Circuit Lower Bounds via Ehrenfeucht-Fraïssé Games

Michal Koucký
Mathematical Institute, AS CR, Prague
<koucky@math.cas.cz>

Clemens Lautemann
Johannes Gutenberg-Universität, Mainz

Sebastian Poloczek
Johannes Gutenberg-Universität, Mainz
<sebastian.poloczek@ikb.de>

Denis Thérien
McGill University, Montréal
<denis@cs.mcgill.ca>

May 4, 2006

Abstract

In this paper we prove that the class of functions expressible by first order formulas with only two variables coincides with the class of functions computable by AC^0 circuits with a linear number of gates. We then investigate the feasibility of using Ehrenfeucht-Fraïssé games to prove lower bounds for that class of circuits, as well as for general AC^0 circuits.

1 Introduction

Circuit complexity occupies a central position in theoretical computer science, and proving lower bounds for explicit functions in this model remains a major challenge. The early result [1, 5] that PARITY cannot be computed in AC^0, i.e. by a constant-depth, polynomial-size circuit constructed with AND and OR gates of unbounded fan-in, had raised hopes that, for the most part, failed to materialize.

In this paper we revisit the topic from a descriptive complexity point of view. This framework considers the expressive power of various logical formalisms; the resources that come into play are, for example, the quantifiers and the numerical predicates that are allowed, the alternations in quantification, or the number of variables. A good example of theorem in this area is due to [6]; a language can be described by a first order formula, with no restriction on numerical predicates, iff it can be recognized by a non-uniform AC^0 circuit. A similar result can be shown if one allows modular quantifiers in the formulas and modular gates in the circuits [3].

In this paper, we will first establish that if we restrict first order logic to formulas that use two variables only then this corresponds exactly to AC^0 circuits that have a linear number of gates. This class is known to be properly contained in general AC^0 [4] but, to our knowledge, no simple and explicit example of this separation has been found. (Ajtai's function [2, 4] is highly non-trivial and one could argue whether it is simple.) Our descriptive complexity result leads us to conjecture that the language $L = A^*ac^*aA^* \subseteq \{a, b, c\}^*$ constitutes such an example. It is easily seen to be expressible by a first order formula using $<$ as numerical predicate, hence it is in AC^0, but it can be shown that no two variable formula with $<$ can describe the set. Our conjecture is that two variable definability forms a structural barrier which cannot be overcome by using more fancy numerical predicates. This idea is a running theme in circuit complexity. General first order definability is such a barrier; the regular language PARITY cannot be expressed by a first order formula using $<$ only, and the Furst-Saxe-Sipser theorem says that no additional numerical predicates however elaborate can be used to make the language first order definable. Quantifier alternation yields another example of this phenomenon; there are well known examples of regular languages that are expressible by first order formulas of quantifier alternation depth k using $<$ but that can be shown to be not expressible in depth $k-1$ even if arbitrary numerical predicates are allowed.

The logical interpretation of circuit classes has an interesting consequence, namely the possibility of using the well known technique of Ehrenfeucht-Fraïssé games to prove lower bounds. In this work, we derive an Ehrenfeucht-Fraïssé game argument for non-expressibility of certain functions by two variable formulas from the circuit lower bound proof given in [4]. The switching lemma which is at the heart of the argument is currently not powerful enough to prove the validity of our conjecture though. A similar Ehrenfeucht-Fraïssé point of view is next developed for general AC^0 circuits, using [5] as basis. An apparent advantage of our technique is that it seems to be more robust in terms of uniformity, i.e. it is readily applicable to prove non-expressibility results for any class of numerical predicates. To the best of our knowledge this is the first Ehrenfeucht-Fraïssé game argument showing non-expressibility of explicit functions in first order logic. It would be interesting to weaken our technique so that it could be used to prove non-expressibility of functions when only restricted class of numerical predicates is allowed. For example non-expressibility using the numerical predicate BIT would imply lower bounds for uniform circuit families.

Our paper is organized as follows. The next section contains basic notation and definitions. In Section 3 we establish the correspondence between two variable first order formulas and linear AC^0 circuits. Section 4 provides the Ehrenfeucht-Fraïssé game argument for non-expressibility of certain functions by two variable first order formulas. Section 5 extends our Ehrenfeucht-Fraïssé game argument into one for proving non-expressibility by any first order formula. Section 6 discusses issues regarding arguments against uniform circuits, and Section 7 provides some final thoughts on our methods.

2 Notation and preliminaries

We assume that the reader is familiar with first order logic and circuit complexity. (See e.g. [7, 9]). We review here our notation.

For any integer $n \geq 1$, let $[n]$ denote $\{1, 2, \ldots, n\}$; let $[0] = \emptyset$.

A logical structure $\langle U, P_1, P_2, \ldots, P_\ell \rangle$ is a set U called *universe* with *predicates* $P_1, P_2, \ldots, P_\ell$ on this universe. Each predicate P_i of arity $a_i \in \mathcal{N} \setminus \{0\}$ is a function $P_i : U^{a_i} \to \{\text{TRUE}, \text{FALSE}\}$. For a structure A with all predicates of arity at most k, the *signature of* A is $\langle s_1, s_2, \ldots, s_k \rangle \in \mathcal{N}^k$, where s_i is the number of predicates of arity i in A. A first order formula is built of quantifiers $\forall$ and $\exists$, connectives $\wedge, \vee, \neg$, variables $x, y, z, \ldots$ and predicates $P_1, P_2, \ldots$. A first order formula ϕ is interpreted over a structure A with predicates $P_1, P_2, \ldots$ of proper arities in the usual way. $A \models \phi$ denotes that ϕ is satisfied by A. For a formula $\phi(x)$ with a free variable x, $\phi(x)|_{x \leftarrow i}$ denotes ϕ after substituting i for all free occurrences of x. A *formula* ϕ *has* k *variables* if only k different variables occur in the formula. Each variable can be reused multiple times leading to a formula of arbitrary quantifier depth. For example, $\forall x \exists y (x < y \wedge ((\exists x\; y < x) \vee (\forall x\; x < y)))$ is a two variable formula of quantifier depth three.

In this paper we fix a finite set $\Sigma = \{b_1, b_2, \ldots, b_m\}$ to be our *alphabet*. For any integer $n \geq 1$, Σ^n denotes the set of all strings of length n over Σ, and Σ^+ denotes $\bigcup_{n \geq 1} \Sigma^n$. For $L \subseteq \Sigma^+$ and an integer $n \geq 1$, $L^{=n}$ denotes $L \cap \Sigma^n$.

In this paper we will consider structures of the following type: $A = \langle [n], \sigma_{b_1}, \sigma_{b_2}, \ldots, \sigma_{b_m}, P_1, \ldots, P_\ell \rangle$, where $\sigma_{b_1}, \ldots, \sigma_{b_m}$ are unary predicates and $P_1, \ldots, P_\ell$ are arbitrary predicates. When predicates $\sigma_{b_1}, \ldots, \sigma_{b_m}$ form a partition of the universe, i.e., for every element of $[n]$ exactly one of the predicates is true, then such predicates naturally correspond to a string in Σ^n. Structures with such predicates will be of interest to us.

We call predicates $\sigma_{b_1}, \ldots, \sigma_{b_m}$ the *input predicates* and we call the remaining predicates the *numerical predicates*. Given an arbitrary structure $A = \langle [n], \sigma_{b_1}, \sigma_{b_2}, \ldots, \sigma_{b_m}, P_1, \ldots, P_\ell \rangle$, we can define from such a structure a family of structures that correspond to all possible strings in Σ^n, namely for $w \in \Sigma^n$ we define $A(w)$ to be the structure $A(w) = \left\langle [n], \sigma'_{b_1}, \ldots, \sigma'_{b_m}, P_1, \ldots, P_\ell \right\rangle$ where $\sigma'_{b_i}(j)$ is TRUE iff $w_j = b_i$. Each string $w \in \Sigma^n$ corresponds naturally to an *assignment* $\sigma_w : [n] \to \Sigma$, where $\sigma_w(j) = w_j$. We will often identify a string w with its assignment σ_w. We will use shorthand $\overline{\sigma}$ for $\sigma_{b_1}, \ldots, \sigma_{b_m}$, and similarly, $\overline{\sigma}(v)$ for $\sigma_{b_1}(v), \ldots, \sigma_{b_m}(v)$.

A *first order formula ϕ with no free variables expresses a boolean function* $f : \Sigma^+ \to \{0, 1\}$ if there is a sequence of structures $\{A_n\}_{n=1,\ldots}$ of the same signature such that $A_n = \langle [n], \overline{\sigma}, P_1, \ldots, P_\ell \rangle$ and for any string $w \in \Sigma^n$, $A_n(w) \models \phi$ iff $f(w) = 1$. A boolean function f is *expressible in first order logic* if there is a first order formula that expresses it. We denote the class of functions expressible in first order logic by FO.

We denote by AC^0 the class of functions computable by families of constant-depth polynomial size circuits consisting of unbounded fan-in $\wedge$, $\vee$ and unary $\neg$ gates where the size is measured with respect to the input size. We call such circuits AC^0 circuits. We call *linear* AC^0 the subclass of AC^0 functions that are computable by AC^0 circuits consisting of *linear number of gates*.

Since we consider languages over arbitrary (non-binary) alphabets, we use the following convention for inputs to boolean circuits. An input $w_1 w_2 \cdots w_n \in \Sigma^n$ is presented to a boolean circuit C as follows: C has an input gate $Q_{b_i,j}$, for every $b_i \in \Sigma$ and $j \in [n]$, where $Q_{b_i,j}$ is set to true iff $w_j = b_i$. One should note that if a different convention of input encoding were chosen our results remain essentially unchanged.

3 First order logic and circuit complexity

It is now well understood that many computational complexity classes admit natural logical descriptions. In this paper we are interested in particular in the relationship between constant depth boolean circuits and first order logic. The following relation was established by Immerman:

Proposition 1 ([6]). *A function f is expressible in first order logic iff f is in AC^0.*

We present here an exact bound on the number of variables needed to express functions in linear AC^0.

Theorem 2. *A function f is expressible by a first order formula with two variables only iff f is in linear AC^0.*

The proof follows from the following two lemmas.

Lemma 3. *For any two variable formula Φ with at most one free variable there is a constant c such that for any structure $A = \langle [n], \overline{\sigma}, \ldots \rangle$ with predicates of proper arities there is a circuit C of size $\leq cn$ and depth $\leq c$ such that:*

1. *If Φ has no free variable then C contains a gate g such that on any input $w \in \Sigma^n$ to C gate g evaluates to one iff Φ evaluates to true on $A(w)$.*

2. *If $\Phi = \Phi(x)$ has one free variable x then C contains gates $g_1, \ldots, g_n$ such that on any input $w \in \Sigma^n$ to C and any $i \in [n]$, gate g_i evaluates to one iff $\Phi(x)|_{x \leftarrow i}$ evaluates to true on $A(w)$.*

Proof. W.l.o.g. Φ does not contain any existential quantifier. We prove the claim by induction on the quantifier depth of Φ and within formulas of the same quantifier depth on the structure of the formula.

Case 1. Φ is an atomic formula with no free variable. The claim is trivially true. If Φ contains one free variable x then $\Phi(x) = R(x, x, \ldots, x)$ for some predicate R and the claim is also obviously true.

Case 2. $\Phi = \Psi \vee \Theta$ or $\Phi = \Psi \wedge \Theta$ or $\Phi = \neg\Psi$ and Φ has no free variable. By induction on the structure of formulas, Ψ and Θ have claimed circuits. By combining these circuits in an obvious way we obtain the required circuit for Φ. We proceed analogously if Φ contains one free variable and is a conjunction, disjunction or negation of two formulas.

Case 3. $\Phi = \forall y \Psi(y)$ and Φ has no free variable. By induction hypothesis on quantifier depth, there is a circuit C_Ψ for formula Ψ containing gates $g_1, \dots, g_n$, where g_i evaluates to $\Psi(y)|_{y \leftarrow i}$. Circuits C is constructed from C_Ψ by adding an extra gate $g = \wedge_{i\in[n]} g_i$.

Case 4. $\Phi = \forall y \Psi(x, y)$, where Φ has one free variable x. This is the only non-trivial case. For some integer $k \geq 1$ that depends only on the structure of Ψ we can transform Φ into a logically equivalent two variable formula

$$\forall y \bigwedge_{\ell=1,\dots,k} \Gamma_\ell(x) \vee \Theta_\ell(y) \vee \Delta_\ell(x, y),$$

where for every $\ell \in [k]$

- $\Gamma_\ell(x)$ is a disjunction of atomic formulas in variable x, formulas of the type $\forall y \varphi(x, y)$, formulas with no free variable, and negations thereof.
- $\Theta_\ell(y)$ is a disjunction of atomic formulas in variable y, formulas of the type $\forall x \varphi(x, y)$, and negations thereof.
- $\Delta_\ell(x, y)$ is a disjunction of atomic formulas containing both variables x and y, and negations thereof. In particular, $\Delta_\ell(x, y)$ does *not* contain any input predicate.

This transformation of formula Φ can be done by converting $\Psi(x, y)$ into conjunctive normal form in the usual way and collecting the appropriate sub-formulas. We can further transform Φ into the following logically equivalent formula

$$\bigwedge_{\ell=1,\dots,k} \Gamma_\ell(x) \vee \forall y(\neg\Delta_\ell(x, y) \to \Theta_\ell(y)).$$

By induction hypothesis on the quantifier depth, for $\ell = 1, \dots, k$, there is a circuit C_{Γ_ℓ} of linear size and constant depth with gates $g_{\Gamma_\ell,i}$ that evaluate to $\Gamma_\ell(x)|_{x\leftarrow i}$. Furthermore, there is also a circuit C_{Θ_ℓ} of linear size and constant depth with gates $g_{\Theta_\ell,j}$ that evaluate to $\Theta_\ell(y)|_{y\leftarrow j}$. We define the set $S_{\ell,i} = \{j \in [n];\ \Delta_\ell(i, j)$ evaluates to false on $A\}$. Since $\Delta_j(x, y)$ does not contain any input predicates, set $S_{\ell,i}$ depends only on the numerical predicates of the structure A.

Circuit C is defined as follows. It contains circuits $C_{\Gamma_1}, \dots, C_{\Gamma_k}$ and $C_{\Theta_1}, \dots, C_{\Theta_k}$ and furthermore for every $i \in [n]$, it contains a sub-circuit computing $\bigwedge_{\ell=1,\dots,k} g_{\Gamma_\ell,i} \vee \bigwedge_{j\in S_{\ell,i}} g_{\Theta_\ell,j}$. The output of the i-th sub-circuit will be a gate g_i. Since every i-th sub-circuit adds only three gates to the overall size of C and $\Delta_\ell(x, y)$ does not contribute by any gate to C, circuit C is of linear size and of constant depth.

There are no other cases so the lemma is proven. □

Lemma 4. *If a function $f : \Sigma^+ \to \{0, 1\}$ is in linear AC^0 then f is expressible by a two variable first order formula.*

Proof. Let $\{C_n\}_{n\geq1}$ be the constant depth linear size circuit family computing f. We can assume that every C_n is a layered circuit of a depth d without negations. (By a usual argument we can push all negation gates toward the input gates and then each $Q_{b,j}$ can be replaced by $\vee_{b'\in\Sigma-\{b\}} Q_{b',j}$.) Furthermore, we assume that every layer of C_n contains exactly cn gates, for some integer $c \geq |\Sigma| = m$, and consists entirely of the same type of gates, either input gates, $\vee$- or $\wedge$-gates. We copy gates as necessary. We also assume that gates in one layer get their inputs only from gates in the previous layer and that all the gates of the last (output) layer d have identical inputs, i.e., they are identical.

We will construct a two variable first order formula ϕ and a family $\{A_n\}_{n\geq 1}$ of first order structures $A_n = \langle [n], \overline{\sigma}, P^1_{1,1}, P^1_{1,2}, \ldots, P^1_{c,c}, P^2_{1,1}, P^2_{1,2}, \ldots, P^d_{c,c} \rangle$ such that for any $w \in \Sigma^n$, ϕ is true on $A_n(w)$ iff C_n evaluates to one on w.

For $n \geq 1$, we fix the input predicates $\overline{\sigma}$ arbitrarily, and we define predicates $P^\ell_{s,t}$, $1 \leq \ell \leq d$, $s, t \in [c]$, as follows. Consider circuit C_n. We label each of its gates at layer $\ell \in \{0, \ldots, d\}$ by a distinct label $g^\ell_{\langle s,r \rangle}$, where $s \in [c]$ and $r \in [n]$. We make sure that for each $i \in [c]$ and $j \in [n]$, $g^0_{\langle i,j \rangle}$ is the label for the input gate $Q_{b_{1+(i \bmod m)},j}$ at the first layer. For $1 \leq \ell \leq d$, $s, t \in [n]$ and every $j, k \in [n]$, we define $P^\ell_{s,t}(j,k)$ to be TRUE iff the gate $g^{\ell-1}_{\langle s,j \rangle}$ is an input to the gate $g^\ell_{\langle t,k \rangle}$ in C_n. That specifies the structure A_n.

Now by induction on ℓ, we show that for each layer $\ell \in \{0, \ldots, d\}$ and each $s \in [c]$, there is a two variable first order formula $\psi^\ell_s(x)$ with one free variable such that for any $n \geq 1$, $w \in \Sigma^n$ and $j \in [n]$, $\psi^\ell_s(x)|_{x \leftarrow j}$ is true on $A_n(w)$ iff gate $g^\ell_{\langle s,j \rangle}$ evaluates to one on input w to C_n.

For $\ell = 0$ and $s \in [c]$ we let $\psi^0_s(x) = \sigma_{b_{1+(s \bmod m)}}(x)$. We continue by induction for $\ell \geq 1$. If layer ℓ contains $\vee$-gates then

$$\psi^\ell_s(x) = \bigvee_{t=1}^{c} \exists y \left(P^\ell_{t,s}(y,x) \wedge \psi^{\ell-1}_t(y) \right).$$

Similarly, if layer ℓ contains $\wedge$-gates then

$$\psi^\ell_s(x) = \bigwedge_{t=1}^{c} \forall y \left(P^\ell_{t,s}(y,x) \rightarrow \psi^{\ell-1}_t(y) \right).$$

We let the formula $\phi = \exists x \psi^d_1(x)$. That concludes the proof. □

Our technique from the proof of Lemma 3 can be used to show that functions expressible by formulas with k variables are computable by AC^0 circuits of size $O(n^{k-1})$. That is a slight improvement on the bound $O(n^k)$ that follows from Immerman's proof. We do not know if our bound is optimal though as the only lower bound that we know how to prove is that there are formulas that use k variables that do not have AC^0 circuits of size $O(n^{k/2-1})$. This can be proven using an argument similar to one in the next proposition. We leave the details of such an argument to the interested reader and state and prove Proposition 5.

Proposition 5. *For any $k \geq 1$, there are functions computable by AC^0 circuit families of size $O(n^k)$ that are not expressible by any first order formula with less than $2k$ variables.*

Proof. The proof is by a counting argument similar to [8]. In this proof we assume that the alphabet is binary, i.e., $\Sigma = \{0,1\}$. The proof clearly extends to any alphabet of size at least two. We use the following two claims.

Claim 6. *For any $n \geq 2k^2$, there are at least $2^{n^{2k}/4}$ different functions $f : \Sigma^n \rightarrow \{0,1\}$ that are computable by AC^0 circuits of size $4n^k + 2n + 1$ and depth 5.*

Proof of claim. Let $m = \lfloor \log n^k \rfloor$. Let $\mathcal{S} = \{S_J\}_{J \subseteq [m]}$ be a family of sets $S_J \subseteq \{I;\ I \subseteq [m]\}$. For $I \subseteq [m]$ define $g_I(x_1, \ldots, x_m) = \bigwedge_{i \in I} x_i \wedge \bigwedge_{i \in [m]-I} \neg x_i$. Define function $f_{\mathcal{S}} : \Sigma^n \rightarrow \{0,1\}$ by

$$f_{\mathcal{S}}(x_1, \ldots, x_n) = \bigvee_{J \subseteq [m]} \left(g_J(x_1, \ldots, x_m) \wedge \bigvee_{I \in S_J} g_I(x_{m+1}, \ldots, x_{2m}) \right).$$

It is easy to see that different families $\mathcal{S}$ and $\mathcal{S}'$ give different functions $f_{\mathcal{S}}$ and $f_{\mathcal{S}'}$, each computable by AC^0 family of circuits of size $4n^k + 2n + 1$ and depth 5. As there are $2^{2^{2m}} \geq 2^{n^{2k}/4}$ different families $\mathcal{S}$, the claim follows. $\square$

Claim 7. *Let ϕ be a first order formula of size s using at most $2k-1$ variables. Then ϕ can be used to express at most $2^{sn^{2k-1}}$ functions $f : \Sigma^n \to \{0,1\}$.*

Proof of claim. By the size of ϕ we understand the number of symbols in the description of ϕ. We want to count the number of non-isomorphic first order structures $A = \langle [n], \sigma_0, \sigma_1, \ldots \rangle$ on which ϕ can be used to express a function $f : \Sigma^n \to \{0,1\}$. First, we can assume that every predicate symbol in ϕ occurs at most once as A can interpret several of them in an identical way. Second, we can assume that every predicate in ϕ is of arity at most $2k-1$ as multiple occurrences of a single variable are useless since every predicate symbol is used only once in ϕ. Thus there are at most $2^{sn^{2k-1}}$ different ways how to interpret the numerical predicates occurring in ϕ. Hence, there are at most $2^{sn^{2k-1}}$ non-isomorphic structures A for ϕ. (We assume that A contains only numerical predicates that occur in ϕ and we do not count different settings of input predicates in A as that would lead to the same function f.) The claim follows. $\square$

We finish the proof of the theorem as follows. There are at most $(s + 2k + c)^s$ logically different first order formulas, where the constant c depends only on the first order language. Pick $n_1 < n_2 < n_3 \cdots$ so that $(s+2k+c)^s 2^{sn^{2k-1}} < 2^{n_s^{2k}/4}$. Construct the circuit family $\{C_n\}_{n\geq 1}$ of circuits of size at most $4n^k+2n+1$ and depth 5, such that for $s \geq 1$, C_{n_s} is not expressible by any first order formula of size s using at most $2k-1$ variables. By Claim 6 and 7 this is possible. The proof follows. $\square$

4 Non-expressibility in first order logic

The relationship that exists between AC^0 and first order logic gives a hope that one could use tools from first order logic to prove circuit lower bounds. Thus far, lower bounds on circuit size [5, 4] were used to prove non-expressibility of functions in first order logic, see e.g., [3].

The equivalence of two variable first order formulas with linear AC^0 is in particular intriguing. It would be of great interest to prove super-linear AC^0 lower bounds for certain regular languages which lie in AC^0, in particular the language $(c^*ac^*b)^*c^*$. Proving such lower bounds would have interesting consequences as this language is related to Integer Addition [8] and it is already known that it cannot be expressed by a two variable first order formula using the linear ordering $<$ on $[n]$ as the only numerical predicate [].

One of the most powerful and elegant proof techniques that first order logic has to offer are Ehrenfeucht-Fraïssé games. That is the tool which we use to prove our non-expressibility results. From our perspective, it should seemingly be easier to argue about two variable formulas than about full-scale first order logic. This intuition turns out to be true in our proofs. However, we fall short of providing dramatically simpler non-expressibility proofs than the one that are known even for "simple" cases of functions known to be outside of AC^0.

In fact, our technique is reminiscent of known techniques, [4, 5], which is not a pure coincidence. We discuss this issue more in Section 7. In this section we give our Ehrenfeucht-Fraïssé game argument for non-expressibility of PARITY in first order logic using formulas with two variables. In particular, we prove:

Theorem 8. *PARITY is not expressible by two variable first order formulas.*

As a consequence we obtain:

Corollary 9. *PARITY is not in linear AC^0.*

4.1 Ehrenfeucht-Fraïssé games

A tool for showing that a boolean function is not expressible in first order logic is that of *Ehrenfeucht-Fraïssé games*. In this section we consider a two pebble variant of Ehrenfeucht-Fraïssé games. A two pebble Ehrenfeucht-Fraïssé game is played by two players—*Spoiler* and *Duplicator*—on two structures A and A' of the same signature. The game proceeds in rounds. In each of the first two rounds of the game Spoiler picks one of the structures and places a new pebble on an arbitrary element of its universe, then Duplicator places another new pebble on an element of his choice of the other structure. All subsequent rounds proceed as follows. Spoiler picks one of the structures and moves the element that was played two rounds ago to another element of its universe. Then Duplicator moves the pebble played two rounds ago on the other structure to another element of its universe; Duplicator is also allowed to keep the pebble at the same location, i.e., do nothing. They alternate in moving pebbles and stop after at most k rounds, where k is a parameter of the game. After each round they check that the sub-structures induced by the two pebbled elements of each universe are isomorphic (with respect to their predicates). If not, Spoiler wins immediately. The Duplicator wins the game only if during all k rounds of the game Spoiler does not win.

A standard observation asserts that Spoiler has a winning strategy in a k round two pebble Ehrenfeucht-Fraïssé game on structures A and A' iff there is a two variable first order formula ϕ of quantifier depth k that is true on A but not on A' [7]. Hence to prove that a boolean function $f : \Sigma^+ \to \{0,1\}$ is not expressible by any two variable first order formula of quantifier depth k it suffices to show that for any structure $A = \langle [n], \overline{\sigma}, P_1, P_2, \ldots \rangle$ with n large enough there are two strings u and w such that $f(u) \neq f(w)$ and Duplicator has a winning strategy in the k round Ehrenfeucht-Fraïssé game on $A(u)$ and $A(w)$.

4.2 Game types

We want to use the existence of winning strategies for Duplicator in Ehrenfeucht-Fraïssé games to prove that certain boolean functions are not expressible in first order logic. It turns out that Duplicator has a winning strategy in an Ehrenfeucht-Fraïssé game if the structures A and A' on which the game is played are *similar* from the perspective of the game. *Game types* capture this perspective. Here we will define game types only for structures with unary and binary predicates. This is without loss of generality as any function that is expressible by a two variable first order formula is expressible by a two variable first order formula that uses only unary and binary predicates.

Let $n, k \geq 1$ be integers. Let A be a structure over a universe $U = [n]$ with signature $\langle r_1 + m, r_2 \rangle$. Let the numerical predicates of arity j be $R_{j,1}, R_{j,2}, \ldots, R_{j,r_j}$ and let $\overline{\sigma}$ be the input predicates. For arbitrary elements $v, u \in U$ define the *isomorphism type of* v to be

$$c^A(v) = R_{1,1}(v) \cdots R_{1,r_1}(v) R_{2,1}(v,v) \cdots R_{2,r_2}(v,v),$$

and the *isomorphism type of* v, u to be

$$\begin{aligned} c^A(v,u) \quad &= \quad c^A(v) c^A(u) R_{2,1}(v,u) \cdots R_{2,r_2}(v,u) \cdot \\ & \quad\quad R_{2,1}(u,v) \cdots R_{2,r_2}(u,v), \end{aligned}$$

where the product means concatenation. Clearly, each $c^A(v)$ can be viewed as a string from a set $C_1^A = \{\text{TRUE}, \text{FALSE}\}^{s_1^A}$, where $s_1^A = r_1 + r_2$, and each $c^A(v,u)$ can be viewed as a string from a set $C_2^A = \{\text{TRUE}, \text{FALSE}\}^{s_2^A}$, where $s_2^A = 2r_1 + 4r_2$.

For every $v \in U$ and integer $i \geq 0$ we define inductively the *i-th two pebble game type $\zeta_i^A(v)$ of element* v

$$\zeta_0^A(v) = \langle \overline{\sigma}(v), c^A(v) \rangle$$

and

$$\zeta_i^A(v) = \left\langle \overline{\sigma}(v), c^A(v), \left\{ \left\langle c^A(v,u), \zeta_{i-1}^A(u) \right\rangle ;\ u \in U \right\} \right\rangle .$$

We let the *k-th two pebble game type of the structure A* be $\zeta_k^A = \{\zeta_{k-1}^A(v);\ v \in U\}$.

The intuition behind these definitions is following. If two elements v and v' of two different first order structures have the same two pebble game type of order k then any k round two pebble Ehrenfeucht-Fraïssé game which starts by placing pebbles on v and v' by Spoiler and Duplicator, respectively, can be won by Duplicator. One can see this by induction, as Duplicator can maintain the invariant that the corresponding pebbled elements have always the same game types.

The number of two pebble game types of order 0 of a single element is at most $h_0^A = 2^m|C_1^A|$, the number of two pebble game types of order $i \geq 1$ of a single element is at most $h_i^A = |C_1^A|2^{m+|C_2^A|h_{i-1}^A}$ and the number of two pebble game types of order k of the structure A is at most $\widehat{h}_k^A = 2^{h_{k-1}^A}$. Note, these numbers depend only on the signature of A.

We can state the following proposition.

Proposition 10. *Let A and A' be two structures of the same signature and let $k \geq 1$ be an integer. There is a two variable first order formula ϕ of quantifier depth k such that $A \models \phi$ and $A' \not\models \phi$ if and only if $\zeta_k^A \neq \zeta_k^{A'}$.*

4.3 Our technique

Our goal is to show that certain functions $f : \Sigma^+ \to \{0,1\}$, e.g. PARITY, are not expressible by two variable first order formulas. In order to show that we will show that for any integer $k \geq 1$ and any sequence of structures $\{A_n\}_{n=1,\ldots}$ of the same signature $\langle r_1 + m, r_2 \rangle$, there exist an integer $n \geq 1$ and $u, w \in \Sigma^n$ such that $f(u) \neq f(w)$ and $\zeta_k^{A_n(u)} = \zeta_k^{A_n(w)}$.

Our strategy for constructing u and w will be as follows. We will pick a large enough integer n and we will find an assignment to a *small* part of the universe of A_n so that the k-th two pebble game type of A_n will already be determined by this partial assignment. That will mean that regardless of how we extend the partial assignment to an assignment σ for the whole universe of A_n, the k-th game type of $A_n(\sigma)$ will be the same. Hence, if among the possible extensions of our partial assignment there will be two assignments that correspond to strings u and w with $f(u) \neq f(w)$ then $\{A_n\}_{n=1,\ldots}$ cannot be used to represent f by two variable first order formulas.

We will need the following simple and intuitive definitions. A *partial assignment to universe* $[n]$ is a function $\sigma : [n] \to \Sigma \cup \{*\}$. A partial assignment σ *fixes* elements of $\sigma^{-1}(\Sigma)$ and leaves the other elements of the universe *unset*. The (partial) assignments σ, π are *compatible* if $\sigma(i) = \pi(i)$ whenever i is fixed by both σ and π. Furthermore, σ *extends* π if σ and π are compatible and $\sigma^{-1}(*) \subseteq \pi^{-1}(*)$. For compatible partial assignments σ and π, $\sigma \cup \pi$ denotes the common extension of σ and π that fixes exactly those elements of the universe that are fixed by σ or π.

Let $A = \langle [n], \overline{\sigma}, \ldots \rangle$ be a first order structure and let $1 \leq i < k$ be integers. For a partial assignment σ and an element $v \in [n]$, we define the *i-th two pebble partial game type of* v to be $\zeta_i^{A,\sigma}(v) = \{\zeta_i^{A(\pi)}(v);\ \pi$ is an assignment that extends $\sigma\}$. We say that a *partial two pebble game type $\zeta_i^{A,\sigma}(v)$ depends only on elements in $S \subseteq \sigma^{-1}(*)$* if $|\zeta_i^{A,\pi}(v)| = 1$ for every partial assignment π that extends σ and that fixes all elements in S. (There may be many different sets S such that $\zeta_i^{A,\sigma}(v)$ depends only on them. Think of $\zeta_i^{A,\pi}(v)$ as a set parametrized by π rather than just a set.) For a set $F \subseteq [n]$, we let $\zeta_i^{A,\sigma}(F) = \bigcup_{v \in F} \zeta_i^{A,\sigma}(v)$ and we say that *$\zeta_i^{A,\sigma}(F)$ depends only on elements in a set $S \subseteq \sigma^{-1}(*)$* if $\zeta_i^{A,\pi}(F) = \zeta_i^{A,\pi'}(F)$ for any two compatible extensions π and π' of σ that both fix all elements of S. We also say that a partial game type *$\zeta_i^{A,\sigma}(v)$ depends on at most l elements* if there exists $S \subseteq \sigma^{-1}(*)$ of size at most l such that $\zeta_i^{A,\sigma}(v)$ depends only on S; similarly for $\zeta_i^{A,\sigma}(F)$. The *k-th two pebble partial game type* of the structure A is $\zeta_k^{A,\sigma} = \zeta_{k-1}^{A,\sigma}([n])$.

The following lemma is the main result of this section.

Lemma 11. *Let $k \geq 1$ be an integer and $\{A_n\}_{n=1,\ldots}$ be a sequence of structures $A_n = \langle [n], \overline{\sigma}, \ldots \rangle$ of the same signature. There exists a constant $c > 0$ such that for any $n, l \geq 1$, there is a partial assignment $\sigma : [n] \rightarrow \Sigma \cup \{*\}$ such that $|\sigma^{-1}(\Sigma)| \leq n/l$ and for all $v \in [n]$, $\zeta_{k-1}^{A_n,\sigma}(v)$ depends on at most $cl^{3^{k-1}-1}$ elements of $[n]$.*

In this lemma we can choose l to be a function of n, e.g., $l(n) = n^{\epsilon}$. Lemma 11 implies Theorem 8.

Proof of Theorem 8. Let $\Sigma = \{0, 1\}$. Pick an arbitrary integer $k \geq 1$. We will show that PARITY cannot be expressed by any two variable first order formula of quantifier depth k. Let $\{A_n\}_{n\geq 1}$ be a family of first order structures. Let c be the constant guaranteed to exist by Lemma 11 and let $n > c3^{3^k} h_{k-1}^{A_n}$. By Lemma 11 there is a partial assignment σ that leaves at least $2n/3$ elements of n unset and so that for all $v \in [n]$, the $k-1$-th two pebble partial game type $\zeta_{k-1}^{A_n,\sigma}(v)$ depends on at most $c3^{3^{k-1}-1}$ elements of $[n]$. By fixing at most $c3^{3^{k-1}-1} h_{k-1}^{A_n}$ additional elements of $[n]$ we can fix $\zeta_k^{A_n,\sigma}$, i.e., $\zeta_k^{A_n,\sigma}$ will not depend on any element of $[n]$. (One by one for each game type of order $k-1$ that is in $\zeta_k^{A_n,\sigma}$ but which is not yet guaranteed to occur in $\zeta_k^{A_n(\pi)}$ for all extensions π of σ, enforce this game type by setting appropriately at most $c3^{3^{k-1}-1}$ elements of $[n]$.)

Now, for any two extensions of σ, assignments σ_u and σ_w, it will be true that $\zeta_k^{A_n(\sigma_u)} = \zeta_k^{A_n(\sigma_w)}$. Since σ leaves at least $n/3$ elements unset, we can pick an extension σ_u to represent a string of odd parity and an extension σ_w to represent a string of even parity. Let u and w be strings that correspond to σ_u and σ_w, respectively. Clearly, PARITY(u)$\neq$PARITY(w) but $\zeta_k^{A_n(u)} = \zeta_k^{A_n(w)}$, hence by Proposition 10, $\{A_n\}_{n\geq 1}$ cannot be used to represent PARITY in connection with any two variable formula of quantifier depth k. Since this is true for any k and any family of first order structures, PARITY cannot be represented by any two variable first order formula. $\square$

4.4 Proof of Lemma 11

In order to prove Lemma 11 we will prove the following switching lemma.

Lemma 12 (Two Pebble Switching Lemma)**.** *Let $n, k \geq 1$ be integers, $0 < \epsilon < 1$ be a real number and A be a first order structure with the universe of size n. Let σ be a partial assignment such that for all $v \in [n]$, $\zeta_{k-1}^{A,\sigma}(v)$ depends on at most l elements. Then there is an extension π of σ such that $|\pi^{-1}(*)| \geq |\sigma^{-1}(*)| - \epsilon n$ and for all $v \in [n]$, $\zeta_k^{A,\pi}(v)$ depends on at most $4\epsilon^{-2}|C_2^A|^2(h_{k-1}^A)^3 l^3$ elements.*

Recall, C_2^A is the set of possible isomorphism types on two elements, and h_{k-1}^A is our upper bound on the number of different two pebble game types of order $k-1$.

Proof of Lemma 12. Set $y = |C_2^A| \cdot (h_{k-1}^A)^2 \cdot l \cdot 2\epsilon^{-1}$ and $z = |C_2^A| \cdot h_{k-1}^A \cdot l \cdot 2\epsilon^{-1} \cdot y$. Initially we let $\pi = \sigma$ and later we will modify π in several iterations.

For every $v \in [n]$, set S_v to be a set of at most l elements so that $\zeta_{k-1}^{A,\sigma}(v)$ depends only on S_v. Furthermore, for every $s \in C_2^A$, define $F_{v,s} = \{T;\ \exists u \in [n],\ \{T\} = \zeta_{k-1}^{A,\pi}(u),\ c^A(v,u) = s\}$, hence, set $F_{v,s}$ contains game types that are guaranteed to occur in any game type from $\zeta_k^{A,\pi}(v)$ for some element u with $c^A(v,u) = s$. Furthermore, define $D_{v,s} = \{u;\ u \in [n],\ c^A(v,u) = s,\ \zeta_{k-1}^{A,\pi}(u) \setminus F_{v,s} \neq \emptyset\}$, so set $D_{v,s}$ contains elements that can still contribute by their $k-1$-st two pebble game type to the k-th game type of v. Clearly, $\zeta_k^{A,\pi}(v)$ depends only on $\bigcup_{s,\ u \in D_{v,s}} S_u$. That might be a large set though. For $\langle v, u \rangle \in [n] \times [n]$ we say that $\langle v, u \rangle$ are *dependent* if $u \in D_{v,c^A(v,u)}$.

We will perform two steps now, in each of them we will set at most $\epsilon n/2$ unset elements in π to 0 or 1. In the first step, we will achieve that for every element u, the number of elements v such that $\langle v, u\rangle$ are dependent will be at most y. In the second step, we will make sure that for every v, there are at most z elements u such that $\langle v, u\rangle$ are dependent. That will imply the theorem. As we change π we also change $F_{v,s}$'s and $D_{v,s}$'s to reflect the changes in π.

Step 1. Iteratively, till there is u such that $|\{\langle v, u\rangle \in [n]\times[n];\ \langle v, u\rangle \text{ are dependent}\}| \geq y$, do the following. Pick such u. For every $v \in [n]$ such that $\langle v, u\rangle$ are dependent, pick $T_v \in \zeta_{k-1}^{A,\pi}(u) \setminus F_{v,c^A(v,u)}$. Let T be the game type among T_v's, that is assigned to the largest number of elements v. Define π on $S_u \cap \pi^{-1}(*)$ so that $\zeta_{k-1}^{A,\pi}(u) = \{T\}$.

Observe that for every u which we deal with above, for at least y/h_{k-1}^A elements v, a new game type T is added into $F_{v,c^A(v,u)}$. For every element v, its $F_{v,s}$'s can be enlarged at most $|C_2^A|\cdot h_{k-1}^A$ times. Hence, at most $n\cdot|C_2^A|\cdot(h_{k-1}^A)^2/y$ elements u are dealt with, which leads to setting at most $n\cdot|C_2^A|\cdot(h_{k-1}^A)^2\cdot l/y = \epsilon n/2$ additional elements in π.

Step 2. Iteratively, till there is an element v such that $|\{\langle v, u\rangle \in [n]\times[n];\ \langle v, u\rangle \text{ are dependent}\}| \geq z$ do the following. Pick such v, and set π for at most $|C_2^A|\cdot h_{k-1}^A \cdot l$ elements of the universe, so that $|\tau_k^{A,\pi}(v)| = 1$.

There are at most $n\cdot y/z$ elements v for which this step will be performed. Hence, at most $\epsilon n/2$ elements w will be set. After the second step, all elements v depend on at most zl elements. □

The combinatorics of the proof of Lemma 12 is very much the same as in proofs of Chaudhuri and Jaikumar, [4]. Originally we independently proved a slightly weaker version of Lemma 12 using a different proof, and only later adopted the simpler combinatorics of Chaudhuri and Jaikumar for this paper.

Switching lemma 12 allows us to prove Lemma 11.

Proof of Lemma 11. Set

$$c = \prod_{i\in[k-1]} \left(4k^2\cdot|C_2^{A_2}|^2\cdot(h_{i-1}^{A_n})^3\right)^{3^{k-1-i}}.$$

We construct σ in $k-1$ iterations. Define $\sigma_0(i) = *$ for all $i \in [n]$. Let $l_0 = 1$ and $\epsilon = 1/(kl)$. Observe, for all v in the universe, $\zeta_0^{A_n,\sigma_0}(v)$ depends only on $\{v\}$. For $i = 1,\dots,k-1$ define $l_i = 4k^2\cdot|C_2^{A_n}|^2\cdot(h_{i-1}^{A_n})^3\cdot l_{i-1}^3\cdot l^2$. By Lemma 12 there is an extension σ_i of σ_{i-1} that sets at most ϵn additional elements of the universe so that for all $v\in[n]$, $\zeta_i^{A_n,\sigma_i}(v)$ depends on at most l_i elements. Setting $\sigma = \sigma_{k-1}$ implies the lemma. □

5 k-pebble Ehrenfeucht-Fraïssé games

In this section we consider the general variant of Ehrenfeucht-Fraïssé games, the k-pebble Ehrenfeucht-Fraïssé games. They are general enough so that one can show non-expressibility of certain functions in fist order logic. We will use k-pebble Ehrenfeucht-Fraïssé games to show the following claim.

Theorem 13. *PARITY is not expressible by any first order formula.*

Let $k \geq 3$ be an integer. A k-pebble Ehrenfeucht-Fraïssé game is again a game between Spoiler and Duplicator which is played on two structures A and A' of the same signature. The game proceeds in rounds. In each round Spoiler picks one of the structures and places a new pebble on an arbitrary element of its universe, then Duplicator places another new pebble on an element of his choice of the other structure. They alternate in placing pebbles and stop after exactly k rounds. At the end of the game we say that the *Duplicator* *won the game* if the sub-structures induced by the k pebbled elements of the two structures are isomorphic (with respect to their predicates); otherwise the *Spoiler won*.

Similarly to the two pebble variant of Ehrenfeucht-Fraïssé games, a standard observation asserts that the Spoiler has a winning strategy in the k-pebble Ehrenfeucht-Fraïssé game on structures A and A' iff there is a first order formula ϕ of quantifier depth k that is true on A but not on A'. Similarly to previous section, to prove that a boolean function $f : \Sigma^+ \to \{0,1\}$ is not expressible by first order formula of quantifier depth k it suffices to show that for any structure $A = \langle [n], \overline{\sigma}, P_1, P_2, \ldots \rangle$ with n large enough there are two strings u and w such that $f(u) \neq f(w)$ and Duplicator has a winning strategy in the k round Ehrenfeucht-Fraïssé game on $A(u)$ and $A(w)$.

5.1 k-pebble game types

We extend the definitions used in the previous section to k-pebble games. Similarly to the two pebble case, any atomic sub-formula of a first order formula of quantifier depth k with no free variable can involve at most k different variables. Hence, if a function is expressible by a first order formula of quantifier depth k then it is expressible by a first order formula of quantifier depth k that uses predicates of arity at most k. Let A be a structure over a universe $U = [n]$ with signature $\langle r_1 + m, r_2, \ldots, r_k \rangle$. Let the numerical predicates of arity j be $R_{j,1}, R_{j,2}, \ldots, R_{j,r_j}$ and let $\overline{\sigma}$ be the input predicates. For arbitrary elements $v_1, \ldots, v_i \in U$ define the *isomorphism type of* $v_1, \ldots, v_i$ to be

$$c^A(v_1, \ldots, v_i) = \prod_{\substack{j \in [k],\, \ell \in [r_j] \\ s:[j] \to [i]}} R_{j,\ell}(v_{s(1)}, v_{s(2)}, \ldots, v_{s(j)}),$$

where the product means concatenation in some fixed order of indices j, ℓ and s. Clearly, each $c^A(v_1, \ldots, v_i)$ can be viewed as a string from a set $C_i^A = \{\textsc{True}, \textsc{False}\}^{s_i^A}$, where $s_i^A = \sum_{j \in [k]} i^j \cdot r_j$. (Note, for $k = 2$ this definition coincides with the previous one.)

Furthermore, for arbitrary elements $v_1, \ldots, v_k \in U$, we define the *game type of elements* $v_1, \ldots, v_k$ recursively as follows

$$\tau_0^A(v_1, \ldots, v_k) = \big\langle \overline{\sigma}(v_k), c^A(v_1, \ldots, v_k) \big\rangle$$

and for $i \in [k-1]$, the *i-th game type of elements* $v_1, \ldots, v_{k-i}$ is

$$\begin{aligned} &\tau_i^A(v_1, \ldots, v_{k-i}) = \\ &\big\langle \overline{\sigma}(v_{k-i}), \{\tau_{i-1}^A(v_1, \ldots, v_{k-i+1});\ v_{k-i+1} \in U\} \big\rangle . \end{aligned}$$

The *k-th game type of structure* A is $\tau_k^A = \{\tau_{k-1}^A(v_1);\ v_1 \in U\}$. The number of different game types of order 0 of k elements is at most $g_{k,0}^A = 2^{m+s_k^A}$, the number of game types of order $i \in [k-1]$ of $k-i$ elements is at most $g_{k,i}^A = 2^{m+g_{k,i-1}^A}$, and the number of game types of order k of the structure A is at most $\widehat{g}_k^A = 2^{g_{k,k-1}^A}$. Note that these upper bounds depend only on the signature of the structure A.

As noted previously the following holds.

Proposition 14. *Let A and A' be two structures of the same signature and let $k \geq 1$ be an integer. There is a first order formula ϕ of quantifier depth k such that $A \models \phi$ and $A' \not\models \phi$ if and only if $\tau_k^A \neq \tau_k^{A'}$.*

Let $A = \langle [n], \overline{\sigma}, \ldots \rangle$ be a first order structure and let $1 \leq i < k$ be integers. For a partial assignment σ and elements $v_1, \ldots, v_{k-i} \in [n]$, we define the *$i$-th partial game type of* $v_1, \ldots, v_{k-i}$ to be $\tau_i^{A,\sigma}(v_1, \ldots, v_{k-i}) = \{\tau_i^{A(\pi)}(v_1, \ldots, v_{k-i});\ \pi \text{ is an assignment that extends } \sigma\}$. We say that a *partial game type $\tau_i^{A,\sigma}(v_1, \ldots, v_{k-i})$ depends only on elements in $S \subseteq \sigma^{-1}(*)$* if $|\tau_i^{A,\pi}(v_1, \ldots, v_{k-i})| = 1$ for every partial assignment π that extends σ and that fixes all elements in S. (There may be many different sets S such that $\tau_i^{A,\sigma}(v_1,\ldots,v_{k-i})$ depends only on them. Think of $\tau_i^{A,\pi}(v_1,\ldots,v_{k-i})$ as a set parametrized by π rather than just a set.) For a set $F \subseteq [n]$, we let $\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},F) = \bigcup_{v\in F}\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},v)$ and we say that $\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},F)$ *depends only on elements in a set* $S \subseteq \sigma^{-1}(*)$ if $\tau_{i-1}^{A,\pi}(v_1,\ldots,v_{k-i},F) = \tau_{i-1}^{A,\pi'}(v_1,\ldots,v_{k-i},F)$ for any two compatible extensions π and π' of σ that both fix all elements of S. We also say that a partial game type $\tau_i^{A,\sigma}(v_1,\ldots,v_{k-i})$ *depends on at most* l *elements* if there exists $S \subseteq \sigma^{-1}(*)$ of size at most l such that $\tau_i^{A,\sigma}(v_1,\ldots,v_{k-i})$ depends only on S; similarly for $\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},F)$. In a similar way we also define *k-th partial game types* $\tau_k^{A,\sigma} = \tau_{k-1}^{A,\sigma}([n])$.

The following lemma is the main result of this section.

Lemma 15. *Let $k \geq 1$ be an integer and $\{A_n\}_{n=1,\ldots}$ be a sequence of structures $A_n = \langle [n], \overline{\sigma}, \ldots\rangle$ of the same signature. There are constants $0 < \epsilon < 1$ and $l \geq 0$ such that for any n large enough, there is a partial assignment $\sigma : [n] \to \Sigma \cup \{*\}$ such that $|\sigma^{-1}(*)| \geq n^\epsilon$ and for any $v \in [n]$, $\tau_{k-1}^{A_n,\sigma}(v)$ depends on at most l elements of $[n]$.*

This lemma suffices to prove Theorem 13 that PARITY is not expressible by any first order formula. Since the proof of such a claim is essentially identical to the one for two variable formulas (Theorem 8, Section 4.3), we omit it here. To prove Lemma 15 we will first prove a switching lemma for k-pebble Ehrenfeucht-Fraïssé games by a technique similar to the one of [5].

Let $n \geq 1$ be an integer. For a set $S \subseteq [n]$ and probability $0 \leq p \leq 1$, we define $\mathcal{R}_{S,p}$ to be the random distribution of partial assignments $\sigma : [n] \to \Sigma \cup \{*\}$ such that for every $i \in S$ and $a \in \Sigma$, $\sigma(i)$ is assigned a independently at random with probability $(1-p)/m$ and $*$ with probability p, and for every $i \notin S$, $\sigma(i) = *$. Note, if $U, V \subseteq [n]$ are disjoint and $\sigma_U \in \mathcal{R}_{U,p}$ and $\sigma_V \in \mathcal{R}_{V,p}$ are taken independently at random then $\sigma_U \cup \sigma_V$ is distributed according to $\mathcal{R}_{U\cup V,p}$.

Lemma 16 (k-pebble Switching Lemma)**.** *Let $k \geq i > 0$, $k' \geq 1$ and $l \geq 0$ be integers and $0 < \epsilon < 1$ be a real number. There exist constants $l' \geq 0$ and $n_0 \geq 0$ such that if A is a first order structure with the universe of size $n \geq n_0$ then the following is true. Let $v_1, v_2, \ldots, v_{k-i}$ be in $[n]$ and let σ be a partial assignment such that for all $v \in [n]$, there exists a set $S_v \subseteq [n]$ of size at most l so that $\tau_{i-1}^{A,\sigma}(v_1,v_2,\ldots,v_{k-i},v)$ depends only on elements in S_v. Let $F \subseteq [n]$ be such that for every $v, w \in F$, $\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},v) = \tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},w)$. Let $S = \bigcup_{v\in F} S_v$. Then $\Pr_{\sigma_S\in\mathcal{R}_{S,1/n^\epsilon}}[\tau_{i-1}^{A,\sigma\cup\sigma_S}(v_1,\ldots,v_{k-i},F)$ depends on at most l' elements $] \geq 1 - 1/n^{k'}$.*

Proof of Lemma 16. Clearly, $\tau_{i-1}^{A,\sigma}(v_1,\ldots,v_{k-i},F)$ depends only on the elements of S. However, S may be arbitrarily large. Our goal is to argue that with a high probability a random partial assignment to elements of S according to $\mathcal{R}_{S,1/n^\epsilon}$ will make $\tau_{i-1}^{A,\sigma\cup\sigma_S}(v_1,\ldots,v_{k-i},F)$ depend only on few unset elements of S. The rough intuition is that either S is indeed large and one can essentially force all possible game types to appear in $\tau_{i-1}^{A,\sigma\cup\sigma_S}(v_1,\ldots,v_{k-i},F)$ or S is small and then almost all its elements will be fixed by σ_S. Either case will force $\tau_{i-1}^{A,\sigma\cup\sigma_S}(v_1,\ldots,v_{k-i},F)$ to depend only on a small number of elements.

The actual proof is by induction on l. For $l = 0$ the lemma is trivial. So assume that the lemma holds for all $l \leq t$ and we prove it for $l = t+1$. Let l'' be the constant l' guaranteed to exist by induction hypothesis for parameters $k \leftarrow k, i \leftarrow i, k' \leftarrow k'+1, l \leftarrow l-1$, and $\epsilon \leftarrow \epsilon$. Define $l' = m^{(k'+2)/\epsilon} 2^{g^A_{k,i-1}} l'' + (k'+2)/\epsilon$. Fix $k, k', i, v_1, \ldots, v_{k-i}$ and F. For a partial assignment π and $v \in [n]$, denote $\tau_{i-1}^{A,\pi}(v_1,v_2,\ldots,v_{k-i},v)$ by $\tau_v(\pi)$ and for a set $U \subseteq [n]$, let $\tau_U(\pi) = \bigcup_{v\in U}\tau_v(\pi)$ and $S_U = \bigcup_{v\in U} S_v$. Consider a maximal set $E \subseteq F$ such that for all distinct $v, w \in E$, $S_v \cap S_w = \emptyset$. There are two cases.

Case 1. $|E| \geq \log^2 n$. We will argue that with a high probability for $\sigma \cup \sigma_S$, all possible game types in $\tau_E(\sigma\cup\sigma_S)$ occur simultaneously at different elements in E, so $\tau_F(\sigma\cup\sigma_S)$ does not depend on any elements of the universe at all. For any $T \in \tau_E(\sigma)$ and any element $v \in E$, $\Pr_{\sigma_{S_v} \in \mathcal{R}_{S_v,1/n^\epsilon}}[\tau_v(\sigma \cup \sigma_{S_v}) = \{T\}] \geq (1/2m)^l$, provided that $n^\epsilon \geq 2$. Since S_v and S_w are disjoint for distinct $v, w \in E$, $\Pr_{\sigma_S \in \mathcal{R}_{S,1/n^\epsilon}}[\exists T \in \tau_E(\sigma);\ \forall v \in E;\ \tau_v(\sigma \cup \sigma_S) \neq \{T\}] \leq g^A_{k,i-1}(1 - (1/2m)^l)^{|E|} \leq 1/n^{k'}$, provided that n is large enough. Thus, in this case the lemma follows.

Case 2. $|E| < \log^2 n$. We will argue first that in this case, with a high probability for a random $\sigma_{S_E} \in \mathcal{R}_{S_E,1/n^\epsilon}$, σ_{S_E} leaves at most $(k'+2)/\epsilon$ elements in S_E unset. After fixing these unset elements (in every possible way) we will be able to use induction hypothesis for l smaller by one as S_v intersects S_E for every $v \in F$. That will allow us to conclude the argument. Observe:

$$\begin{aligned} &\Pr_{\sigma_{S_E} \in \mathcal{R}_{S_E,1/n^\epsilon}}[|S_E \cap \sigma^{-1}_{S_E}(*)| > (k'+2)/\epsilon] \leq \\ \leq\ & \binom{l \log^2 n}{\frac{k'+2}{\epsilon}} \left(\frac{1}{n^\epsilon}\right)^{\frac{k'+2}{\epsilon}} \\ \leq\ & \frac{1}{n^{k'+1}} \end{aligned}$$

Pick σ_{S_E} such that $|S_E \cap \sigma^{-1}_{S_E}(*)| \leq (k'+2)/\epsilon$. Let $S'_E = S_E \cap \sigma^{-1}_{S_E}(*)$. Pick an arbitrary partial assignment $\sigma_{S'_E}$ that fixes all elements in S'_E and leaves everything else unset. Clearly, for any $v \in E$, $|\tau_v(\sigma \cup \sigma_{S_E} \cup \sigma_{S'_E})| = 1$, and for all $v \in F \setminus E$, $\tau_v(\sigma \cup \sigma_{S_E} \cup \sigma_{S'_E})$ depends on at most $l-1$ elements, since S_v intersects S_E. Partition elements v in $F \setminus E$ into blocks $F_1, \dots, F_t$ according to their $\tau_v(\sigma \cup \sigma_{S_E} \cup \sigma_{S'_E})$ and apply induction hypothesis to each block of the partition with parameter k' set to $k'+1$, parameter l set to $l-1$, σ set to $\sigma \cup \sigma_{S_E} \cup \sigma_{S'_E}$ and ϵ, k and i unchanged. Then for every block F_j of the partition, $\Pr[\tau_{F_j}(\sigma \cup \sigma_{S_E} \cup \sigma_{S'_E} \cup \sigma_{S_{F_j} \setminus S_E})$ depends on at most l'' elements $] \geq 1 - 1/n^{k'+1}$, where the probability is taken over $\sigma_{S_{F_j} \setminus S_E}$ chosen at random according to $\mathcal{R}_{S_{F_j} \setminus S_E, 1/n^\epsilon}$.

For $\sigma_S \in \mathcal{R}_{S,1/n^\epsilon}$ we say that *a bad event B_S occurs* if either $|S_E \cap \sigma^{-1}_S(*)| > (k'+2)/\epsilon$, or $|S_E \cap \sigma^{-1}_S(*)| \leq (k'+2)/\epsilon$ and for some assignment $\sigma_{S'_E}$ of elements in $S_E \cap \sigma^{-1}_S(*)$, there is a block F_j in the partition of $F \setminus E$ according to $\tau_v(\sigma \cup \sigma'_S \cup \sigma_{S'_E})$ (where σ'_S agrees with σ_S on S_E and is unset elsewhere) such that $\tau_{F_j}(\sigma \cup \sigma''_S \cup \sigma_{S'_E})$ depends on more than l'' elements (where σ''_S agrees with σ_S on $S_E \cup S_{F_j}$ and is unset elsewhere).

There are at most $m^{(k'+2)/\epsilon}$ different assignments $\sigma_{S'_E}$ and there are at most $2^{g^A_{k,i-1}}$ blocks in every partition of $F \setminus E$. If B_S does not occur then $\tau_F(\sigma \cup \sigma_S \cup \sigma_{S'_E})$ depends on at most $2^{g^A_{k,i-1}} l''$ elements, hence, $\tau_F(\sigma \cup \sigma_S)$ depends on at most l' elements. Thus for n large enough, $\Pr_{\sigma_S \in \mathcal{R}_{S,1/n^\epsilon}}[\tau_F(\sigma \cup \sigma_S)$ does not depend on at most l' elements$] \leq \Pr_{\sigma_S \in \mathcal{R}_{S,1/n^\epsilon}}[B_S] \leq (1 + m^{(k'+2)/\epsilon} 2^{g^A_{k,i-1}})/n^{k'+1} \leq 1/n^{k'}$. Hence the lemma follows. □

We state the following useful proposition.

Proposition 17. *For every integers $k, l \geq 1$, a real number $0 < p < 1$, a first order structure $A = \langle [n], \sigma, \dots \rangle$, a partial assignment $\sigma : [n] \to \Sigma \cup \{*\}$, sets $U \subseteq V \subseteq \sigma^{-1}(*)$, $v_1, \dots, v_{k-i} \in [n]$ and a set $F \subseteq [n]$, the following is true:* $\Pr_{\sigma_U \in \mathcal{R}_{U,p}}[\tau^{A,\sigma \cup \sigma_U}_{i-1}(v_1, \dots, v_{k-i}, F)$ *depends on at most l elements*$] \leq \Pr_{\sigma_V \in \mathcal{R}_{V,p}}[\tau^{A,\sigma \cup \sigma_V}_{i-1}(v_1, \dots, v_{k-i}, F)$ *depends on at most l elements*$]$.

Since the proposition is trivial, we leave it without a proof.

Proof of Lemma 15. Let n be large enough. We construct σ in $k-1$ iterations. Define $\sigma_0(i) = *$ for all $i \in [n]$. Define $l_0 = 1$ and $\epsilon_0 = 1$ and further inductively for $i = 1, \dots, k-1$, $\epsilon_i = 3^{-i}$ and $l_i =$

$1 + 2^{g^A_{k,i-1}} l'_i$, where l'_i is the constant l' guaranteed to exist by Lemma 16 for the parameters set as follows: $k \leftarrow k,\ i \leftarrow i,\ k' \leftarrow k - i + 1,\ l \leftarrow l_{i-1}$ and $\epsilon \leftarrow \epsilon_{i-1}/2$.

For $i = 1, \ldots, k-1$, given that we already have a partial assignment σ_{i-1} we are going to construct σ_i. We assume that σ_{i-1} leaves at least $n^{\epsilon_{i-1}}$ elements of $[n]$ unset and that for all $v_1, \ldots, v_{k-i+1} \in [n]$, $\tau_{i-1}^{A,\sigma_{i-1}}(v_1, \ldots, v_{k-i+1})$ depends on at most l_{i-1} elements.

Let $S_i = \sigma_{i-1}^{-1}(*)$. We pick $\sigma_{S_i} \in \mathcal{R}_{S_i, 1/n^{\epsilon_{i-1}/2}}$ at random and we define $\sigma_i = \sigma_{i-1} \cup \sigma_{S_i}$. We claim that with probability at least $1/4$, σ_i leaves at least n^{ϵ_i} elements of n unset and that for any $v_1, \ldots, v_{k-i} \in [n]$, $\tau_i^{A,\sigma_i}(v_1, \ldots, v_{k-i})$ depends on at most l_i elements of $[n]$. Since that happens with a positive probability, we can fix a particular σ_i satisfying those properties.

Since $|S_i| \geq n^{\epsilon_{i-1}}$, the expected number of unset elements in $\sigma_{i-1} \cup \sigma_{S_i}$ is at least $n^{\epsilon_{i-1}}/n^{\epsilon_{i-1}/2} = n^{\epsilon_{i-1}/2}$. Hence by Chernoff bound

$$\Pr_{\sigma_{S_i} \in \mathcal{R}_{S_i, 1/n^{\epsilon_{i-1}/2}}} \left[|S_i \cap \sigma_{S_i}^{-1}(*)| \leq n^{\epsilon_{i-1}/3} \right] \leq 1/4,$$

for all n large enough. Thus, it suffices to show that $\Pr_{\sigma_{S_i}}[\forall v_1, \ldots, v_{k-i} \in [n];\ \tau_i^{A,\sigma_{i-1} \cup \sigma_{S_i}}(v_1, \ldots, v_{k-i})$ depends on at most l_i elements $] \geq 1/2$.

Consider arbitrary elements $v_1, \ldots, v_{k-i} \in [n]$. Partition all elements $v \in [n]$ into at most $2^{g^A_{k,i-1}}$ classes $F_1, \ldots, F_t$ according to $\tau_{i-1}^{A,\sigma_{i-1}}(v_1, \ldots, v_{k-i}, v)$. We know that $\tau_{i-1}^{A,\sigma_{i-1}}(v_1, \ldots, v_{k-i}, v)$ depends on at most l_{i-1} elements of the universe. We can apply Lemma 16 and Proposition 17 to obtain that $\Pr_{\sigma_{S_i} \in \mathcal{R}_{S_i, 1/n^{\epsilon_{i-1}/2}}}[\tau_{i-1}^{A,\sigma_{i-1} \cup \sigma_{S_i}}(v_1, \ldots, v_{k-i}, F_j)$ depends on at most l'_i elements $] \geq 1 - 1/n^{k-i+1}$, for all $j = 1, \ldots, t$.

It follows that $\Pr[\tau_i^{A,\sigma_{i-1} \cup \sigma_{S_i}}(v_1, \ldots, v_{k-i})$ depends on at most l_i elements $] \geq 1 - 2t/2n^{k-i+1} \geq 1 - 1/2n^{k-i}$, where the probability is taken over a random $\sigma_{S_i} \in \mathcal{R}_{S_i, 1/n^{\epsilon_{i-1}/2}}$. Since there are only n^{k-i} choices for $v_1, \ldots, v_{k-i}$, our claim follows. This finishes the proof of Lemma 15. $\square$

6 Uniform AC^0 and Ehrenfeucht-Fraïssé games

In previous sections we have considered expressibility of functions in first order logic with arbitrary numerical predicates and its relationship with AC^0. A more refined relationship was found between uniform version of AC^0 and first order logic than that provided by Proposition 1. In the definition of AC^0 we did not put any restriction on how hard it should be to actually construct individual circuits in a circuit family. Hence, AC^0 contains even some uncomputable functions. To eliminate this artifact, one often considers only *uniform* families of circuits. A circuit family $\{C_n\}_{n \geq 1}$ is *uniform* if there is a program P that on input $n \geq 1$ outputs circuit C_n. Depending on the resources we allow the program P to use and on how the circuit should be output we obtain different variants of uniformity.

In [3], Barrington et al. study different variants of uniformity for AC^0 circuits. They observe that an appropriate measure of uniformity for AC^0 circuits is DLOGTIME-*uniformity*. A circuit family $\{C_n\}_{n \geq 1}$ is DLOGTIME-*uniform* if there is a program P that on input $\langle n, i, j \rangle$, where n, i, j are integers represented in binary, outputs in time $O(\log n)$ the type of j-th gate of C_n and whether i-th gate is an input to it. (See [3] for more details.) Hence, by *uniform* AC^0 we will mean the class of functions that are computable by DLOGTIME-uniform constant depth polynomial size circuit families.

Barrington et al. also establish a connection between uniform AC^0 and first order logic with the BIT predicate. The BIT predicate is a binary predicate that on a structure $A = \langle [n], \overline{\sigma}, BIT \rangle$ is interpreted so that for $i, j \in [n]$, $BIT(i,j)$ is TRUE iff the i-th bit of the binary representation of j is set to one. As usual we will denote by $FO[BIT]$ the class of functions expressible by first order formulas using BIT as the only numerical predicate. Barrington et al. prove the following equivalence.

Proposition 18 ([3]). *A function f is in $FO[BIT]$ iff f is in uniform AC^0.*

Our proof technique in Sections 4 and 5 works against first order logic with arbitrary numerical predicates, and thus against non-uniform AC^0. Our Ehrenfeucht-Fraïssé game arguments in this case seem to be rather complex. Hence, the natural question arises whether arguments against $FO[BIT]$ would not be considerably simpler. The uniformity of AC^0 seems to be expressed very naturally in first order logic so could one take an advantage of that?

It turns out, possibly unsurprisingly, that in the case of two variable formulas with BIT the only predicate we can prove a substantial strengthening of Lemma 11.

Proposition 19. *Let $k \geq 1$ be an integer and $\{A_n\}_{n=1,\dots}$ be a sequence of structures $A_n = \langle [n], \overline{\sigma}, BIT\rangle$. There exists a constant c such that for all n large enough, there is a partial assignment $\sigma : [n] \to \Sigma \cup \{*\}$ which sets at most $\log^c n$ elements of the universe, such that $\zeta_k^{A,\sigma}$ does not depend on any element.*

The proof will appear in the full paper.

One might hope to be able to extend this proposition to an arbitrary number of variables. That would have very interesting consequences, e.g., in a construction of oracles that separate the polynomial hierarchy from PSPACE. Unfortunately it is not possible to extend this proposition to arbitrary number of variables as that would contradict a result of Ajtai [2] who constructs a uniform AC^0 circuit family for a certain approximate counting function. That function cannot be fixed by fixing a small number of inputs as a generalization of Proposition 19 would imply.

Despite this we think that Ehrenfeucht-Fraïssé games in the area of lower bounds for uniform AC^0 warrant more investigation.

7 Discussion: Circuit lower bounds via Ehrenfeucht-Fraïssé games

Our Ehrenfeucht-Fraïssé game arguments resemble very much classical arguments for circuit lower bounds. This is not completely a coincidence as in the end we have drawn inspiration for overcoming certain technical difficulties from the proofs of Furst, Saxe and Sipser, [5] and for this paper we have used the combinatorics of Chaudhuri and Jaikumar [4] in the proof of Lemma 12. Hence, contrary to our original hope, our Ehrenfeucht-Fraïssé game arguments are not simpler than classical lower bounds.

We tend to think that the fact that our Ehrenfeucht-Fraïssé game arguments are complex may not be just a coincidence, either. By looking back at our results we see that the internal structures of first order structures and circuits are closely related. Consider a simple example. We can embed a circuit C of size m into a first order structure A with its universe of size m by mapping each gate of the circuit into one element of the universe. We can add predicates to the structure which indicate types of gates and which gate is an input to which gate. (Compare with the proof of Lemma 4.) Consider also a partial assignment to this new structure which fixes its game type. Such a partial assignment closely corresponds to a partial assignment to circuit C which fixes each of its gates. (In the partial assignment to A we are indeed interested only in the setting of the elements that correspond to input gates of C.)

Hence, fixing the game type of A corresponds to fixing the output of every gate in C. But for a circuit there are only two ways to fix its gate—0 and 1. In the case of a first order structure there is enormous wealth of possible game types which can be fixed at every element. The complexity of a first order structure gets only magnified as we try to embed a circuit of size $O(n^k)$ into a structure on universe of size n (consider a proof of Proposition 1, [6].) We feel that from these facts stems an intrinsic complexity of Ehrenfeucht-Fraïssé game arguments based on the random restriction technique.

Thus it would be of great interest to devise an Ehrenfeucht-Fraïssé argument that would not be based on random restrictions. In particular, this could be feasible and of even greater interest in the context of first order logic with BIT as the only numerical predicate.

Dedication

This work is dedicated to Clemens, who did not live to see the final version of this paper. Clemens passed away after a short battle with cancer in April 2005. Clemens was a key partner in obtaining the results contained in this paper. He was a good mathematician, an inspiring teacher, a kind person.

Acknowledgements

The first and fourth authors greatly benefited from enlightening discussions with Arkadev Chattopadhyay and Mike Saks.

References

[1] M. Ajtai. Σ_1^1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.
[2] M. Ajtai. Approximate counting with uniform constant depth circuits. In *In J.-Y Cai, ed. Advances in Computational Complexity Theory, DIMACS Series in Disc. Math. and Theoret. Comp. Sci.*, pages 1–20, 1993.
[3] D. M. Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Sciences*, 41(3):274–306, Dec. 1990.
[4] S. Chaudhuri and J. Radhakrishnan. Deterministic restrictions in circuit complexity. In *Proceedings of the 28-th annual ACM symposium on Theory of computing*, pages 30–36, 1996.
[5] M. Furst, J. Saxe, and M. Sipser. Parity, circuits and the polynomial time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.
[6] N. Immerman. Languages that capture complexity classes. *SIAM J. of Computing*, 16(4):760–778, 1987.
[7] N. Immerman. *Descriptive complexity*. Springer, New York, 1999.
[8] M. Koucký, P. Pudlák, and D. Thérien. Bounded-depth circuits: Separating wires from gates. In *Proceedings of the 37-th annual ACM symposium on Theory of computing*, pages 257–265, 2005.
[9] C. Papadimitriou. *Computational complexity*. Addison-Wesley, New York, 1994.