k pairwise unequal variables and $n \geq \max(5, k+2)$. For each nonempty, proper subset T of $e^{\mathbf{n}}$, $S_n(T) = \{gT : g \in S_n\}$ (the* orbit *of T) contains at least n elements.*

PROOF. Let m be the number of elements in $S_n(T)$. Thus, $S_n(T)$ consists of elements $h_1T, \ldots, h_mT$ where $h_1 = id$ and $h_2, \ldots, h_m \in S_n - \{id\}$. Now every $g \in S_n$ is associated with a permutation $\hat{g}$ of $S_n(T) = S_m$ where $\hat{g}(h_iT) = (gh_i)T$. The mapping taking g to $\hat{g}$ is a group homomorphism from S_n to S_m. The kernel of this homomorphism is a normal subgroup of S_n. Since $n \geq 5$ there are only three normal subgroups of S_n; they are S_n, A_n, and $\{id\}$. The kernel cannot be S_n because for every g in the kernel, $\hat{g}$ is the identity and in particular $gT = \hat{g}(h_1T) = T$, but from the previous lemma, if $a = (a_1, \ldots, a_k) \in T$ and $b = (b_1, \ldots, b_k) \notin T$, there is a $g \in S_n$ such that $ga = b$, hence g is not in the kernel. Similarly, the kernel cannot be A_n. Therefore, the kernel is $\{id\}$ and the homomorphism is an embedding of S_n into S_m. This gives the desired result that $m \geq n$. ■

Theorem 5.9 *There exist polynomial-time computable functions which are not in $\#L$ for* any *logic L.*

PROOF. The only property of L that we use is that L does not distinguish between isomorphic structures. As in the proof of Theorem 5.2, we consider functions on structures over the empty vocabulary. That is, we restrict to structures of the form $\mathbf{n} = \{0, \ldots, n-1\}$. Suppose that $F \in \#L$. By definition,

$$F(\mathbf{n}) = |\{(\bar{T}, \bar{c}) : \mathbf{n} \models \psi(\bar{T}, \bar{c})\}|$$

for some $\psi \in L$. If L is closed under $\wedge, \vee$ and first-order quantifications then we can replace constants and combine relations so that

$$F(\mathbf{n}) = |\{T : \mathbf{n} \models \psi(T)\}|$$

for some $\psi \in L$. There is no loss of generality in making this assumption since we can close L under these operations and then produce a polynomial time computable function not in the expanded $\#L$.

We show that if $F(\mathbf{n})$ is unbounded, then $F(\mathbf{n}) \geq n$ for all sufficiently large n. Let k be the arity of T. There are only a bounded number of equality types of k-tuples and therefore only a bounded number of unions of equality types of k-tuples. Since $F(n)$ is unbounded, for every sufficiently large n there is a T such that $\mathbf{n} \models \psi(T)$ and T is *not* a union of equality types. Thus, for such an $\mathbf{n}$ and T there exists an equality type e of k-tuples such that $T \cap e^{\mathbf{n}}$ is a nonempty, proper subset of $e^{\mathbf{n}}$.

We wish to show that the orbit of T under the group action of S_n is of size at least n. It suffices to show that the orbit of $T \cap e^{\mathbf{n}}$ is of size at least n. We may assume that e is the equality type of pariwise unequal variables (otherwise, eliminate redundant variables and reduce the arity of $T \cup e^{\mathbf{n}}$ accordingly). By the previous proposition, the orbit of $T \cap e^{\mathbf{n}}$ is of size at least n for sufficiently large n.

In particular, the function $G(\mathbf{n}) = n - 1$ is not in $\#L$ for any logic L. ■

The arguments in the proofs of Theorem 5.2 and Theorem 5.9 also yield the following technical lemma which we state here for future reference.

Lemma 5.10 *Let $L \supseteq$ FO be a logic that is closed under first-order operations and let $F \in \#L$ be a function on structures over the empty vocabulary. If F is bounded by a constant, then for every $k \in \mathbb{N}$, the set $\{\mathbf{n} : F(\mathbf{n}) = k\}$ is definable in L.*

PROOF. Let $F(\mathbf{n}) = |\{T : \mathbf{n} \models \psi(T)\}|$ for some $\psi \in L$. Since F is bounded, the arguments given above imply that for some n_0 and all $n \geq n_0$, every relation T with $\mathbf{n} \models \psi(T)$ is a union of equality types. The case where $n < n_0$ can be handled by a separate first-order formula, so we may asssume that n is indeed suffiently large. Let U be the set of unions of equality types of the appropriate arity and, for $u \in U$, let $\alpha_u(\bar{x})$ be a quantifier-free formula defining u. The condition that $F(\mathbf{n}) = k$ can be defined by a formula stating that there exist precisely k unions u of equality types that satisfy ψ. More formally,

$$F(\mathbf{n}) = k \iff \bigvee_{\substack{J \subseteq U \\ |J| = k}} \bigwedge_{u \in J} \psi(\alpha_u/T) \wedge \bigwedge_{u \in (U-J)} \neg\psi(\alpha_u/T).$$

Thus, the set $\{\mathbf{n} : F(\mathbf{n}) = k\}$ is definable in L. ■

Remark. We use the term *logic* here in the sense of model theory (see [4]). Our definition is very liberal: a logic L associates with each vocabulary τ a set $L(\tau)$ of sentences and a satisfaction relation $\models$ between τ-structures and sentences $\psi \in L(\tau)$. Depending on the context, some conditions may be imposed, e.g., that $L(\tau)$ be recursive. One condition always present, and the only one we use in the proof of Theorem 5.9, is the invariance of the satisfaction relation under isomorphisms, i.e., $\mathfrak{A} \models \psi$ and $\mathfrak{A} \cong \mathfrak{B}$ imply $\mathfrak{B} \models \psi$.

In descriptive complexity theory, it is often assumed that certain fixed relations, e.g., an ordering, are present. We do not consider such built-in relations as part of the logic (as, say, equality is), but as a means to restrict attention to a particular class of finite structures such as the class of ordered finite structures. Clearly non-expressibility for ordered structures implies non-expressibility for arbitrary structures, but not *vice versa*. For instance, in least fixed point logic FP, we cannot define EVEN, but on ordered structures, the order can be used to search through the structure and express not only EVEN, but all polynomial-time computable queries [21, 35].

Theorem 5.9 pertains to the class of arbitrary finite structures and does not hold for the class of ordered finite structures (where $\#\mathrm{FO} = \#\mathrm{P}$).

An interesting question arises concerning "logics with numbers" such as fixed point logic with counting (FP + C). This logic was originally proposed by Immerman. It is defined over two-sorted structures $\mathfrak{A}^* = \mathfrak{A} \cup (\mathbf{n}, \leq)$ where $\mathfrak{A}$, the first sort, is a τ-structure and $(\mathbf{n}, \leq)$, the second sort, is an ordered structure of the same cardinality. The connection between the two sorts is given by counting terms $\#_x[\varphi(x)]$ interpreted as the number of elements x satisfying φ. The logic (FP + C) is the closure of first-order logic over these two-sorted structures under counting terms (or equivalently, counting quantifiers) and under the rule for defining inflationary fixed points (over both sorts). Although this logic fails to capture polynomial-time [9], it is interesting and provides a natural level of expressiveness between FP and polynomial time, with many equivalent characterizations [17]. (FP + C) is a logic in our sense: for every vocabulary τ we have a set of sentences $\psi \in (\mathrm{FP} + \mathrm{C})(\tau)$; given a τ-structure $\mathfrak{A}$ we determine whether $\mathfrak{A} \models \psi$ by interpreting ψ in the two-sorted extension $\mathfrak{A}^*$ in the obvious way.

Thus, Definition 2.2 gives a class $\#(\mathrm{FP} + \mathrm{C})$ of counting functions, namely the class of functions

$$F(\mathfrak{A}) = |\{(\bar{P}, \bar{c}) : (\mathfrak{A}, \bar{P}, \bar{c}) \models \psi\}|$$

where ψ is a sentence in (FP + C) over the vocabulary $\tau \cup \{\bar{P}, \bar{c}\}$. Note that $\bar{P}$ and $\bar{c}$ range over $\mathfrak{A}$, not over $\mathfrak{A}^*$.

Clearly, $\#(\mathrm{FP} + \mathrm{C})$ is more powerful than $\#\mathrm{FP} = \#\mathrm{FO}$ since it contains (the characteristic function of) EVEN. On the other hand, Theorem 5.9 tells us that $\#(\mathrm{FP} + \mathrm{C})$ fails to define some simple functions, such as $n - 1$.

Question. What is the power of $\#(\mathrm{FP} + \mathrm{C})$?

We could consider a variant of $\#(\mathrm{FP} + \mathrm{C})$, deviating from Definition 2.2 by allowing the counting of objects ranging over both sorts. The proof of Theorem 5.9 does not extend to this class. We can, for instance, define the function $n - 1$ by counting the elements in the second sort distinct from 0:

$$n - 1 = |\{i : \mathfrak{A}^* \models \exists j (j < i)\}|.$$

However, it should be noted, that in this case we again consider a restricted class of structures only. This extended definition for $\#(\mathrm{FP} + \mathrm{C})$ is also somewhat pathological, because the operator $\#$ is no longer monotone: while $(\mathrm{FP} + \mathrm{C}) \subseteq \Sigma^1_1$, we have $\#(\mathrm{FP} + \mathrm{C}) \not\subseteq \#\Sigma^1_1$. Nevertheless it is interesting to determine the power of this variant of $\#(\mathrm{FP} + \mathrm{C})$.

6 Capturing #P and spanP almost everywhere

Theorem 5.9 reveals a general weakness of classes $\#L$ on structures with many automorphisms. However, in a probabilistic sense, $\#\Sigma^1_1$ comes very close to capturing spanP, provided that the underlying vocabulary has at least one binary predicate. A similar result holds for #P and #FO. For simplicity of exposition we will reason about graphs, but our arguments apply *mutatis mutandis* to structures of any non-monadic relational vocabulary. As in the previous section, we consider *unordered* structures.

Theorem 6.1 *Let F be a graph invariant.*

(i) If $F \in \#\mathrm{P}$, then there exists a function $F' \in \#\mathrm{FO}$ such that $F = F'$ on almost all graphs.

(ii) If $F \in \mathrm{spanP}$, then there exists a function $F' \in \#\Sigma_1^1$ such that $F = F'$ on almost all graphs.

The proof of this theorem relies on fundamental results related to the graph isomorphism problem.

Definition 6.2 Let $\mathcal{G}$ be an class of graphs closed under isomorphism. A *canonical ordering* on $\mathcal{G}$ is a function mapping each $G = (V, E)$ in $\mathcal{G}$ to a linear order $\leq_G$ on V such that any isomorphism between graphs G and G' in $\mathcal{G}$ is also an isomorphism between the ordered graphs $(G, \leq_G)$ and $(G', \leq_{G'})$.

Not every class of graphs has a canonical ordering. A necessary and sufficient condition for $\mathcal{G}$ to have a canonical ordering is that every graph in $\mathcal{G}$ be rigid (i.e., have just one automorphism, the trivial automorphism). Finding a canonical ordering on a class $\mathcal{G}$ of rigid graphs is at least as difficult as the graph isomorphism problem on $\mathcal{G}$. Nonetheless, Babai, Erdős and Selkow [2] showed the following.

Theorem 6.3 *There is a class $\mathcal{G}$ of graphs for which the following conditions hold.*

(i) Almost every graph belongs to $\mathcal{G}$.

(ii) $\mathcal{G}$ has a polynomial-time computable canonical ordering.

Although the proof of this takes a considerable amount of calculation, the ordering is simple to describe. Consider a random graph $G = (V, E)$ on n vertices. Order V by degree in descending order. Let H be the first $\lceil 3 \log n \rceil$ vertices in this order. Almost surely the two following conditions hold.

1. The degrees of vertices in H are distinct and strictly greater than the degrees of vertices in $V - H$.

2. Each of the vertices in $V - H$ is connected to the vertices of H in a unique way.

Let $\mathcal{G}$ be the set of graphs G satisfying these two conditions. The canonical ordering $\leq_G$ is given by listing elements of H by descending degree and then the listing elements of $V - H$ lexicographically according to their connections to H. Clearly $\leq_G$ can be computed in polynomial time on $\mathcal{G}$.

Proof of Theorem 6.1. Let $\mathcal{G}$ and $\leq_G$ be as in the preceding theorem. There is a deterministic polynomial-time Turing machine M which, given the encoding of a pair $(G, \leq)$ where $G \in \mathcal{G}$, decides whether $\leq$ is the canonical ordering $\leq_G$. Thus, there is a first-order formula ϑ over the vocabulary $\{E, \leq, S\}$ such that for graphs $G \in \mathcal{G}$

$$(G, \leq, S) \models \vartheta \text{ iff}$$

(i) S encodes the (unique) computation of M on $\mathrm{code}(G, \leq)$;

(ii) M accepts $\mathrm{code}(G, \leq)$.

Whenever $G \in \mathcal{G}$ there are unique relations $\leq$ and S such that $G \models \vartheta(\leq, S)$; these relations are $\leq_G$ and the relation S encoding the computation of M on code$(G, \leq_G)$. Let F be a graph invariant in #P (respectively, spanP) defined by a NPTM machine. By Theorem 1.1 (respectively, Theorem 5.1), there is a first-order (respectively, existential second-order) formula $\psi(E, \leq, \bar{T}, \bar{c})$ such that for any fixed linear order $\leq$, $F(G) = |\{(\bar{T}, \bar{c}) : G \models \psi(E, \leq, \bar{T}, \bar{c})\}|$. Then for all $G \in \mathcal{G}$,

$$F(G) = |\{(\leq, S, \bar{T}, \bar{c}) : G \models \psi(E, \leq, \bar{T}, \bar{c}) \wedge \vartheta(\leq, S)\}|.$$

■

7 Closure Properties

In the last few years there has been a considerable effort to investigate closure properties of function classes like #P and spanP. For instance, it has been shown that these classes are closed under (a general form of) addition and multiplication, as well as under (a restricted form of) exponentiation and binomial coefficients. On the other hand it has also been proved that these classes are *not* closed under other operations, like subtraction, division and numerous others, *unless certain generally believed assumptions in complexity theory fail.* In this section we investigate the status of these closure properties for logically defined counting classes $\#L$.

In many cases, the most general form in which closure properties (e.g., for #P) have been established, involves the function class UPF.

Definition 7.1 A function G belongs to UPF if there exists a nondeterministic polynomial-time Turing machine which on every input x has precisely one accepting computation path and $G(x)$ is the output produced by that path.

Lemma 7.2 *Let $f \in$ UPF be a function into $\mathbb{N}$. Then $f \in$ #P.*

Although the definition of UPF makes sense for arbitrary functions, we will need to consider only UPF-functions into the natural numbers whose values $G(x)$ are bounded by a polynomial in $|x|$. The following theorem summarizes most known closure properties for #P, as they appear in [6]. By default, F and G are functions mapping words over some alphabet Γ to natural numbers.

Theorem 7.3 *Let $F, F' \in$ #P and G be a polynomially bounded function in* UPF*. Then the following functions belong to* #P*:*

- *(i)* **Addition:** $F + F'$.
- *(ii)* **Multiplication:** FF'.
- *(iii)* **Generalized addition:** $\sum_{|y|=|x|^k} F(x, y)$.
- *(iv)* **Generalized multiplication:** $\prod_{i<|x|^k} F(x, i)$. [5]
- *(v)* **Powers:** F^G.

[5] Note that we here have a function $F : \Gamma^* \times \mathbb{N} \to \mathbb{N}$.

(vi) **Binomial coefficients:** $\binom{F}{G}$.

(vii) **Exponentiation:** 2^F *and* $2^F - 1$*, provided* $F(x)$ *is bounded by a polynomial in* $|x|$.

We want to define analogous closure properties for classes $\#L$. By this we mean that the closure properties should make sense for any L and any class of structures, but that for the special case where we have only ordered structures, the logical closure property for #FO is the same as the corresponding one for #P.

We start with a simple observation:

Proposition 7.4 *For every logic* L *closed under positive first-order operations, the class* $\#L$ *is closed under addition and multiplication.*

PROOF. Let $F, G \in \#L$ be defined by the formulae $\psi_F(T)$ and $\psi_G(S)$ in the sense that $f(\mathfrak{A}) = |\{T : \mathfrak{A} \models \psi_F(T)\}|$, and similarly for G. Without loss of generality we assume that S and T are distinct relation symbols of the same arity. Then

$$\begin{aligned}(F+G)(\mathfrak{A}) &= |\{(T,R) : \mathfrak{A} \models (\forall x\, Rx \wedge \psi_F(T)) \vee (\forall x \neg Rx \wedge \psi_G(T))\}| \\ (FG)(\mathfrak{A}) &= |\{(T,S) : \mathfrak{A} \models \psi_F(T) \wedge \psi_G(S)\}|.\end{aligned}$$

∎

Proposition 7.5 (Closure under generalized addition.) *Let* F *be a function in* $\#L$ *over the vocabulary* $\tau \cup \{T\}$ *(where* T *is a* k*-ary predicate symbol). Then the function* $G(\mathfrak{A}) = \sum_{\mathfrak{B}=(\mathfrak{A},T)} F(\mathfrak{B})$ *also belongs to* $\#L$.

PROOF. Let F be defined by the expression

$$F(\mathfrak{B}) = |\{(\bar{S}, \bar{c}) : \mathfrak{B} \models \psi(\bar{S}, \bar{c})\}|.$$

Here ψ is a formula over $\tau \cup \{T\}$ with parameters $\bar{S}$ and $\bar{c}$. But ψ can also be considered as a formula over the vocabulary τ with parameters $T, \bar{S}, \bar{c}$ defining the function

$$G(\mathfrak{A}) = |\{(T, \bar{S}, \bar{c}) : \mathfrak{A} \models \psi(T, \bar{S}, \bar{c})\}|.$$

∎

In the sequel, we assume that L contains FO and is closed under positive first-order operations.

Proposition 7.6 (Closure under generalized multiplication.) *Let* F *be a function in* $\#L$ *over the vocabulary* $\tau \cup \{\bar{a}\}$ *(where* $\bar{a} = a_1, \ldots, a_k$*). Then the function* $G(\mathfrak{A}) = \prod_{\mathfrak{B}=(\mathfrak{A},\bar{a})} F(\mathfrak{B})$ *also belongs to* $\#L$.

PROOF. Let F be defined by the expression

$$F(\mathfrak{B}) = |\{T : \mathfrak{B} \models \psi(T)\}|$$

where ψ is a formula over $\tau \cup \{\bar{a}\}$ with parameter T. Let S be a new relation symbol with $\mathrm{arity}(S) = k + \mathrm{arity}(T)$. Given a structure $\mathfrak{A}$ and instances S and $\bar{a}$ we define $S_{\bar{a}} = \{\bar{b} : (\bar{a}, \bar{b}) \in S\}$;

moreover we denote by $\psi(S_{\bar{a}}/T)$ the formula obtained from ψ by replacing every occurrence of $T(\bar{z})$ by $S(\bar{a}, \bar{z})$. We consider $\forall \bar{a}\, \psi(S_{\bar{a}}/T)$ as a formula over τ with parameters S and define

$$G(\mathfrak{A}) = |\{S : \mathfrak{A} \models \forall \bar{a}\, \psi(S_{\bar{a}})\}| = \sum_{\mathfrak{B}=(\mathfrak{A},T)} F(\mathfrak{B}).$$

Since $S = \bigcup_{\bar{a}} \{\bar{a}\} \times S_{\bar{a}}$ it follows that the number of appropriate predicates S is the product over all $\bar{a}$ of the number of $S_{\bar{a}}$ satisfying ψ; therefore,

$$G(\mathfrak{A}) = \prod_{\mathfrak{B}=(\mathfrak{A},\bar{a})} F(\mathfrak{B}).$$

■

The idea of this proof is useful to establish other closure properties as well. To define them we need a model-theoretic analogue to the class UPF. There is a related notion in model theory (which was studied long before the advent of complexity theory): implicit definition.

Definition 7.7 A formula $\psi(T_0, \ldots, T_m)$ over the vocabulary $\tau \cup \{T_0, \ldots, T_m\}$ is an *implicit definition* of a query Q on a class $\mathcal{C}$ of τ-structures if for all structures $\mathfrak{A} \in \mathcal{C}$

- there exists a unique tuple $T_0, \ldots, T_m$ such that $\mathfrak{A} \models \psi(T_0, \ldots, T_m)$;
- if $\mathfrak{A} \models \psi(T_0, \ldots, T_m)$ then $Q(\mathfrak{A}) = T_0$. [6]

A well-known result in classical model theory is Beth's Definability Theorem (see e.g., [19, p. 301]) stating that every query on the class of all (finite and infinite) τ-structures implicitly definable in first-order logic is also explicitly first-order definable, i.e., definable by a formula $\varphi(\bar{x})$ such that $Q(\mathfrak{A}) = \{\bar{a} : \mathfrak{A} \models \varphi(\bar{a})\}$ for every $\mathfrak{A} \in \mathcal{C}$. There also has been considerable effort in model theory to investigate the status of analogues to Beth's Theorem for more powerful logics than FO (see [4]). For first-order logic, Beth's result mostly serves as an excuse to disregard implicit definitions, since they don't give additional expressiveness. However, on finite structures, Beth's Theorem fails, and implicit definitions provide more expressive power than explicit ones. In fact, implicit definability is closely related to complexity classes like UP and in particular to the existence of one-way functions, as has been shown by Kolaitis [25] and Grädel [16]. Also, we have used in the proof of Theorem 5.5 the fact that every query definable in least fixed point logic is implicitly first-order definable.

Here rather than implicit definitions of queries, we need implicit definitions of polynomially bounded functions. Accordingly, we introduce a new class.

Definition 7.8 The class of *polynomially bounded, implicitly L-definable functions into* $\mathbb{N}$, denoted $\mathrm{pbi}(L)$, is the class of functions G which assigns to a structure $\mathfrak{A}$ the cardinality of an implicitly L-definable query on $\mathfrak{A}$. This means that there is an implicit definition $\psi(T_0, \ldots, T_m)$ such that $G(\mathfrak{A}) = |T_0|$ for the unique tuple $\bar{T}$ with $\mathfrak{A} \models \psi(\bar{T})$.

Proposition 7.9 *Let $\mathcal{C}$ be a class of ordered structures.*

(i) A query Q on $\mathcal{C}$ is in UPF *if and only if it is implicitly definable in first-order logic.*

[6] The classical notion of implicit definability is slightly different, with formulae containing only one new predicate symbol (i.e., $m = 0$). However, for finite model theory, the present definition turned out to more useful, cf. [25]).

(ii) A polynomially bounded function from $\mathcal{C}$ into $\mathbb{N}$ is in UPF *if and only if it is in* pbi(FO).

The proof is straightforward.

Proposition 7.10 (Closure under powers and binomial coefficients.) *Let $F \in \#L$ and $G \in \mathrm{pbi}(L)$. Then the functions F^G and $\binom{F}{G}$ are in $\#L$.*

Proof. Let $F(\mathfrak{A}) = |\{R : \mathfrak{A} \models \psi(R)\}|$ and $G(\mathfrak{A}) = |T_0|$ for the unique tuple $T_0, \ldots, T_m$ such that $\mathfrak{A} \models \varphi(\bar{T})$, where $\psi(R)$ and $\varphi(\bar{T})$ are formulae from L. Let S be a new predicate symbol with $\mathrm{arity}(S) = \mathrm{arity}(T_0) + \mathrm{arity}(R)$.

We define new functions H and J by the expressions

$$\begin{aligned} H(\mathfrak{A}) &= |\{(S, \bar{T}) : \mathfrak{A} \models \varphi(\bar{T}) \wedge \alpha(S, \bar{T})\}| \\ J(\mathfrak{A}) &= |\{(S, \bar{T}) : \mathfrak{A} \models \varphi(\bar{T}) \wedge \alpha(S, \bar{T}) \wedge \beta(S, \bar{T})\}| \end{aligned}$$

where

$$\begin{aligned} \alpha(S, \bar{T}) &= \forall \bar{x} \, (\neg T_0 \bar{x} \rightarrow \forall \bar{z} \, \neg S \bar{x} \bar{z}) \wedge \forall \bar{x} \, (T_0 \bar{x} \rightarrow \psi(S_{\bar{x}}/R)) \\ \beta(S, \bar{T}) &= \forall \bar{x} \, \forall \bar{y} \, ((\bar{x} \neq \bar{y} \wedge T_0 \bar{x} \wedge T_0 \bar{y}) \rightarrow S_{\bar{x}} \neq S_{\bar{y}}). \end{aligned}$$

Here $S_{\bar{x}}$ is defined in the same way as in the previous proof, and $S_{\bar{x}} \neq S_{\bar{y}}$ is shorthand for an appropriate first-order formula expressing this condition. Note that there is precisely one tuple $\bar{T}$ satisfying φ, so we just have to count the number of appropriate S. For $\bar{x} \notin T_0$, only $S_{\bar{x}} = \varnothing$ is appropriate. For $\bar{x} \in T_0$, the number of appropriate $S_{\bar{x}}$ is precisely $F(\mathfrak{A})$. In the defining expression for $J(\mathfrak{A})$ we have the additional condition that all $S_{\bar{x}}$ (for $\bar{x} \in T_0$) are distinct. Thus, it follows that $H = F^G$ and $J = \binom{F}{G}$. ∎

Proposition 7.11 (Closure under exponentiation.) *Let $F \in \#L$ be defined by an expression $F(\mathfrak{A}) = |\{\bar{a} : \mathfrak{A} \models \psi(\bar{a})\}|$ where $\psi \in L$. Then the functions 2^F and $2^F - 1$ are in $\#L$.*

Proof. The defining expressions are

$$\begin{aligned} 2^{F(\mathfrak{A})} &= |\{T : \mathfrak{A} \models \forall \bar{a} \, (T(\bar{a}) \rightarrow \psi(\bar{a}))\}| \\ 2^{F(\mathfrak{A})} - 1 &= |\{T : \mathfrak{A} \models \forall \bar{a} \, (T(\bar{a}) \rightarrow \psi(\bar{a})) \wedge \exists \bar{a} \, T(\bar{a})\}|. \end{aligned}$$

∎

We now turn to closure properties that probably do not hold for #P and spanP.

Definition 7.12 Let $\mathcal{F}$ be a class of functions into $\mathbb{N}$.

(i) $\mathcal{F}$ is *closed under span of k functions* if for all $f_1, \ldots, f_k \in \mathcal{F}$, the function

$$\mathrm{span}(f_1, \ldots, f_k)(x) := |\{f_i(x) : i = 1, \ldots, k\}|$$

is in $\mathcal{F}$.

(ii) For any tuple $\bar{a} = a_1, \ldots, a_k$ of natural numbers, let $\mathrm{plu}(\bar{a})$ be the set of elements that occur most often in $\bar{a}$, i.e., the set of all b such that for all $j \leq k$, $|\{i : a_i = a_j\}| \leq |\{i : a_i = b\}|$. The class $\mathcal{F}$ is *closed under weak plurality of k functions* if for all $f_1, \ldots, f_k$ there exists a $g \in \mathcal{F}$ such that $g(x) \in \mathrm{plu}(f_1(x), \ldots, f_k(x))$ for all x.

(iii) $\mathcal{F}$ is *closed under strong plurality of k functions* if for all $f_1, \ldots, f_k$ the function

$$\mathrm{plu}^*(f_1, \ldots, f_k)(x) := \min \mathrm{plu}(f_1(x), \ldots, f_k(x))$$

is in $\mathcal{F}$.

(iv) $\mathcal{F}$ is *closed under medians* if for every odd k and all $f_1, \ldots, f_k \in \mathcal{F}$, the function $\mathrm{med}(f_1, \ldots, f_k)$, which maps x to the median of $(f_1(x), \ldots, f_k(x))$ is in $\mathcal{F}$.

Ogiwara and Hemachandra [29] have proved that the polynomial-time hierarchy, and numerous other complexity classes, collapse to UP if and only if #P should be closed under any (and hence all) of the following operations: subtraction, division, span, weak plurality and strong plurality. A slightly less drastic collapse of complexity classes would occur, if #P should turn out to be closed under medians or under maxima and minima. We refer to [29] for more details.

These closure properties do not hold for #FO.

Proposition 7.13 #FO *is not closed under any of the operations subtraction, division, span, weak and strong plurality, minima and median.*

PROOF. Obviously the functions n and 1 belong to #FO, but the proof of Theorem 5.9 shows that $n - 1$ does not. For every $F \in$ #P, the function $n!F$ belongs to #FO. In particular, $n!$ (the number of linear orderings) belongs to #FO. Therefore, if #FO were closed under division, then #P $\subseteq$ #L, contradicting Theorem 5.9.

Let $\mathcal{C} = \{\mathbf{n} : n \text{ even}\}$. We know that the constant functions and the functions $n!\chi_{\mathcal{C}}$ and $n!\chi_{\bar{\mathcal{C}}}$ are in #FO (count the pairs $(<, T)$ such that $<$ is a linear order and T is the set of even elements with respect to $<$ such that T does not contains (resp. contains) the maximal element). Further, #FO is closed under addition.

Note that

$$\chi_{\mathcal{C}} = \min(n!\chi_{\mathcal{C}}, n!\chi_{\bar{\mathcal{C}}} + 1) = \mathrm{med}(0, 1, n!\chi_{\mathcal{C}}).$$

Since $\chi_{\mathcal{C}} \notin$ #FO, we infer that #FO is closed neither under minima nor medians. (Note that the same argument applies to any set of finite structures over the empty vocabulary such that $\mathcal{C} \in$ NP $\cap$ Co-NP, but $\chi_{\mathcal{C}} \notin$ #FO.)

Next, it follows by Lemma 5.10 that the function $1 + \chi_{\mathcal{C}}$ does not belong to #FO. Since $\mathrm{span}(0, n!\chi_{\mathcal{C}}) = 1 + \chi_{\mathcal{C}}$ it follows that #FO is not closed under span.

Finally, let the functions $f_1, \ldots, f_5$ be defined as follows: $f_i = in!\chi_{\bar{\mathcal{C}}}$ for $i = 1, 2$ and $f_i = in!\chi_{\mathcal{C}}$ for $i = 3, 4, 5$. Then the only function g such that $g(\mathbf{n}) \in \mathrm{plu}(f_1(\mathbf{n}), \ldots, f_5(\mathbf{n}))$ is $\chi_{\mathcal{C}}$. Therefore, #FO is not closed under weak and strong plurality.

∎

Note that this result does not depend on any unproved hypothesis from complexity theory.

References

[1] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, *Proof verification and intractability of approximation problems*, in Proc. 33rd IEEE Symp. on Foundations of Computer Science, Los Angeles, 1992, IEEE Computer Society Press, pp. 210–214.

[2] L. Babai, P. Erdös, and S. Selkow, *Random graph isomorphisms*, SIAM Journal on Computing, 9 (1980), pp. 628–635.

[3] J. Barwise, *On Moschovakis closure ordinals*, Journal of Symbolic Logic, 42 (1977), pp. 292–296.

[4] J. Barwise and S. Feferman, eds., *Model-Theoretic Logics*, Springer-Verlag, 1985.

[5] T. Behrendt, K. Compton, and E. Grädel, *Optimization problems: Expressibility, approximation properties, and expected asymptotic growth of optimal solutions*, in Computer Science Logic, 6th Workshop, CSL '92, San Miniato 1992, Selected Papers, E. Börger, G. Jäger, H. K. Büning, S. Martini, and M. Richter, eds., vol. 702 of LNCS, Springer-Verlag, 1993, pp. 43–60.

[6] R. Beigel, J. Gill, and U. Hertrampf, *Counting classes: Thresholds, parity, mods and fewness*, in Proc. 7th Annual Symp. on Theoretical Aspects of Computer Science STACS 90, no. 415 in Lecture Notes in Computer Science, New York, 1990, Springer-Verlag, pp. 49–57.

[7] B. Bollobas, *Random Graphs*, Academic Press, 1985.

[8] J. R. Büchi, *Weak second-order arithmetic and finite automata*, Z. Math. Logik Grundlagen Math., 6 (1960), pp. 66–92.

[9] J. Cai, M. Fürer, and N. Immerman, *An optimal lower bound on the number of variables for graph identification*, in Proc. 30th IEEE Symp. on Foundations of Computer Science, 1989, pp. 612–617.

[10] K. J. Compton, *0-1 laws in logic and combinatorics*, in NATO Adv. Study Inst. on Algorithms and Order, I. Rival, ed., D. Reidel, 1988, pp. 353–383.

[11] C. Elgot, *Decision problems of finite-automata design and related arithmetics*, Trans. Amer. Math. Soc., 98 (1961), pp. 21–51.

[12] R. Fagin, *Generalized first–order spectra and polynomial–time recognizable sets*, in Complexity of Computation, SIAM-AMS Proceedings, Vol. 7, R. M. Karp, ed., 1974, pp. 43–73.

[13] R. Fagin, *Probabilities on finite models*, Journal of Symbolic Logic, 41 (1976), pp. 50–58.

[14] H. Gaifman, *Concerning measures in first-order calculi*, Israel Journal of Mathematics, 2 (1964), pp. 1–18.

[15] Y. V. Glebskiĭ, D. I. Kogan, M. I. Liogon'kiĭ, and V. A. Talanov, *Range and degree of realizability of formulas in the restricted predicate calculus*, Cybernetics, 5 (1969), pp. 142–154.

[16] E. Grädel, *Definability on finite structures and the existence of one-way functions*, Methods of Logic in Computer Science, 1 (1994), pp. 299–314.

[17] E. Grädel and M. Otto, *Inductive definability with counting on finite structures*, in Computer Science Logic, 6th Workshop, CSL '92, San Miniato 1992, Selected Papers, E. Börger, G. Jäger, H. K. Büning, S. Martini, and M. Richter, eds., vol. 702 of LNCS, Springer-Verlag, 1993, pp. 231–247.

[18] Y. Gurevich, *Logic and the challenge of computer science*, in Current trends in theoretical computer science, E. Börger, ed., Computer Science Press, 1988, pp. 1–57.

[19] W. Hodges, *Model Theory*, Cambridge University Press, 1993.

[20] N. Immerman, *Upper and lower bounds for first-order expressibility*, Journal of Computer and System Sciences, 25 (1982), pp. 76–98.

[21] ——, *Relational queries computable in polynomial time*, Information and Control, 68 (1986), pp. 86–104.

[22] ——, *Languages that capture complexity classes*, SIAM Journal of Computing, 16 (1987), pp. 760–778.

[23] ——, *Descriptive and computational complexity*, in Computational Complexity Theory, Proc. Symp. Applied Math., Vol. 38, J. Hartmanis, ed., American Mathematical Society, 1989, pp. 75–91.

[24] J. Köbler, U. Schöning, and J. Toran, *On counting and approximation*, Acta Informatica, 26 (1989), pp. 363–379.

[25] P. Kolaitis, *Implicit definability on finite structures and unambiguous computations*, in Proc. 5th IEEE Symp. on Logic in Computer Science, 1990, pp. 168–180.

[26] P. Kolaitis and M. Thakur, *Logical definability of NP-optimization problems.* To appear in Information and Computation.

[27] ——, *Approximation properties of NP minimization classes*, in Proc. 6th IEEE Symp. on Structure in Complexity Theory, 1991, pp. 353–366.

[28] P. Kolaitis and M. Vardi, *Infinitary logics and 0–1 laws*, Information and Computation, 98 (1992), pp. 258–294.

[29] M. Ogiwara and L. Hemachandra, *A complexity theory for feasible closure properties*, in Proc. 6th IEEE Symp. on Structure in Complexity Theory, 1991, pp. 16–29.

[30] C. Papadimitriou and M. Yannakakis, *Optimization, approximization and complexity classes*, Journal of Computer and System Sciences, 43 (1991), pp. 425–440.

[31] B. Poizat, *Deux ou trois choses que je sais de L_n*, Journal of Symbolic Logic, 47 (1982), pp. 641–658.

[32] S. Saluja, K. V. Subrahmanyam, and M. Thakur, *Descriptive complexity of #p functions*, in Proc. 7th IEEE Symp. on Structure in Complexity Theory, 1992.

[33] B. A. Trakhtenbrot, *Finite automata and the logic of monadic predicates*, Doklady Akademii Nauk SSR, 140 (1961), pp. 326–329.

[34] L. Valiant, *The complexity of computing the permanent*, Theoretical Computer Science, 8 (1979), pp. 189–201.

[35] M. Y. Vardi, *The complexity of relational query languages*, in Proc. 14th ACM Symp. on Theory of Computing, 1982, pp. 137–146.