Non-Definability Results for Randomised First-Order Logic

Kord Eickmeyer

Humboldt-Universität zu Berlin
Under den Linden 6
10099 Berlin, Germany

Abstract

We investigate the expressive power of randomised first-order logic (BPFO) on restricted classes of structures. While BPFO is stronger than FO in general, even on structures with a built-in addition relation, we show that BPFO is not stronger than FO on structures with a unary vocabulary, nor on the class of equivalence relations. The same techniques can be applied to show that evenness of a linear order, and therefore graph connectivity, can not be defined in BPFO. Finally, we show that there is an FO[≤]-definable query on word structures which can not be defined in BPFO[+1].

1998 ACM Subject Classification F.4.1 Model theory; F.1.2 Probabilistic computation

Keywords and phrases Descriptive complexity, randomised logics, derandomisation

Digital Object Identifier 10.4230/LIPIcs.CSL.2011.218

1 Introduction

In [5], we introduced randomised logics as a tool for analysing randomised complexity classes using descriptive complexity theory. Randomised algorithms can be defined from deterministic ones by introducing a second input, namely a string of random bits whose length depends only on the length of the input and which is drawn uniformly at random from the set of all strings of that length. The outcome of such an algorithm $\mathbb{A}$ may then depend both on its input and on the particular choice of the random string, and for each fixed input x we get a certain acceptance probability, say $p_{\mathbb{A}}(x)$.

To define randomised complexity classes, one restricts attention to algorithms which have a probability gap, i.e., there is a certain interval $(\alpha, \beta] \subseteq [0, 1]$ such that $p_{\mathbb{A}}(x) \notin (\alpha, \beta]$ for all inputs x. Such an algorithm is said to accept its input if $p_{\mathbb{A}}(x) > \beta$. By parallel repetition and thresholding, this gap may be amplified, so that the definition of, say, randomised polynomial time or randomised logspace is very robust under the choice of the interval $(\alpha, \beta]$ (cf. [1]). However, if one does not demand any probability gap, the resulting complexity class PP becomes rather powerful, as witnessed by Toda's theorem [13] stating that P^{PP} contains the full polynomial hierarchy.

In [5], we defined randomised first-order logic BPFO in a similar manner by introducing additional relation symbols which are interpreted randomly. This way, we can define the satisfaction probability $\Pr(A \models \varphi)$ of a sentence φ in a structure A, and just like in the case of randomised algorithms we demand this to be outside of some interval $(\alpha, \beta]$ for all finite structures A. We then say that $A \models \varphi$ if this probability is $> \beta$ (see section 3 for details). Barrington et al.'s famous result that FO captures dlogtime-uniform AC^0 on structures with addition and multiplication easily carries over to the randomised world, i.e., one obtains a logic capturing dlogtime BPAC^0 on such structures. Similarly, randomised least fixed-point logic BPLFP captures BPP on ordered structures. Equipped with very

Computer Science Logic 2011 (CSL'11).
Editor: Marc Bezem; pp. 218–232

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

weak counting abilities, one also obtains a logic capturing BPP on all structures, albeit one with an undecidable syntax.

Previous research on the expressive power of logics on random structures mostly dealt with finite relational structures in which *all* relations were defined randomly. In some cases, the underlying universe was assumed to be ordered, but the ordering was not accessible to the logic. This holds true, for example, of the various 0-1-laws for first-order and infinitary logics [8, 6], which imply that derandomisation is possible on structures over the empty vocabulary. While these results have been generalised to probability distributions other than uniform (cf. [11]), hardly any work has been done on structures with random as well as non-random relations. Reasoning about partly random structures appears to require much more powerful tools, and the only previous work in this direction which we are aware of is by Shelah [10] and Boppana and Spencer [2], who prove what they call *smoothness laws* for ordered random structures, i.e., they only consider the case where the non-random part is a linear order. While there is no convergence law in this case, Boppana and Spencer prove that for every first-order sentence φ,

$$|\Pr(\mathcal{O}_n \models \varphi) - \Pr(\mathcal{O}_{n+1} \models \varphi)| = O\left(\frac{\log^d n}{n}\right),$$

where d is the quantifier depth of φ. We use essentially the same proof technique to show that BPFO can be derandomised on structures with a unary vocabulary and on equivalence classes; with the minor adjustment that we allow for arbitrary random relations instead of just random undirected graphs, their results imply theorem 8(a). Our application of that technique in proving Lemma 5 is complicated by the fact that we consider, for the non-random part, any structure defined over a unary vocabulary.

In contrast to randomised complexity classes such as BPP, for which there is evidence towards the fact that they can be derandomised (i.e., BPP = PTIME, cf. [9]), first-order logic provably gains expressive power by randomisation. In [5], we obtained the following results:

- on additive structures, $\mathsf{BPFO} \not\preceq \mathsf{FO}$, i.e., there is a query of additive structures which is definable in BPFO but not in FO
- on ordered structures, $\mathsf{BPFO} \not\preceq \mathsf{MSO}$
- $\mathsf{BPFO} \not\preceq \mathsf{C}^{\omega}_{\infty\omega}$ (infinitary counting logic)

On the other hand, we obtained the derandomisation results that $\mathsf{BPFO} \preceq \mathsf{MSO}$ on additive structures and $\mathsf{BPFO} \preceq \Sigma_2$ on all structures (both of which are basically translations of the Sipser-Gács-Lautemann-Theorem that $\mathsf{BPP} \subseteq \Sigma^p_2$) and $\mathsf{BPFO} \preceq \mathsf{FO}$ on structures over the empty vocabulary.

There is an elaborate machinery of tools for proving non-definability results in classical logics, most importantly game theoretic methods such as Ehrenfeucht-Fraïssé games and applications of Håstad's Switching lemma to first-order logic via a translation to AC^0 circuit families. To apply these methods to show that, say, the class of all connected graphs is not definable in first-order logic, one constructs, for each sentence φ, a pair of graphs G and G' such that $G \models \varphi \Leftrightarrow G' \models \varphi$, but only exactly one of the two is connected.

For proving non-definability in randomised logics, however, one has to prove that certain sentences can not have a probability gap. Therefore one has to investigate the behaviour of these sentences on *all* finite structures. For example, let A be a $\{P, R\}$-structure, where P is a unary relation and R a binary relation. We view the relation R as a function

$$f : \begin{cases} V(A) & \to 2^{P(A)} \\ a & \mapsto \{b \in P(A) \mid (a, b) \in R(A)\} \end{cases}$$

from the universe of A to subsets of $P(A)$ (cf. Figure 1). The following sentence in $\mathsf{FO}[\{P,R\}]$ is satisfied iff f is injective:

$$\varphi_{\text{inj}} = \forall x \forall y \exists z \, (Pz \wedge \neg(Rxz \leftrightarrow Ryz))$$

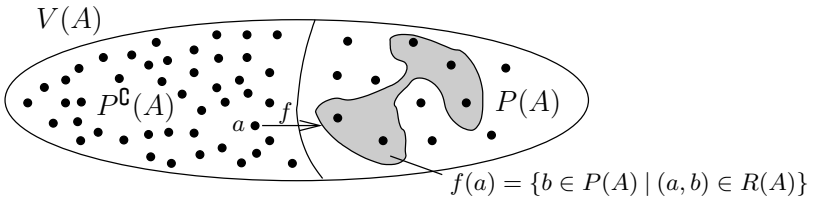

Figure 1 The random relation R interpreted as a function.

Up to isomorphism, a $\{P\}$-structure A is determined by its total number of element n and the number of elements k in $P(A)$. Now fix a $\{P\}$-structure A and let X be a randomly chosen $\{P,R\}$-expansion of A. The probability that f as defined above is injective is monotonely decreasing in n for fixed k and monotonely increasing in k for fixed n. In fact, because the range of the function f doubles if k is increased by 1, for almost all n this probability makes a sudden jump from nearly 0 for $k \leq k_n$ to nearly 1 at $k > k_n + 1$ for some k_n. In this sense, φ_{inj} *almost* has a gap. In [5] we used a similar sentence together with a binary relation to impose additional structures on $V(A)$ and $P(A)$ which can not be of size n and k such that $\Pr(A \models \varphi)$ is in $(0.2, 0.5)$.

In the present paper we show that binary relation symbols are actually necessary for this: On the class of all structures over vocabularies of only unary relations, BPFO is not more expressive than FO. For our above example this implies that for every $0 < \alpha < \beta < 1$, there is a $\{P\}$-structure A such that $\Pr(A \models \varphi_{\text{inj}}) \in (\alpha, \beta)$. Our proof uses a result of Boppana [3] on the average sensitivity of AC^0-circuits; a similar approach has been taken in [2] to proof smoothness laws for first-order logic.

In section 6, we then investigate the question of how expressive BPFO is on word models, i.e., structures in which all non-unary relations depend only on the size of the structure. Let Σ be a finite alphabet. With every word $w \in \Sigma^*$ we associate a structure which has one universe element for each position in w. The vocabulary of the structure contains one unary predicate P_a for each $a \in \Sigma$, along with some relations which only depend on the length of w. Two common choices for these relations are

- a binary successor relation, which we denote by $+1$ or $y \doteq x + 1$ and which is supposed to hold true iff y is the position immediately to the right of x, and
- a binary linear ordering relation $\leq$, where $x \leq y$ is supposed to hold true iff x is to the left of or identical to y.

The expressive power of various logics on these word models has been the subject of intensive study, cf. [12] for a comprehensive overview. As for complexity theory, while MSO-model-checking on word models is fixed-parameter tractable when parameterised by the size of the formula, this is not the case for general structures unless PTIME = NP.

When we speak of $\mathsf{FO}[+1]$, $\mathsf{FO}[\leq]$, $\mathsf{BPFO}[+1]$, and $\mathsf{BPFO}[\leq]$, we mean (randomised) first-order logic restricted to word models of the appropriate type. The very low expressive power of first-order logic on word models suggests that, as in the case of BPFO on unary structures, it might not be possible to ensure a probability gap on all finite structures (or at least on all word models) to get a BPFO-definable query on word models which is not definable in FO. As a first step in this direction, we show that there is an $\mathsf{FO}[\leq]$-definable query which can not be defined in $\mathsf{BPFO}[+1]$.

2 Preliminaries

We consider only finite structures over relational vocabularies. That is, a vocabulary σ is a finite set of relation symbols, each with an associated arity $r > 0$. A σ-structure A is a finite set $V(A)$ together with a subset $R(A) \subseteq V(A)^r$ for each relation symbol $R \in \sigma$ of arity r. An isomorphism $f : A \xrightarrow{\sim} B$ is a bijective function $f : V(A) \to V(B)$ such that for all r-ary $R \in \sigma$,

$$(a_1, \dots, a_r) \in R(A) \text{ iff } (f(a_1), \dots, f(a_r)) \in R(B),$$

and two structures A and B are called isomorphic (written $A \cong B$) if such an isomorphism exists. A *query* $\mathcal{Q}$ is a class of structures closed under isomorphisms. A partial isomorphism $a_1 \dots a_k \mapsto b_1 \dots b_k$ consists of k elements $a_1, \dots, a_k \in V(A)$ and k elements $b_1, \dots, b_k \in V(B)$ such that

$$(a_{i_1}, \dots, a_{i_r}) \in R(A) \text{ iff } (b_{i_1}, \dots, b_{i_r}) \in R(B)$$

for every r-ary $R \in \sigma$ and $1 \leq i_1, \dots, i_r \leq k$. For vocabularies $\sigma \subseteq \tau$, a *τ-expansion* of a σ-structure A is any τ-structure B for which $V(B) = V(A)$ and $R(B) = R(A)$ for all $R \in \sigma$.

First-order (FO) formulas are built from atomic formulas $x \doteq y$ and $Rx_1 \dots x_r$ for r-ary $R \in \sigma$ by boolean junctors, existential and universal quantification. The models relation $\models$, free variables, and quantifier depth of a formula are defined as usual. A sentence is a formula without free variables. For an FO-sentence φ, we denote by $\mathrm{Mod}(\varphi)$ the class of all finite structures A with $A \models \varphi$. A query $\mathcal{Q}$ is said to be definable in FO if there is a sentence φ such that $\mathcal{Q} = \mathrm{Mod}(\varphi)$.

Two structures A and B are called m-equivalent, written $A \equiv_m B$, if they satisfy exactly the same FO-formulas of quantifier rank up to m. By Ehrenfeucht's Theorem (cf. [4]), this is equivalent to the existence of a winning strategy for Duplicator in the following game (called Ehrenfeucht-Fraïssé game):

Two players, called Spoiler and Duplicator, take turns in choosing elements from two structures A and B. Spoiler moves first. If, in the k-th round, Spoiler chooses an element a_k from structure A, Duplicator has to answer with an element b_k from structure B, and vice versa. Duplicator wins if, after m rounds have been played, $a_1 \dots a_m \mapsto b_1 \dots b_m$ is a partial isomorphism.

After fixing a linear order on σ, a σ-structure A may be encoded (non-uniquely) by a string $x_A \in \{0,1\}^*$ of length polynomial in $|V(A)|$, by encoding the information $(a_1, \dots, a_r) \in R(A)$ for every tuple $(a_1, \dots, a_r) \in V(A)^r$ and every relation symbol $R \in \sigma$ by one letter. An FO-sentence φ of quantifier depth d may be translated into a family of boolean circuits $(C_n)_{n \geq 1}$ of depth d and size $n^{O(1)}$ such that

$$A \models \varphi \text{ iff } C_{|A|}(x_A) = 1,$$

and the outcome of $C_{|A|}(x_A)$ is independent of the particular string representing A. The circuits C_n are composed of negation gates and $\vee$ and $\wedge$ gates of arbitrary fan-in.

A result of Boppana gives a bound on the sensitivity of such circuit families:

▶ **Theorem 1.** *Let $f : \{0,1\}^* \to \{0,1\}$ be a boolean function computable by a family $(C_n)_{n \geq 0}$ of boolean circuits of depth d, size $n^{O(1)}$ consisting of negation gates and $\vee$ and $\wedge$-gates of unbounded fan-in. If x is chosen uniformly at random from $\{0,1\}^n$ then*

$$\mathbb{E}\left|\{1 \leq i \leq n \mid f(x) \neq f(x^{(i)})\}\right| \leq O(\log^{d-1} n),$$

where $x^{(i)}$ is the string x with the i-th bit flipped.

The expected value in the theorem is called the *average sensitivity* of f. For a proof, see [3].

3 Randomised logics

We briefly review the definition of randomised logics given in [5]. Throughout this section, let τ and ρ be disjoint vocabularies. Relations over ρ will be "random", and we will reserve the letter R for relation symbols from ρ. We are interested in *random* $(\tau \cup \rho)$*-expansions* of τ-structures. For a τ-structure A, by $\mathcal{X}(A, \rho)$ we denote the class of all $(\tau \cup \rho)$-expansions of A. We view $\mathcal{X}(A, \rho)$ as a probability space with the uniform distribution. Note that we can "construct" a random $X \in \mathcal{X}(A, \rho)$ by deciding independently for all k-ary $R \in \rho$ and all tuples $\vec{a} \in V(A)^k$ with probability $1/2$ whether $\vec{a} \in R(X)$. We are mainly interested in the probabilities

$$\Pr_{X \in \mathcal{X}(A,\rho)}(X \models \varphi)$$

that a random $(\tau \cup \rho)$-expansion of a τ-structure A satisfies a sentence φ of vocabulary $\tau \cup \rho$ of some logic. For brevity, we denote the above probability by $\Pr(A \models \varphi)$ whenever the vocabulary ρ of random relations is clear from the context.

▶ **Definition 2.** Let L be a logic and $0 \leq \alpha \leq \beta \leq 1$.

1. A formula $\varphi \in \mathsf{L}[\tau \cup \rho]$ that defines a k-ary query has an $(\alpha, \beta]$-*gap* if for all τ-structures A and all $\vec{a} \in V(A)^k$ it holds that

   $$\Pr(A \models \varphi[\vec{a}]) \leq \alpha \qquad \text{or} \qquad \Pr(A \models \varphi[\vec{a}]) > \beta.$$

2. The logic $\mathsf{P}_{(\alpha,\beta]}\mathsf{L}$ is defined as follows: For each vocabulary τ,

   $$\mathsf{P}_{(\alpha,\beta]}\mathsf{L}[\tau] := \bigcup_{\rho} \big\{ \varphi \in \mathsf{L}[\tau \cup \rho] \mid \varphi \text{ has an } (\alpha, \beta]\text{-gap} \big\},$$

   where the union ranges over all vocabularies ρ disjoint from τ. To define the semantics, let $\varphi \in \mathsf{P}_{(\alpha,\beta]}\mathsf{L}[\tau]$ be a sentence (the definition for arbitrary formulas is straightforward). Let ρ be such that $\varphi \in \mathsf{L}[\tau \cup \rho]$. Then for all τ-structures A,

   $$A \models \varphi \quad :\Leftrightarrow \quad \Pr(A \models \varphi) > \beta,$$

   and $\mathrm{Mod}(\varphi)$ is the class of all structures A with $A \models \varphi$.

It is easy to see that for every logic L and all α, β with $0 \leq \alpha \leq \beta \leq 1$ the logic $\mathsf{P}_{(\alpha,\beta]}\mathsf{L}$ is a well-defined logic, in the sense that the $\models$-relation is invariant under isomorphisms of the structure and under renamings and extensions of the vocabulary (see [5] for details). We will be focusing on the logic

$$\mathsf{BPFO} := \mathsf{P}_{(1/3,2/3]}\mathsf{FO}$$

in this paper. The strength of this logic does not depend on the exact choice of the parameters α and β, which justifies the arbitrary choice of the constants $1/3, 2/3$ in the definition. As for first-order logic, we say that a query $\mathcal{Q}$ is *definable* in BPFO if there is a sentence $\varphi \in \mathsf{BPFO}$ with $\mathcal{Q} = \mathrm{Mod}(\varphi)$.

4 BPFO = FO on structures with unary vocabulary

In [5] we gave several examples of queries which were definable in BPFO but (in particular) not in FO. A common feature of these queries is that they are defined on structures over a vocabulary with at least binary relations. In this section we will prove that this is in fact necessary:

▶ **Theorem 3.** *Let $\tau = \{P_1, \dots, P_s\}$ be a vocabulary containing only unary relations, and let $\varphi \in \mathsf{BPFO}$. Then there is a (non-randomised) $\mathsf{FO}[\tau]$-sentence defining the same query as φ.*

We may restrict ourselves to structures in which every element satisfies exactly one of the P_i, and we call these *τ-coloured* structures. In fact, a τ-structure can be seen as a set partitioned into 2^s classes, where the elements in each class satisfy exactly the same predicates P_i. We introduce a new vocabulary $\tau' = \{P'_I \mid I \subseteq [s]\}$ and associate with each τ-structure a τ'-coloured structure and vice versa in the obvious way. Similarly, each atomic formula $P_i x$ can be expressed as a boolean combination of atomic formulas $P'_I x$ and vice versa.

Up to isomorphism, a (finite) τ-coloured structure is described uniquely by a tuple $\vec{n} = (n_1, \dots, n_s) \in \mathbb{N}^s$ of non-negative integers giving the size of each class, and we will denote structures by such tuples. We denote the size of such a structure by $\|\vec{n}\| := \sum_{i=1}^{s} n_i$. For each $k \in \mathbb{N}$ we define an equivalence relation $\sim_k$ on $\mathbb{N}^s$ by saying $\vec{n} \sim_k \vec{m}$ iff

$$n_i = m_i \qquad \text{or} \qquad n_i \geq k \text{ and } m_i \geq k$$

for all $1 \leq i \leq s$. Then $\sim_k$ gives exactly the expressive power of first-order sentences of quantifier rank k on τ-coloured structures:

▶ **Lemma 4.** *Let φ be an $\mathsf{FO}[\tau]$-sentence of quantifier rank $\leq k$. Then on τ-coloured structures, $\mathrm{Mod}(\varphi)$ is a union of $\sim_k$-equivalence classes. Conversely, every union of $\sim_k$-equivalence classes can be defined by an $\mathsf{FO}[\tau]$-sentence of quantifier rank $\leq k$.*

Proof. This is a standard application of Ehrenfeucht-Fraïssé games, see, e.g., [4, ex. 2.3.12]. ◀

We may thus restate Theorem 3 as follows:

▶ **Lemma 5.** *Let $\tau = \{P_1, \dots, P_s\}$ be as above and let ρ be any relational vocabulary with $\tau \cap \rho = \emptyset$. Then for every $\varphi \in \mathsf{FO}[\tau \cup \rho]$ and $0 < \alpha < \beta < 1$ one of the following holds:*

1. *there is a tuple $(n_1, \dots, n_s) \in \mathbb{N}^s$ with*

   $$\Pr(A \models \varphi) \in (\alpha, \beta)$$

   or
2. *there is a $k \in \mathbb{N}$ such that for all $\vec{n}, \vec{m}$ with $\vec{n} \sim_k \vec{m}$ the probabilities $\Pr(\vec{n} \models \varphi)$ and $\Pr(\vec{m} \models \varphi)$ are either both $\leq \alpha$ or both $\geq \beta$.*

The proof of this lemma is based on the fact that, if we make a large colour class a little smaller by removing one element, the satisfaction probability of an $\mathsf{FO}[\tau \cup \rho]$-sentence does not change by much. Here, *large* means both absolutely large (at least a certain number of elements) and relatively large, i.e., containing at least some constant fraction of all elements. This is made precise in the following lemma, which we prove below:

▶ **Lemma 6.** *Let $\tau = \{P_1, \dots, P_s\}$ and ρ be vocabularies as above, and $\varphi \in \mathsf{FO}[\tau \cup \rho]$. For every $c, \epsilon > 0$ there is a $k = k_{c,\epsilon,\varphi} \in \mathbb{N}$ such that the following holds: If $\vec{n} \in \mathbb{N}^s$ is a tuple such that $n_i \geq c\,\|\vec{n}\|$ and $n_i \geq k$, then*

$$|\Pr(\vec{n} \models \varphi) - \Pr(\vec{n}' \models \varphi)| < \epsilon,$$

where $n'_i = n_i - 1$ and $n'_j = n_j$ for $j \neq i$.

Proof of Lemma 5. Let φ be any $\mathsf{FO}[\tau \cup \rho]$-sentence and let $k = k_{1/s,\beta-\alpha,\varphi}$ be the constant which Lemma 6 yields for $c = 1/s$ and $\epsilon = \beta - \alpha$. For any tuple $\vec{n} = (n_1, \ldots, n_s) \in \mathbb{N}^s$, the tuple $\vec{\nu}$ with

$$\nu_i = \min\{n_i, k\}$$

is a canonical representative of its $\sim_k$-equivalence class. We give a sequence

$$\vec{n} = \vec{n}_0, \vec{n}_1, \ldots, \vec{n}_l = \vec{\nu}$$

of tuples such that $\vec{n}_i \sim_k \vec{n}_{i+1}$ and

$$|\Pr(\vec{n}_i \models \varphi) - \Pr(\vec{n}_{i+1} \models \varphi)| < \beta - \alpha$$

hold for all $0 \leq i < l$. We define such a sequence by successively decreasing one of the maximal entries which are greater than k until there are no such entries left. Because any maximal entry of a tuple $\vec{n} \in \mathbb{N}^s$ must be at least $\|\vec{n}\|/s$, Lemma 6 precisely states that the satisfaction probability of φ never changes by more than $\beta - \alpha$ in each step, as claimed.

But now the satisfaction probabilities $\Pr(\vec{n}_i \models \varphi)$ along the sequence are either all $\leq \alpha$, all $\geq \beta$, or one of them is in the open interval (α, β). Because $\vec{\nu}$ is the same for all tuples in a $\sim_k$-equivalence class, the statement of the theorem follows. ◀

Notice that there may well be $\vec{n}$ and $\vec{m}$ with $\vec{n} \sim_k \vec{m}$ and such that $|\Pr(\vec{n} \models \varphi) - \Pr(\vec{m} \models \varphi)|$ is arbitrarily close to 1, but in that case, for every $\Pr(\vec{n} \models \varphi) < \alpha < \beta < \Pr(\vec{m} \models \varphi)$ we can find a $\vec{u}$ with $\Pr(\vec{u} \models \varphi) \in (\alpha, \beta)$.

Proof of lemma 6. We introduce a new unary relation symbol Q and define an $\mathsf{FO}[\tau \cup \rho \cup \{Q\}]$-formula ψ by restricting all quantifiers of φ to $Q \cup \bigcup_{j \neq i} P_j$. That is, we define ψ recursively from φ by

- if $\varphi = \exists x \varphi'$ then $\psi := \exists x(Qx \vee \bigvee_{j \neq i} P_j x) \wedge \psi'$,
- if $\varphi = \forall x \varphi'$ then $\psi := \forall x\big((Qx \vee \bigvee_{j \neq i} P_j x) \to \psi'\big)$,
- if $\varphi = \neg\varphi'$, then $\psi := \neg\psi'$,
- if $\varphi = \varphi' \vee \varphi''$, then $\psi := \psi' \vee \psi''$,
- if $\varphi = \varphi' \wedge \varphi''$, then $\psi := \psi' \wedge \psi''$, and
- $\psi := \varphi$ otherwise.

Define $\vec{m}$ by

$$m_i := 2n_i \qquad \text{and} \qquad m_j := n_j \text{ for } j \neq i.$$

Treating Q as a random relation (along with the relations in ρ) and conditioning on the size of $Q \cap P_i$ we get

$$\Pr(\vec{n} \models \varphi) = \Pr_{X \in \mathcal{X}(\vec{m}, \rho \cup \{Q\})} \big(X \models \psi \;\big|\; |Q \cap P_i| = n_i\big)$$

and

$$\Pr(\vec{n}' \models \varphi) = \Pr_{X \in \mathcal{X}(\vec{m}, \rho \cup \{Q\})} \big(X \models \psi \;\big|\; |Q \cap P_i| = n_i - 1\big).$$

Our goal is to show that these two (conditional) probabilities are not too far apart. We first translate the sentence ψ into a bounded-depth, polynomial-size circuit C as in Figure 2. The depth d of this circuit is equal to the quantifier depth of ψ, and it has one input for each relation symbol in $\rho \cup \{Q\}$ and each tuple of universe elements of appropriate arity. (We

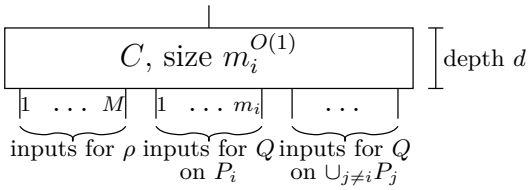

Figure 2 A polynomial-size, bounded-depth circuit for ψ

assume the unary predicates $P_1, \ldots, P_s$ to be hard-wired into the circuit.) In particular, there are $m_i = 2n_i$ inputs which determine the set $Q \cap P_i$.

The inputs corresponding to $Q \cap \bigcup_{j\neq i} P_j$ are, by our construction of ψ, irrelevant and we fix them to 0. Suppose there are M inputs corresponding to random relations in ρ. For each way of fixing these inputs to a certain value $y \in \{0,1\}^M$ we get a circuit C_y on m_i inputs, which is of the same depth as C. Furthermore, because $M = \|\vec{n}\|^{O(1)}$ and we assumed n_i to be $\Omega(\|\vec{n}\|)$, the size of C_y is polynomial in m_i.

By Theorem 1, the average sensitivity of C_y is polylogarithmic in n_i, and therefore also in m_i. This means that if $Q \subseteq [m_i]$ and $q \in [m_i]$ are chosen uniformly and independent of each other, then

$$\Pr(C_y(Q) \neq C_y(Q \triangle \{q\})) < \frac{(\log m_i)^{O(1)}}{m_i} < m_i^{-0.9}$$

for m_i large enough. Notice that Boppana's upper bound depends only on the size and depth of the C_y and thus it is independent of the particular choice of y.

Let A be the event that both $|Q \cap P_i| = n_i$ and $q \in Q$. Then

$$\Pr(A) = \frac{1}{2^{2n_i+1}} \binom{2n_i}{n_i},$$

which is $\Theta(n_i^{-1/2})$ and therefore $\Theta(m_i^{-1/2})$ by standard calculations (see, e.g., [7]). By the independence of the inputs of C we have

$$\Pr(\vec{n} \models \varphi) = 2^{-M} \sum_y \Pr\left(C_y(Q) = 1 \mid A\right)$$

and

$$\Pr(\vec{n}' \models \varphi) = 2^{-M} \sum_y \Pr\left(C_y(Q \triangle \{q\}) = 1 \mid A\right)$$

We may now bound the difference of these probabilities as follows:

$$\begin{aligned}
&|\Pr(\vec{n} \models \varphi) - \Pr(\vec{n}' \models \varphi)| \\
&\leq 2^{-M} \sum \Pr\left(C_y(Q) \neq C_y(Q \triangle \{q\}) \;\middle|\; A\right) \\
&\leq 2^{-M} \sum \frac{\Pr\left(C_y(Q) \neq C_y(Q \triangle \{q\}) \cap A\right)}{\Pr(A)} \\
&\leq 2^{-M} \sum \frac{\Pr\left(C_y(Q) \neq C_y(Q \triangle \{q\})\right)}{\Pr(A)} \\
&\leq m_i^{-0.9} \cdot \Theta(m^{1/2}) < m_i^{-0.3}
\end{aligned}$$

for m_i large enough. We assumed $m_i \geq k$, and thus this difference is $< \epsilon$ if we choose k large enough. ◀

The above proof technique can be adapted to yield the following somewhat stronger result:

▶ **Theorem 7.** *Let $\sigma = \{E\}$ be a vocabulary containing just one binary relation E, and let $\mathcal{EQ}$ be the class of all finite structures A for which $E(A)$ is an equivalence relation. Then* BPFO = FO *on $\mathcal{EQ}$.*

▶ Remark. Note that because $\mathcal{EQ}$ is definable in FO, for every sentence φ with a probability gap on $\mathcal{EQ}$ there is a sentence φ' which is equivalent to φ on $\mathcal{EQ}$ and has a probability gap on all finite structures.

Proof. Up to isomorphism, a structure $A \in \mathcal{EQ}$ is determined by a function $f^A : \mathbb{N} \to \mathbb{N}$ such that $f^A(s)$ counts the number of equivalence classes of size s (so that $|V(A)| = \sum s f^A(s) =: \|f\|$). For each $k \in \mathbb{N}$ we define a function

$$f_k^A(s) = \begin{cases} \min\{k, f^A(s)\} & \text{if } s < k, \\ \min\{k, \sum_{i \geq k} f^A(i)\} & \text{if } s = k, \\ 0 & \text{if } s > k. \end{cases}$$

We say $A \sim_k B$ if $f_k^A(s) = f_k^B(s)$ for all $s \in \mathbb{N}$. By standard techniques, a query $\mathcal{Q} \subseteq \mathcal{EQ}$ is definable in FO iff it is a union of $\sim_k$-equivalence classes for some k. A function f is *k-canonical* if $f(s) \leq k$ for all s and $f(s) = 0$ for all $s > k$. The k-canonical functions form a system of representatives for the equivalence relation $\sim_k$, and we denote the representative equivalent to f by $\tilde{f}$.

For notational convenience, again we assume there is only one random relation symbol R. Fix a formula $\varphi \in \{E, R\}$ and an $\epsilon > 0$. As in Lemma 6 we show that there is a k such that for every f there is a sequence

$$f = f_0 \sim_k f_1 \sim_k f_2 \sim_k \cdots \sim_k f_l = \tilde{f}$$

with $|\Pr(f_i \models \varphi) - \Pr(f_{i+1} \models \varphi)| < \epsilon$ along the sequence. To get from f_i to f_{i+1} we proceed as follows: Suppose $n := \|f_i\| > k^3$. If one equivalence class has $> n^{1/3}$ elements (i.e. $f_i(s) > 0$ for some $s > n^{1/3}$) we remove one element from that class. Otherwise, there must be an $s \leq n^{1/3}$ such that $f(s) > n^{1/3}$.In this case, remove an entire equivalence class of size s. Finally, if $\|f_i\| \leq k^3$, we may remove elements from equivalence classes of size $> k$ and remove an equivalence class of size s if there are more than k classes of that size. Proceeding in this way we eventually reach $\tilde{f}$.

Removing an element from a class is done by randomly choosing from a class of twice the size, and removing a class of a certain size is done by randomly choosing among twice as many classes of that size. We defer details to the full version of this paper. ◀

5 Some queries which are not definable in BPFO

Using the same techniques as in the proof of Theorem 3, we obtain the following non-definability results:

▶ **Theorem 8.** *The following queries on finite structures are not definable in* BPFO*:*

(a) Over the vocabulary $\{\leq\}$ containing a binary relation symbol $\leq$, the query "$\leq$ defines a linear order of even cardinality"

(b) Over the vocabulary $\{E\}$ containing a binary relation symbol E, the query "E defines a connected graph"

(c) Over the vocabulary $\{+1\}$ containing a binary relation symbol $+1$, the query "the universe elements form an initial segment of the natural numbers, treating $+1$ as a successor relation".

Proof. Denote by $\mathcal{O}_n$ the linear order on n elements. For query (a), introduce a new random unary relation P on a linear order of length $2n$ and relativise all quantifiers to P as in the proof of Lemma 6. Letting n tend to infinity, this shows that

$$\left| \Pr_{\mathcal{O}_n,\rho}(X \models \varphi) - \Pr_{\mathcal{O}_{n-1},\rho}(X \models \varphi) \right| \to 0$$

for any $\mathsf{FO}[\{\leq\} \cup \rho]$-sentence φ. In a different context, this result had already been obtained by Boppana and Spencer [2], using essentially the same argument.

Non-definability of query (b) follows because we can define a graph on $\mathcal{O}_n$ in FO which is connected iff n is even. Namely, identifying the elements of the linear order with the first n natural numbers, connect elements

- x and $x+2$ for all $1 \leq x \leq n-2$,
- 2 and $n-1$.

Thus a BPFO-sentence defining connected graphs could be used to define evenness of a linear order (see [4] for details). A similar argument works for query (c). ◀

6 Randomised First-Order Logic on Words

As before, we denote by $\mathsf{FO}[+1]$, $\mathsf{FO}[\leq]$, $\mathsf{BPFO}[+1]$, and $\mathsf{BPFO}[\leq]$ (randomised) first-order logic restricted to word models of the appropriate type. There are two natural definitions of BPFO on restricted classes of structures, namely one which demands BPFO sentences to have a gap on *all* finite structures, and one which demands this only on structures from the restricted class. Because the fact that $\leq$ defines a linear order is definable in FO, word models of the second type can be defined in FO and this distinction does not affect the expressive power of $\mathsf{BPFO}[\leq]$. In contrast to this, the successor relation $+1$ can not be defined in FO, because connexness of the transitive closure of $+1$ is not definable. By Theorem 8(c), this holds true also for BPFO. Therefore, the two definitions of $\mathsf{BPFO}[+1]$ potentially have different expressive power. Our counterexample in Theorem 9 works for both variants.

The expressive power of $\mathsf{FO}[+1]$ and $\mathsf{FO}[\leq]$ is well understood, see [12]. In particular, the query

$$Q := a^*ba^*ca^* \subseteq \{a,b,c\}^*$$

of all words which contain exactly one b to the left of exactly one c and an arbitrary number of as is not definable in $\mathsf{FO}[+1]$. It is easily seen to be definable in $\mathsf{FO}[\leq]$ by the sentence

$$\exists x \exists y (P_b x \wedge P_c y \wedge x \leq y \wedge \forall z (P_a z \vee z \doteq x \vee z \doteq y)).$$

We show that Q is not definable in $\mathsf{BPFO}[+1]$:

▶ **Theorem 9.** *There is no $\mathsf{BPFO}[+1]$-sentence φ such that*

$$w \models \varphi \quad \Leftrightarrow \quad w \in Q$$

for all $w \in \{a,b,c\}^*$.

Proof. Let $\sigma = \{+1, P_a, P_b, P_c\}$ be the vocabulary of our word models. We show the theorem by exhibiting a sequence of pairs of words v_n, w_n such that

(i) $v_n \in Q$, $w_n \notin Q$ for all $n \geq 1$ and
(ii) for every vocabulary ρ disjoint from σ and every $\mathsf{FO}[\sigma \cup \rho]$-sentence φ,

$$|\Pr(v_n \models \varphi) - \Pr(w_n \models \varphi)| \to 0 \qquad (n \to \infty).$$

In fact, choosing

$$v_n = a^n b a^n c a^n \qquad w_n = a^n c a^n b a^n$$

will do. Condition (i) is obviously satisfied. For condition (ii), let ρ be disjoint from σ and let φ be a sentence of quantifier rank r. The successor relation induces a distance measure on the elements of the structures, which we denote by d; we assume $d(x, y) = 1$ if $x = y + 1$ or $y = x + 1$. We denote by d_r the bounded distance function

$$d_r(x, y) := \begin{cases} d(x, y) & \text{if } d(x, y) \leq r \\ \infty & \text{otherwise.} \end{cases}$$

By $S^r(x)$ we denote the r-ball around an element x in (a $(\sigma \cup \rho)$-expansion of) a word structure A, i.e.,

$$S^r(x) := \{y \in V(A) \mid d(x, y) \leq r\},$$

and if $a_1, \ldots, a_k$ are elements of $V(A)$, then $A|_{S^r(a_1,\ldots,a_k)}$ denotes the induced substructure of A on the union $\bigcup_{i=1}^{k} S^r(a_k)$ of the r balls around these elements. We say that two sets $U, V \subseteq V(A)$ *touch* if there are $x \in U$ and $y \in V$ with $x = y + 1$ or $y = x + 1$.

For $n > 3^r$, the word structures v_n and w_n satisfy exactly the same first-order sentences of quantifier rank up to r. A winning strategy for the r-move Ehrenfeucht-Fraïssé-game on v_n and w_n can be given explicitly as follows: For ease of notation, we denote the first and the last position of v_n by a_1 and a_2, the unique position containing a b by a_3 and that containing a c by a_4, and likewise for $b_1, \ldots, b_4$. Suppose after k moves, elements $a_5, \ldots, a_{k+4}$ have been chosen in v_n, and elements $b_5, \ldots, b_{k+4}$ have been chosen in w_n. Assume Spoiler chooses an element a in v_n. Throughout the game, Duplicator maintains the property that

$$d_{3^{r-k}}(a_i, a_j) = d_{3^{r-k}}(b_i, b_j) \tag{1}$$

for $1 \leq i, j \leq k + 4$. Notice that this property holds before the first move (i.e., for $a_1, \ldots, a_4$ and $b_1, \ldots, b_4$) if $n > 3^r$. Let $r' = r - k - 1$ be the number of rounds remaining after the k-th move.

(I) If a is in $v_n|_{S^{3^{r'}}(a_1,\ldots,a_{k+4})}$, then choose the corresponding element in w_n, i.e., the unique element $b \in V(w_n)$ which has

$$d_{3^{r'}}(a_i, a) = d_{3^{r'}}(b_i, b)$$

for $1 \leq i \leq k + 4$. This is possible because if $d(b_i, b), d(b_j, b) \leq 3^{r'}$, then $d(b_i, b_j) \leq 2 \cdot 3^{r'} < 3^{r-k}$ and $d_{3^{r-k}}(a_i, a_j) = d_{3^{r-k}}(b_i, b_j)$ by property (1).
(II) Otherwise, choose any element of w_n which has distance $> 3^{r'}$ from all elements $b_1, \ldots, b_{k+4}$.

Duplicator's answer if Spoiler chooses an element b in w_n is determined analogously. After r rounds have been played, the map $a_i \mapsto b_i$ is a partial isomorphism, because all relations in σ are determined by d_1-distances. This is because on the words v_n and w_n, the relations P_a, P_b and P_c depend only on the d_1-distance from u and v, which are parts of the tuples.

We now extend this strategy to random expansions X of v_n and Y of w_n. Let

$$c_0 := 1, \qquad c_{i+1} := 4r_i + 2.$$

In the game on X and Y, Duplicator maintains the stronger property that after the k-th move,

$$X_k := X|_{S^{c_r-k}(a_1,\dots,a_{k+4})} \cong Y|_{S^{c_r-k}(b_1,\dots,b_{k+4})} =: Y_k, \tag{2}$$

treating the a_is and b_is as constants. That this, there is an isomorphism $f : X_k \xrightarrow{\sim} Y_k$ such that $f(a_i) = b_i$ for $1 \leq 1 \leq k+4$. This is of course not possible for all random expansions: At the very least, the random expansions have to agree on the c_r-balls around min, max, u and v. If this is the case, then with very high probability Duplicator can indeed maintain property (2), as we will now show. The argument resembles the proof of the classical 0-1-law for first-order logic (cf. [4]), but it involves some more housekeeping to deal with the additional structure introduced by the +1-relation.

Let μ_w denote the uniform probability measure on the set $\mathcal{X}(w,\rho)$, i.e.,

$$\mu_w(V) := \frac{|V|}{|\mathcal{X}(w,\rho)|}$$

for $V \subseteq \mathcal{X}(w,\rho)$. For ease of notation we drop the subscript w. Let s be the number of non-isomorphic $(\sigma \cup \rho)$-expansions of $v_{2c_r+2}|_{S^{c_r}(\min,\max,u,v)}$, and let $A_1,\dots,A_s$ be structures representing these isomorphism types. Notice that the four c_r-balls which make up the universe of this substructure do not touch, as is the case in all v_n and w_n for large enough n. We let $V_n^{(j)}$ be the set of all $(\sigma \cup \rho)$-expansions X of v_n with

$$X|_{S^{c_r}(\min,\max,u,v)} \cong A_j,$$

and analogously for $W_n^{(j)}$. If the c_r-balls around min, max, u and v do not touch, then the induced substructures of v_n and w_n on the union of these balls are isomorphic. Thus for large enough n, the $V_n^{(j)}$ ($W_n^{(j)}$) form a partition of $\mathcal{X}(v_n,\rho)$ ($\mathcal{X}(w_n,\rho)$), and

$$\mu\left(V_n^{(j)}\right) = \mu\left(W_n^{(j)}\right) = \frac{1}{s}.$$

For any two structures $X \in V_n^{(j)}$ and $Y \in W_n^{(j)}$, the tuples $a_1,\dots,a_4$ and $b_1,\dots,b_4$ as defined above satisfy property (2). We now show that there are subsets $\hat{V}_n^{(j)} \subset V_n^{(j)}$ and $\hat{W}_n^{(j)} \subset W_n^{(j)}$ such that Duplicator can maintain property (2) for r moves on structures taken from these subsets.

To be precise, we define Duplicator's strategy if Spoiler chooses a from structure X as follows:

(I) If a is in $X|_{S^{2c_{r'}+1}(a_1,\dots,a_{k+4})}$, then choose the corresponding element in Y, i.e., the unique element $b \in V(Y)$ which has

$$d_{c_{r'}}(a_i, a) = d_{c_{r'}}(b_i, b)$$

for $1 \leq i \leq k+4$. These are exactly the a whose $c_{r'}$-ball touches the $c_{r'}$-ball around some previously chosen a_i.

(II) Otherwise, choose any element of Y which has distance $> 2c_{r'} + 1$ from all elements $b_1, \dots, b_{k+4}$. Thus the $c_{r'}$-ball around the newly chosen element touches no $c_{r'}$-ball around a previously chosen element.

Moves of type (I) in the above strategy can always be carried out by Duplicator and maintain property (2). Moves of type (II) can only fail if there is a tuple $b_1, \dots, b_{k+4}$ in Y and a $(\sigma \cup \rho)$-structure Z containing elements $a_1, \dots, a_{k+4}$ and a such that

- $Z \in \mathcal{X}(v_n, \rho)$,
- $Z|_{S^{c_{r-k}}(a_1,\dots,a_{k+4})} \cong Y|_{S^{c_{r-k}}(b_1,\dots,b_{k+4})}$,
- $d(a, a_i) > 2c_{r'} + 1$ for $1 \leq i \leq k+4$, and
- $Z|_{S^{c_{r'}}(a_1,\dots,a_{k+4},a)} \ncong Y|_{S^{c_{r'}}(b_1,\dots,b_{k+4},b)}$ for all $b \in V(Y)$.

Let $m := 3n + 2 = |V(Y)|$. There are $O(m^r)$ many possible tuples $b_1, \dots, b_{k+4}$, and for each such tuple, there are only constantly (depending only on ρ) many choices for Z and $a_1, \dots, a_{k+4}, a$ with non-isomorphic $Z|_{S^{c_{r'}}(a_1,\dots,a_{k+4},a)}$. But for each of these $O(m^r)$ possibilities, there is a subset $M \subset V(Y)$ with

- $|M| = \Omega(n)$,
- $d(b, b_i) > 2c_{r'} + 1$, for each $b \in M$ and $1 \leq i \leq k+4$, and
- $d(b, b') > 2c_{r'} + 1$ for every $b, b' \in M$.

Because the $c_{r'}$-balls around the elements of M do not overlap, each of the elements in M satisfies

$$Z|_{S^{c_{r'}}(a_1,\dots,a_{k+4},a)} \cong Y|_{S^{c_{r'}}(b_1,\dots,b_{k+4},b)}$$

independently with some probability $p > 0$ depending only on r' and ρ. The probability that none of the $b \in M$ satisfies this is therefore $(1-p)^{|M|} = e^{-\Omega(n)}$, and by a union bound, there is a subset $\hat{W}_n^{(j)} \subset WV_n^{(j)}$ with

$$\mu\big(\hat{W}_n^{(j)}\big) = \big(1 - o(1)\big)\mu\big(W_n^{(j)}\big)$$

and such that on structures $Y \in \hat{W}_n^{(j)}$, Duplicator can maintain property (2) for r many moves when challenged to move in Y. A subset $\hat{V}_n^{(j)} \subset V_n^{(j)}$ can be defined analogously.

But now we have defined disjoint sets $\hat{V}_n^{(1)}, \dots, \hat{V}_n^{(s)} \subset \mathcal{X}(v_n, \rho)$ and $\hat{W}_n^{(1)}, \dots, \hat{W}_n^{(s)} \subset \mathcal{X}(w_n, \rho)$ such that

(a) $\left|\mu(\hat{V}_n^{(j)}) - \mu(\hat{W}_n^{(j)})\right| \to 0$ for $n \to \infty$ and all $1 \leq j \leq s$,

(b) $\mu\left(\bigcup_j \hat{V}_n^{(j)}\right) \to 1$ for $n \to \infty$

(c) for every n and j, if $X \in \hat{V}_n^{(j)}$ and $Y \in \hat{W}_n^{(j)}$, then $X \cong_r Y$.

This implies that for every $\mathsf{FO}[\sigma \cup \rho]$-sentence φ,

$$|\Pr(v_n \models \varphi) - \Pr(w_n \models \varphi)| \to 0$$

as $n \to \infty$, and therefore Q is not definable in $\mathsf{BPFO}[+1]$. ◀

7 Conclusion

We have shown non-definability results for randomised first-order by bounding the difference

$$|\Pr(A \models \varphi) - \Pr(B \models \varphi)|$$

for certain pairs of σ-structures A and B and $\mathsf{FO}[\sigma \cup \rho]$-sentences φ. We did so using two very different tools:

- Boppana's result on the average sensitivity of bounded-depth polynomial size circuits, and
- Ehrenfeucht-Fraïssé-games on (partially) random structures.

These two approaches have very different strengths and weaknesses: The Ehrenfeucht-Fraïssé-game approach worked well on the query Q because all but a finite number of positions in each of the strings v_n and w_n looked exactly the same to any FO-sentence of quantifier rank $\leq r$. This is not the case in the two-coloured structure with colour-class sizes n and $\log n$, for example. This approach might be extended by drawing the random expansions of A and B from a well-chosen joint distribution.

In order to apply Boppana's result to bound the difference

$$|\Pr(A \models \varphi) - \Pr(B \models \varphi)|$$

between the acceptance probability of φ in two structures A and B, we defined a larger structure within which we were able to define a structure C (using an additional random relation) such that $C \cong A$ with probability at least $n^{-1+\epsilon}$, and such that changing the additional random relation on one tuple resulted in $C \cong B$ with high probability. With this method we could bound the above difference for enough pairs of structures to actually derandomise BPFO on structures with a unary vocabulary completely. This approach was made possible by the fact that the structures A and B for which we applied it had lots of automorphisms, making it easy to define them within the bigger structure with high probability.

It seems reasonable to conjecture that $\mathsf{BPFO}[+1]$ can be derandomised to $\mathsf{FO}[+1]$. This is because to an FO-sentence of quantifier rank r, two positions in the string which are further apart than 3^r are completely non-related, and thus it should be possible to generate chains of strings $w_0, \ldots, w_l$ by only changing small parts in each step to get a version of Lemma 5 for strings. However, neither the Ehrenfeucht-Fraïssé-game approach nor the approach using Boppana's lemma seem to suffice for this.

Acknowledgements

The author would like to thank Martin Grohe and Nicole Schweikardt for helpful discussions on this research topic, and an anonymous referee for pointing out the similarities to the work of Boppana and Spencer [2]. Thanks also to Anuj Dawar for suggesting the extension of Theorem 3 to equivalence classes.

References

1 Sanjeev Arora and Boaz Barak. *Computational Complexity.* Cambridge University Press, 2009.

2 Ravi Boppana and Joel Spencer. Smoothness laws for random ordered graphs. In Ravi Boppana and James Lynch, editors, *Logic and Random Structures*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, pages 15–32. American Mathematical Society, 1995.

3 Ravi B. Boppana. The average sensitivity of bounded-depth circuits. *Information Processing Letters*, 63(5):257–261, 1997.

4 H.-D. Ebbinghaus and J. Flum. *Finite Model Theory.* Perspectives in Mathematical Logic. Springer-Verlag, 2nd edition, 1999.

5 Kord Eickmeyer and Martin Grohe. Randomisation and derandomisation in descriptive complexity theory. In *Computer Science Logic*, volume 6247 of *LNCS*, pages 275–289. Springer-Verlag, 2010.

6 R. Fagin. Probabilities on finite models. *Journal of Symbolic Logic*, 41:50–58, 1976.

7 W. Feller. *An Introduction to Probability Theory and Its Aplications*, volume I. John Wiley & Sons, 1957.

8 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. *Kibernetika*, 2:17–28, 1969. Englisch translation, Cybernetics 5:142–154,1969.

9 Russell Impagliazzo and Avi Wigderson. PTIME = BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *STOC*, pages 220–229, 1997.

10 Saharon Shelah. Very weak zero one law for random graphs with order and random binary functions. *Random Structures & Algorithms*, 9(4):351–358, 1996.

11 Joel Spencer. *The Strange Logic of Random Graphs*. Springer, 2001.

12 Howard Straubing. *Finite Automata, Formal Logic, and Circuit Complexity*. Birkhäuser, 1994.

13 S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.