DESCRIPTIVE COMPLEXITY OF FINITE STRUCTURES: SAVING THE QUANTIFIER RANK

OLEG PIKHURKO AND OLEG VERBITSKY

Abstract. We say that a first order formula Φ *distinguishes* a structure M over a vocabulary L from another structure M' over the same vocabulary if Φ is true on M but false on M'. A formula Φ *defines* an L-structure M if Φ distinguishes M from any other non-isomorphic L-structure M'. A formula Φ *identifies* an n-element L-structure M if Φ distinguishes M from any other non-isomorphic n-element L-structure M'.

We prove that every n-element structure M is identifiable by a formula with quantifier rank less than $(1-\frac{1}{2k})n+k^2-k+2$ and at most one quantifier alternation, where k is the maximum relation arity of M. Moreover, if the automorphism group of M contains no transposition of two elements, the same result holds for definability rather than identification.

The Bernays-Schönfinkel class consists of prenex formulas in which the existential quantifiers all precede the universal quantifiers. We prove that every n-element structure M is identifiable by a formula in the Bernays-Schönfinkel class with less than $(1-\frac{1}{2k^2+2})n+k$ quantifiers. If in this class of identifying formulas we restrict the number of universal quantifiers to k, then less than $n-\sqrt{n}+k^2+k$ quantifiers suffice to identify M and, as long as we keep the number of universal quantifiers bounded by a constant, at total $n-O(\sqrt{n})$ quantifiers are necessary.

§1. Introduction. Let M be a structure over a vocabulary L. A closed first order formula Φ with relation symbols in $L \cup \{=\}$ is either true or false on M. If M' is another L-structure isomorphic with M, then Φ is equally true or false on M and M'. On the other hand, if M is finite and M' is non-isomorphic with M, then there is a formula $\Phi_{M,M'}$ that is true on M and false on M'. As it is well known, for infinite structures this is not necessary true. In this paper, however, we deal only with finite structures. We call the number of elements of a structure M its *order*.

If a first order formula Φ is true on M but false on M', we say that Φ *distinguishes* M *from* M'. We say that Φ *defines* an L-structure M if Φ distinguishes M from any other non-isomorphic L-structure M'. Furthermore, a formula Φ *identifies* a finite L-structure M if Φ distinguishes M from any other non-isomorphic L-structure M' of the same order.

We address the question of how simple a formula identifying (defining) a finite structure can be. The complexity measure of a first order formula we use here is the quantifier rank, that is, the maximum number of nested quantifiers in a formula. Let $\mathrm{I}(M)$ (resp. $\mathrm{D}(M)$) denote the minimum quantifier rank of a formula identifying (resp. defining) a structure M. We will pay a special attention to formulas of restricted logical structure. The *alternation number* of a formula Φ is the maximum number of quantifier alternations over all possible sequences of nested quantifiers under the assumption that Φ is reduced to its negation normal form, i.e., all negations are assumed to occur only in front of atomic subformulas. By $\mathrm{I}_l(M)$ and $\mathrm{D}_l(M)$ we denote the variants of $\mathrm{I}(M)$ and $\mathrm{D}(M)$ for the class of formulas with alternation number at most l.

We will estimate $\mathrm{I}(M)$ and $\mathrm{D}(M)$ as functions of the order of M. The latter is denoted throughout the paper by n. A simple upper bound for $\mathrm{I}(M)$ is

$$\mathrm{I}_0(M) \le n.$$

Indeed, every structure M is identified by formula

$$\exists x_1 \ldots \exists x_n \left(\bigwedge_{1\le i<j\le n} x_i \ne x_j \wedge \Psi_M(x_1,\ldots,x_n) \right), \tag{1}$$

where Ψ_M is the conjunction that gives an account of all relations between elements of M and negations thereof. For example, if M consists of a single binary relation R^M on the set $\{1,\ldots,n\}$, then

$$\Psi_M = \bigwedge_{(i,j)\in R^M} R(x_i,x_j) \wedge \bigwedge_{(i,j)\notin R^M} \neg R(x_i,x_j).$$

It is an easy exercise to show that, if M has only unary relations, then $\mathrm{I}_0(M) \le (n+1)/2$. In [14] we prove the following results. If M has only unary and binary relations, then $\mathrm{I}_1(M) \le (n+3)/2$. In the particular case that M is an ordinary undirected graph, we are able to improve on the alternation number by showing that then $\mathrm{I}_0(M) \le (n+5)/2$. It is not hard to show that these bounds are tight up to a small additive constant. If M is a k-uniform hypergraph, we have the bound $\mathrm{I}_1(M) \le (1-1/k)n + 2k - 1$.

Here we continue the research initiated in [14] and prove a general upper bound

$$\mathrm{I}_1(M) < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2, \tag{2}$$

where k, here and throughout, denotes the maximum relation arity of the vocabulary L.

A simple upper bound for $\mathrm{D}(M)$ is

$$\mathrm{D}_1(M) \le n + 1.$$

An appropriate defining formula is

$$\exists x_1 \ldots \exists x_n \forall x_{n+1} \left(\bigwedge_{1 \le i < j \le n} (x_i \ne x_j) \ \wedge \ \bigvee_{i=1}^{n} (x_{n+1} = x_i) \ \wedge \ \Psi_M(x_1, \ldots , x_n) \right),$$

where Ψ_M is as in (1). The upper bound of $n + 1$ is generally best possible. For example, we have $\mathrm{D}\,(M_n) = n + 1$ if M_n consists of the single totally true unary relation or is a complete graph on n vertices. However, for a quite representative class of structures we are able to prove a better bound. We call a structure *irredundant* if its automorphism group contains no transposition of two elements. Similarly to (2), for any irredundant structure M we obtain

$$\mathrm{D}_1(M) < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 1. \tag{3}$$

This is a qualitative extension of a result in [14], where the bound $\mathrm{D}_1(M) \le n/2+2$ is proved for any irredundant structure M with maximum relation arity 2. On the other hand, there are simple examples of irredundant structures with $\mathrm{D}\,(M) \ge n/4$ (see Remark 4.4).

In fact, the bound $\mathrm{D}_1(M) < (1-\frac{1}{2k})n+k^2-k+2$ may not hold only for structures with a simple, easily recognizable property. Namely, given elements u and v of M, let us call them *similar* if the transposition of u and v is an automorphism of M. It turns out that, either we have the upper bound for $\mathrm{D}_1(M)$ or otherwise M has more than $(1 - \frac{1}{2k})n + (k - 1)^2$ pairwise similar elements. In the latter case we are able to easily compute the value of $\mathrm{D}\,(M)$ up to an additive constant of k. For graphs such a dichotomy result was obtained in [14].

Furthermore, we address the identification of finite structures by formulas of the simplest logical structure, namely, those in the *prenex normal form* (or *prenex formulas*). In this case the quantifier rank is just the number of quantifiers occurring in a formula. Let Σ_1 (resp. Π_1) consist of the existential (resp. universal) prenex formulas. Furthermore, let Σ_i (resp. Π_i) be the extension of $\Sigma_{i-1} \cup \Pi_{i-1}$ with prenex formulas whose quantifier prefix begins with $\exists$ (resp. with $\forall$) and has less than i quantifier alternations. In particular, Σ_2 is the well-known Bernays-Schönfinkel class of formulas (see [4] for the role of this class in finite model theory). Define $\mathrm{P}_i(M)$ to be the minimum number of quantifiers in a $\Sigma_i \cup \Pi_i$ formula identifying a structure M. Similarly, let $\mathrm{BS}\,(M)$ be the minimum number of quantifiers of an identifying formula in the Bernays-Schönfinkel class Σ_2. We hence have the following hierarchy:

$$\begin{gathered} \mathrm{I}\,(M) \le \mathrm{I}_{i-1}(M) \le \mathrm{P}_i(M) \le \mathrm{P}_{i-1}(M), \qquad i \ge 1; \\ \mathrm{P}_2(M) \le \mathrm{BS}\,(M) \le \mathrm{P}_1(M) \le n. \end{gathered} \tag{4}$$

The upper bound of n is here due to the identifying formula (2). The bound $\mathrm{P}_1(M) \leq n$ is generally best possible. It is attained, for example, if M consists of the single unary relation true on all but one elements of the structure.

Our concern becomes therefore $\mathrm{BS}\,(M)$, the next member at the top of the hierarchy (4). We prove that

$$\mathrm{BS}\,(M) < \left(1 - \frac{1}{2k^2+2}\right) n + k. \tag{5}$$

Though the multiplicative constant in (5) is worse than that in the bound (2), the bound (5) may be regarded as a qualitative strengthening of (2) because the class of formulas in the former result is much more limited than that in the latter result. Curiously, the bound (5) strengthens the bound (2) also quantitatively if we consider a somewhat unusual complexity measure of a formula, namely, the total number of quantifiers occurring in it.

If we restrict the number of universal quantifiers to a constant, Bernays-Schönfinkel formulas become much less powerful. Let $\mathrm{BS}_q(M)$ denote the minimum total number of quantifiers in a Bernays-Schönfinkel formula identifying M with at most q universal quantifiers. We prove that $\mathrm{BS}_k(M) < n - \sqrt{n} + k^2 + k$ and that $\mathrm{BS}_q(M) \geq n - O(\sqrt{n})$ as long as q is bounded by a constant.

To prove (2), we use the characterization of the quantifier rank of a formula distinguishing structures M and M' as the length of the *Ehrenfeucht game* on M and M' [3] (an essentially equivalent characterization in terms of partial isomorphisms between M and M' and extensions thereof is due to Fraïssé [5]). Unlike (2), our proof of (5) uses a direct approach. Nevertheless, both the results share the same background which is based on the notion of a base of a structure M.

Given a set X of elements of M and elements u and v of M, we say that X *separates* u and v if the extension of the identity map of X onto itself taking u to v is not a partial automorphism of M. Clearly, no X can separate similar u and v. On the other hand, if X separates every two non-similar elements in the complement of X, we call X a *base* of M. Every M trivially has $(n-1)$-element bases. Our technical results imply that a considerably smaller base always exists.[1]

Related work. Our paper is focused on the descriptive complexity of *individual* structures as opposed to the descriptive complexity of *classes* of structures. The latter is the subject of a large research area, which is emphasized much on the monadic second order logic (we refer the reader to the survey [4] and textbooks [2, 8]).

[1]In fact, we do not state this explicitly. However, it is easy to derive from the estimate (39) that every structure has a base with less than $(1 - \frac{1}{2k^2+1})n$ elements. On the other hand, there are structures whose all bases have at least $n/2$ elements. A simple example is given by the graph with m pairwise non-adjacent edges.

The identification of graphs in first order logic is studied in [9, 10, 1, 6, 7] in aspects relevant to computer science. The main focus of this line of research is on the minimum number of variables in an identifying formula, where formulas are in the first order language enriched by *counting* quantifiers. This complexity measure of a formula corresponds to the dimension of the Weisfeiler-Lehman algorithm that succeeds in finding a canonic form of a graph [1].

The present paper studies, in a sense, the worst case descriptive complexity of a structure. Two other possibilities, the "best" and average structures, are considered in [13] and [11] in the case of graphs.

Organization of the paper. In Section 2 we explain the notation used throughout the paper, recall some basic definitions, define the Ehrenfeucht game and state its connection to distinguishing non-isomorphic structures in first order logic. In Section 3 we introduce some relations, partitions, transformations, and constructions over a finite structure and explore their properties. The main task performed in this section is construction of a particular base in an arbitrary structure. We will benefit from these preliminaries while proving our both main results, bounds (2) and (5), in Sections 4 and 5 respectively. In Section 4 we also prove the bound (3) and the other definability results. Section 6 is devoted to identification by Bernays-Schönfinkel formulas with bounded number of universal quantifiers. In Section 7 we focus on graphs and improve the bound (5) for this class of structures. We conclude with a list of open problems in Section 8.

§2. Background.

2.1. Notation. Writing $\bar{u} \in U^k$ for a set U and a positive integer k, we mean that $\bar{u} = (u_1, \dots, u_k)$ with $u_i \in U$ for every $i \le k$. If $u, v \in U$, then $\bar{u}^{(uv)}$ denotes[2] the result of substituting v in place of every occurrence of u in $\bar{u}$ and substituting u in place of every occurrence of v in $\bar{u}$. Here (uv) denotes the transposition of u and v, that is, the permutation of U interchanging u and v and leaving the remaining elements unchanged. Given a function ϕ defined on U, we extend it over U^k by $\phi(\bar{u}) = (\phi(u_1), \dots, \phi(u_k))$ for $\bar{u} \in U^k$.

Notation id_U stands for the identity map of a set U onto itself. The domain and range of a function f are denoted by $\mathrm{dom}\, f$ and $\mathrm{range}\, f$ respectively. By $f^{(k)}$ we denote the k-fold composition of f.

2.2. Basic definitions. A *k-ary relation R on a set V* (or a *relation R of arity k*) is a function from V^k to $\{0, 1\}$. A *vocabulary* is a finite sequence $R_1, \dots, R_m$ of relation symbols along with a sequence $k_1, \dots, k_m$ of positive integers, where each

[2] The double use of the character u here should not be confusing: We will often use u to denote a single element of a sequence $\bar{u}$.

k_i is the arity of the respective R_i. If L is a vocabulary, a finite *structure* A *over* L (or an L-*structure* A) is a finite set $V(A)$, called the *universe*, along with relations $R_1^A, \ldots, R_m^A$, where R_i^A has arity k_i. The *order* of A is the number of elements in the universe $V(A)$. If $U \subseteq V(A)$, then A induces on U the structure $A[U]$ with the universe $V(A[U]) = U$ and relations $R_1^{A[U]}, \ldots, R_m^{A[U]}$ such that $R_i^{A[U]}\bar{a} = R_i^A\bar{a}$ for every $\bar{a} \in U^{k_i}$. Two L-structures A and B are *isomorphic* if there is a one-to-one map $\phi : V(A) \to V(B)$, called *an isomorphism from* A *to* B, such that $R_i^A\bar{a} = R_i^B\phi\bar{a}$ for every $i \le m$ and all $\bar{a} \in V(A)^{k_i}$. An *automorphism of* A is an isomorphism from A to itself. If $U \subseteq V(A)$ and $W \subseteq V(B)$, we call a one-to-one map $\phi : U \to W$ a *partial isomorphism from* A *to* B if it is an isomorphism from $A[U]$ to $B[W]$.

Without loss of generality we assume first order formulas to be over the set of connectives $\{\neg, \wedge, \vee\}$.

Definition 2.1. *A* sequence of quantifiers *is a finite word over the alphabet* $\{\exists, \forall\}$. *If* S *is a set of such sequences, then* $\exists S$ *(resp.* $\forall S$*) means the set of concatenations* $\exists s$ *(resp.* $\forall s$*) for all* $s \in S$. *If* s *is a sequence of quantifiers, then* $\bar{s}$ *denotes the result of replacement of all occurrences of* $\exists$ *to* $\forall$ *and vice versa in* s. *The set* $\bar{S}$ *consists of all* $\bar{s}$ *for* $s \in S$.

Given a first order formula Φ*, its set of* sequences of nested quantifiers *is denoted by* $\mathrm{Nest}(\Phi)$ *and defined by induction as follows:*

1) $\mathrm{Nest}(\Phi) = \{\lambda\}$ *if* Φ *is atomic, where* λ *denotes the empty word.*
2) $\mathrm{Nest}(\neg\Phi) = \overline{\mathrm{Nest}(\Phi)}$.
3) $\mathrm{Nest}(\Phi \wedge \Psi) = \mathrm{Nest}(\Phi \vee \Psi) = \mathrm{Nest}(\Phi) \cup \mathrm{Nest}(\Psi)$.
4) $\mathrm{Nest}(\exists x\Phi) = \exists\,\mathrm{Nest}(\Phi)$ *and* $\mathrm{Nest}(\forall x\Phi) = \forall\,\mathrm{Nest}(\Phi)$.

The quantifier rank *of a formula* Φ*, denoted by* $\mathrm{qr}(\Phi)$*, is the maximum length of a string in* $\mathrm{Nest}(\Phi)$.

Given a sequence of quantifiers s*, let* $\mathrm{alt}(s)$ *denote the number of occurrences of* $\exists\forall$ *and* $\forall\exists$ *in* s. *The* alternation number *of a first order formula* Φ *is the maximum* $\mathrm{alt}(s)$ *over* $s \in \mathrm{Nest}(\Phi)$.

Given an L-structure A and a closed first order formula Φ whose relation symbols are from $L \cup \{=\}$, we write $A \models \Phi$ if Φ is true on A and $A \not\models \Phi$ otherwise. Given A, a formula $\Psi(x_1, \ldots, x_m)$ with m free variables $x_1, \ldots, x_m$, and a sequence $a_1, \ldots, a_m$ of elements in $V(A)$, we write $A, a_1, \ldots, a_m \models \Psi(x_1, \ldots, x_m)$ if $\Psi(x_1, \ldots, x_m)$ is true on A with each x_i assigned the respective a_i.

If B is another L-structure, we say that a formula Φ *distinguishes* A *from* B if $A \models \Phi$ but $B \not\models \Phi$. We say that Φ *defines* an L-structure A (up to an isomorphism) if Φ distinguishes A from any non-isomorphic L-structure B. We say that Φ *identifies* an L-structure A of order n (up to an isomorphism in the class of L-structures of the same order) if Φ distinguishes A from any non-isomorphic L-structure B of order n.

By $\mathrm{D}(A,B)$ (resp. $\mathrm{D}_l(A,B)$) we denote the minimum quantifier rank of a formula (resp. with alternation number at most l) distinguishing a structure A from a structure B. By $\mathrm{D}(A)$ (resp. $\mathrm{D}_l(A)$) we denote the minimum quantifier rank of a formula defining A (resp. with alternation number at most l). By $\mathrm{I}(A)$ (resp. $\mathrm{I}_l(A)$) we denote the minimum quantifier rank of a formula identifying A (resp. with alternation number at most l).

LEMMA 2.2. *Let A be a finite structure over vocabulary L. Then the following equalities hold true:*

$$\begin{aligned} \mathrm{D}(A) &= \max\{\mathrm{D}(A,B) : B \ncong A\}, \\ \mathrm{D}_l(A) &= \max\{\mathrm{D}_l(A,B) : B \ncong A\}, \\ \mathrm{I}(A) &= \max\{\mathrm{D}(A,B) : B \ncong A,\ |V(B)| = |V(A)|\}, \\ \mathrm{I}_l(A) &= \max\{\mathrm{D}_l(A,B) : B \ncong A,\ |V(B)| = |V(A)|\}, \end{aligned}$$

where $\cong$ denotes the isomorphism relation between L-structures.

PROOF. We prove the first equality; The proof of the others is similar. Given an L-structure B non-isomorphic with A, let Φ_B be a formula of minimum quantifier rank distinguishing A from B, that is, $\mathrm{qr}(\Phi_B) = \mathrm{D}(A,B)$. Let $R = \max_B \mathrm{qr}(\Phi_B)$. We have $\mathrm{D}(A) \ge R$ because $\mathrm{D}(A) \ge \mathrm{D}(A,B)$ for every B. To prove the reverse inequality $\mathrm{D}(A) \le R$, notice that A is defined by the formula $\Phi = \bigwedge_B \Phi_B$ whose quantifier rank is R. The only problem is that Φ is an infinite conjunction (a $FO_{\infty\omega}$-formula). However, as it is well known, over a fixed finite vocabulary there are only finitely many inequivalent first order formulas of bounded quantifier rank (see e.g. [1, 2, 8]). We therefore can reduce Φ to a finite conjunction. ⊣

2.3. The Ehrenfeucht game. Let A and B be structures over the same vocabulary with disjoint universes. The r-round Ehrenfeucht game on A and B, denoted by $\mathrm{EHR}_r(A,B)$, is played by two players, Spoiler and Duplicator, with r pairwise distinct pebbles $p_1, \ldots, p_r$, each given in duplicate. Spoiler starts the game. A *round* consists of a move of Spoiler followed by a move of Duplicator. In the s-th round Spoiler selects one of the structures A or B and places p_s on an element of this structure. In response Duplicator should place the other copy of p_s on an element of the other structure. It is allowed to place more than one pebble on the same element. We will use a_s (resp. b_s) to denote the element of A (resp. B) occupied by p_s, irrespectively of who of the players places the pebble on this element. If after every of r rounds it is true that

$$a_i = a_j \text{ iff } b_i = b_j \text{ for all } i, j \le s,$$

and the component-wise correspondence between $(a_1, \ldots, a_s)$ and $(b_1, \ldots, b_s)$ is a partial isomorphism from A to B, this is a win for Duplicator; Otherwise the winner is Spoiler.

The l-*alternation* Ehrenfeucht game on A and B is a variant of the game in which Spoiler is allowed to switch from one structure to another at most l times during the game, i.e., in at most l rounds he can choose the structure other than that in the preceding round.

The following statement provides us with a robust technical tool.

LEMMA 2.3. *Let A and B be non-isomorphic structures over the same vocabulary.*

1) $\mathrm{D}(A, B)$ *equals the minimum r such that Spoiler has a winning strategy in* $\mathrm{EHR}_r(A, B)$.
2) $\mathrm{D}_l(A, B)$ *equals the minimum r such that Spoiler has a winning strategy in the l-alternation* $\mathrm{EHR}_r(A, B)$. $\dashv$

We refer the reader to [2, Theorem 1.2.8], [8, Theorem 6.10], or [16, Theorem 2.3.1] for the proof of the first claim and to [12] for the second claim.

§3. Exploring structural properties of finite structures.

3.1. A few useful relations. Throughout this section we are given an arbitrary finite structure M over vocabulary L. We abbreviate $V = V(M)$.

DEFINITION 3.1. *For $a, b \in V$ we write $a \sim b$ if the transposition (ab) is an automorphism of M. In other words, $a \sim b$ if, for every l-ary relation R of M, we have $R\bar{a} = R\bar{a}^{(ab)}$ for all $\bar{a} \in V^l$.*

LEMMA 3.2. *$\sim$ is an equivalence relation on V.*

PROOF. The relation is obviously reflexive and symmetric. The transitivity follows from the facts that the composition of automorphisms is an automorphism and that the transposition (ac) is decomposed into a composition of (ab) and (bc). $\dashv$

Given $X \subset V$, we will denote its complement by $\overline{X} = V \setminus X$.

DEFINITION 3.3. *Let $X \subset V$ and $a, b \in \overline{X}$. We write $a \equiv_X b$ if id_X extends to an isomorphism from $M[X \cup \{a\}]$ to $M[X \cup \{b\}]$. In other words, for every l-ary relation R of M, we have $R\bar{a} = R\bar{a}^{(ab)}$ for all $\bar{a} \in (X \cup \{a\})^l$.*

Furthermore, we write $a \approx_X b$ if the transposition (a, b) is an automorphism of $M[X \cup \{a, b\}]$. In other words, for every l-ary relation R of M, we have $R\bar{a} = R\bar{a}^{(ab)}$ for all $\bar{a} \in (X \cup \{a, b\})^l$.

Clearly, $a \approx_X b$ implies $a \equiv_X b$. It is also clear that $\equiv_X$ is an equivalence relation on $\overline{X}$. In contrast to this, simple examples show that $a \approx_X b$ is generally not an equivalence relation.

DEFINITION 3.4. *$\mathcal{C}(X)$ is the partition of $\overline{X}$ into $\equiv_X$-equivalence classes. Furthermore, $\mathcal{C}^m(X) = \{C \in \mathcal{C}(X) : |C| \le m\}$.*

The following lemma points some trivial but important properties of the partition $\mathcal{C}(X)$.

LEMMA 3.5.

1) *If $X_1 \subseteq X_2$, then $\mathcal{C}(X_2)$ is a refinement of $\mathcal{C}(X_1)$ on $\overline{X_2}$.*
2) *For any X, the $\sim$-equivalence classes restricted to $\overline{X}$ refine the partition $\mathcal{C}(X)$.* ⊣

In the sequel M' denotes another L-structure.

DEFINITION 3.6. *Let $\phi : X \to X'$ be a partial isomorphism from M to M'. Let $a \in \overline{X}$ and $a' \in \overline{X'}$. We write $a \equiv_\phi a'$ if ϕ extends to an isomorphism from $M[X \cup \{a\}]$ to $M'[X' \cup \{a'\}]$.*

LEMMA 3.7. *Let $\phi : X \to X'$ be a partial isomorphism from M to M'. Then the following claims are true.*

1) *Assume that $a \equiv_X b$ and $a' \equiv_{X'} b'$. Then $a \equiv_\phi a'$ iff $b \equiv_\phi b'$.*
2) *Assume that $a \equiv_\phi a'$ and $b \equiv_\phi b'$. Then $a \equiv_X b$ iff $a' \equiv_{X'} b'$.*
3) *Let $\bar\phi$ be a partial isomorphism from M to M' which is an extension of ϕ. If $a \in \operatorname{dom} \bar\phi \setminus X$, then $a \equiv_\phi \bar\phi(a)$.*
4) *Let $\bar\phi$ be a partial isomorphism from M to M' which is an extension of ϕ. Let $a, b \in \operatorname{dom} \bar\phi \setminus X$. Then $a \equiv_X b$ iff $\bar\phi(a) \equiv_{X'} \bar\phi(b)$.* ⊣

The proof is easy. Item 1 of the lemma makes the following definition correct.

DEFINITION 3.8. *Let $\phi : X \to X'$ be a partial isomorphism from M to M'. Let $C \in \mathcal{C}(X)$ and $C' \in \mathcal{C}(X')$. We write $C \equiv_\phi C'$ if $a \equiv_\phi a'$ for some (equivalently, for all) $a \in C$ and $a' \in C'$.*

3.2. A couple of useful transformations. Let M be a finite structure of order n with the maximum relation arity k. Let $X \subseteq V(M)$. We define two transformations that, if applicable to X, extend it to a larger set.

Transformation T: If there exists a set $S \subseteq \overline{X}$ with at most $k-1$ elements such that $|\mathcal{C}(X \cup S)| > |\mathcal{C}(X)|$, take the lexicographically first such S and set $T(X) = X \cup S$. Otherwise T is not applicable to X.

Transformation E: Apply T iteratively as long as it is applicable. The result is denoted by $E(X)$. In other words, $E(X) = T^{(n)}(X)$. If T is not applicable at all, set $E(X) = X$.

LEMMA 3.9. *Assume that T is not applicable to X. If $C \in \mathcal{C}(X) \setminus \mathcal{C}^2(X)$, then $a \approx_X b$ for every $a, b \in C$.*

PROOF. Let $C \in \mathcal{C}(X)$ and $|C| \geq 3$. Given a and b in C, we have to show that $a \approx_X b$. In other words, our task is, given an l-ary relation R of M and $\bar{a} \in (X \cup \{a, b\})^l$, to show that $R\bar{a} = R\bar{a}^{(ab)}$. If $\bar{a}$ contains no occurrence of a or no occurrence of b, this equality is true because $a \equiv_X b$. It remains to consider the case that $\bar{a}$ contains occurrences of both a and b.

Claim A. Let u, v, and w be pairwise distinct elements in C. Let R be an l-ary relation of M and $\bar{u} \in (X \cup \{u, v\})^l$ with occurrences of both u and v. Then $R\bar{u} = R\bar{u}^{(vw)}$.

Proof of Claim. If $R\bar{u} \neq R\bar{u}^{(vw)}$, then removal of u from C to X splits C into at least two $\equiv_{X\cup\{u\}}$-subclasses, containing v and w respectively. This contradicts the assumption that T is not applicable to X. ■

Let c be an arbitrary element in $C \setminus \{a, b\}$. Applying Claim A repeatedly three times, we obtain

$$R\bar{a} = R\bar{a}^{(bc)} = R(\bar{a}^{(bc)})^{(ab)} = R((\bar{a}^{(bc)})^{(ab)})^{(ac)} = R\bar{a}^{(bc)(ab)(ac)} = R\bar{a}^{(ab)},$$

as required. ⊣

LEMMA 3.10. $|E(X) \setminus X| \leq (k-1)|\mathcal{C}(E(X)) \setminus \mathcal{C}(X)|$. ⊣

3.3. The many-layered base of a finite structure.

DEFINITION 3.11. *Suppose that a finite structure M with maximum relation arity k is given. For $X \subset V(M)$, let $Y(X) = \bigcup_{C \in \mathcal{C}^{k+1}(X)} C$. We set*

$$\begin{aligned}
&X_0 = Y_0 = \emptyset,\\
&X_i = E(X_{i-1} \cup Y_{i-1}) \text{ for } 1 \leq i \leq k,\\
&Y_i = Y(X_i) \text{ for } 1 \leq i \leq k,\\
&X_{k+1} = X_k \cup Y_k,\\
&Z = V(M) \setminus X_{k+1}.
\end{aligned}$$

We will call X_{k+1} the base of *M.*

An important role of the base of a finite structure is due to the following fact (cf. the more general Definition 5.3).

LEMMA 3.12. *On Z the relations $\equiv_{X_k}$, $\equiv_{X_{k+1}}$, and $\sim$ coincide.*

PROOF. We start with relations $\equiv_{X_k}$ and $\sim$. Assume on the contrary that $a \equiv_{X_k} b$ but $a \not\sim b$ for some $a, b \in Z$. The latter means that, for some l-ary relation R of M and $\bar{a} \in V^l$ with at least one occurrence of a,

$$R\bar{a}^{(ab)} \neq R\bar{a}. \tag{6}$$

Denote $A = \{a_1, \dots , a_l\} \setminus \{a, b\}$. Since $|A| \leq k-1$ and the Y_i's are pairwise disjoint, there is $j \leq k$ such that

$$A \cap Y_j = \emptyset. \tag{7}$$

Remove all elements from $A \setminus X_j$ to X_j and set $X'_j = X_j \cup A$. Due to (6), this operation has the effect that

$$a \not\approx_{X'_j} b. \tag{8}$$

No class in $\mathcal{C}(X_j)$ can disappear completely: The classes in $\mathcal{C}^{k+1}(X_j)$ can only split up because of (7), the classes in $\mathcal{C}(X_j) \setminus \mathcal{C}^{k+1}(X_j)$ can lose up to $k-1$ elements and/or split up.

Since $a \equiv_{X_k} b$ and $a, b \in Z$, both a and b belong to the same $\equiv_{X_k}$-class C^* containing at least $k+2$ elements. Let C be the $\equiv_{X_j}$-class such that $C^* \subseteq C$. We now show that C is split up after modifying X_j and therefore $|\mathcal{C}(X'_j)| > |\mathcal{C}(X_j)|$, making a contradiction to the construction of X_j.

Indeed, if $a \not\equiv_{X'_j} b$, we have two subclasses containing respectively a and b. If $a \equiv_{X'_j} b$, it follows by Lemma 3.9 from (8) that the class in $\mathcal{C}(X'_j)$ containing a and b is exactly $\{a, b\}$. After removing at most $k-1$ elements, in C there remain at least 3 elements and therefore C must have at least one more $\equiv_{X'_j}$-subclass besides $\{a, b\}$.

Thus, on Z the relations $\equiv_{X_k}$ and $\sim$ are identical. By Item 1 of Lemma 3.5, on Z the relation $\equiv_{X_{k+1}}$ refines $\equiv_{X_k}$. By Item 2 of the same lemma the converse is also true. It follows that on Z the relations $\equiv_{X_{k+1}}$ and $\equiv_{X_k}$ also coincide. ⊣

Lemma 3.13. *Let n be the order of M and k be the maximum relation arity of M. We have*

$$\sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + \frac{|Z|}{2} > \frac{n}{2k} + \frac{1}{2} - \frac{1}{2k} \quad \text{if } k \geq 2 \tag{9}$$

and

$$2k \sum_{i=1}^{k-1} |\mathcal{C}^{k+1}(X_i)| + (k+1)|\mathcal{C}^{k+1}(X_k)| + (k-1)|\mathcal{C}(X_k)| + |Z| \geq n + k - 1. \tag{10}$$

Proof. By Lemma 3.10 we have

$$|X_1| \leq (k-1)(|\mathcal{C}(X_1)| - 1), \tag{11}$$

$$|X_i \setminus (X_{i-1} \cup Y_{i-1})| \leq (k-1)(|\mathcal{C}(X_i)| - |\mathcal{C}(X_{i-1} \cup Y_{i-1})|) \tag{12}$$

for $2 \leq i \leq k$. Note that

$$|\mathcal{C}(X_i)| = |\mathcal{C}^{k+1}(X_i)| + |\mathcal{C}(X_i) \setminus \mathcal{C}^{k+1}(X_i)|$$

and

$$|\mathcal{C}(X_i) \setminus \mathcal{C}^{k+1}(X_i)| \le |\mathcal{C}(X_i \cup Y_i)|$$

for $1 \le i \le k$. The latter inequality is true because, according to Item 1 of Lemma 3.5, the partition $\mathcal{C}(X_i \cup Y_i)$ is a refinement of $\mathcal{C}(X_i) \setminus \mathcal{C}^{k+1}(X_i)$. Combining it with (11) and (12), we obtain

$$|X_1| \le (k-1)(|\mathcal{C}^{k+1}(X_1)| + |\mathcal{C}(X_1 \cup Y_1)| - 1) \tag{13}$$

$$|X_i \setminus (X_{i-1} \cup Y_{i-1})| \le (k-1)(|\mathcal{C}^{k+1}(X_i)| + \mathcal{C}(X_i \cup Y_i) - |\mathcal{C}(X_{i-1} \cup Y_{i-1})|) \tag{14}$$

Summing up (13) and (14) over all $2 \le i \le k$, we have

$$|X_1| + \sum_{i=2}^{k} |X_i \setminus (X_{i-1} \cup Y_{i-1})| \le (k-1)\left(\sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + |\mathcal{C}(X_k \cup Y_k)| - 1\right). \tag{15}$$

According to Lemma 3.12,

$$\mathcal{C}(X_k \cup Y_k) = \mathcal{C}(X_k) \setminus \mathcal{C}^{k+1}(X_k) \tag{16}$$

and, as a consequence,

$$|\mathcal{C}(X_k \cup Y_k)| \le |Z|/(k+2). \tag{17}$$

From (15) we conclude, using (16), that

$$|X_1| + \sum_{i=2}^{k} |X_i \setminus (X_{i-1} \cup Y_{i-1})| \le (k-1)\left(\sum_{i=1}^{k-1} |\mathcal{C}^{k+1}(X_i)| + |\mathcal{C}(X_k)| - 1\right) \tag{18}$$

and, using (17), that

$$|X_1| + \sum_{i=2}^{k} |X_i \setminus (X_{i-1} \cup Y_{i-1})| \le (k-1)\left(\sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + \frac{|Z|}{k+2} - 1\right). \tag{19}$$

Notice also a trivial inequality

$$|Y_i| \le (k+1)|\mathcal{C}^{k+1}(X_i)|. \tag{20}$$

It is easy to see that

$$n = |X_1| + \sum_{i=2}^{k} |X_i \setminus (X_{i-1} \cup Y_{i-1})| + \sum_{i=1}^{k} |Y_i| + |Z|. \tag{21}$$

Using (18) and (20), we derive from (21) that

$$n \le 2k \sum_{i=1}^{k-1} |\mathcal{C}^{k+1}(X_i)| + (k+1)|\mathcal{C}^{k+1}(X_k)| + (k-1)|\mathcal{C}(X_k)| + |Z| - (k-1),$$

which implies (10). Using (19) and (20), we derive from (21) that

$$n \le 2k \sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + \left(2 - \frac{3}{k+2}\right) |Z| - (k-1), \tag{22}$$

which implies (9). ⊣

§4. Identifying finite structures with smaller quantifier rank.

THEOREM 4.1. *Let L be a vocabulary with maximum relation arity k. For every L-structure M of order n we have*

$$\mathrm{I}_1(M) < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2.$$

The proof takes the next two subsections. The case of $k = 1$ is an easy exercise and we will assume that $k \ge 2$. According to Lemma 2.2, it suffices to consider an arbitrary L-structure M' non-isomorphic with M and of the same order n, and estimate the value of $\mathrm{D}_1(M, M')$. We will design a strategy enabling Spoiler to win the Ehrenfeucht game on M and M' in less than $(1 - \frac{1}{2k})n + k^2 - k + 2$ moves with at most one alternation between the structures. This will give us the desired bound by Lemma 2.3.

4.1. Spoiler's strategy. The strategy splits play into $k+2$ phases. Spoiler will play almost all the time in M, possibly with one alternation from M to M' at the end of the game. For each vertex $v \in V(M)$ selected by Spoiler up to Phase i, let $\phi_i^*(v)$ denote the vertex in $V(M')$ selected in response by Duplicator. Thus, each subsequent ϕ_{i+1}^* extends ϕ_i^*. Provided Phase i has been already finished but the game not yet, ϕ_i^* is a partial isomorphism from M to M'. Under the same condition, it will be always the case that $\operatorname{dom} \phi_i^* \subseteq X_i$. We will use notation $\tilde{Y}_{i-1} = \operatorname{dom} \phi_i^* \cap Y_{i-1}$. Recall that the sets X_i and Y_i are defined by Definition 3.11 so that $Y_{i-1} \subset X_i$.

PHASE 1.
Spoiler selects all vertices in X_1. Let $X_1' = \phi_1^*(X_1)$.
END OF PHASE DESCRIPTION.

PHASE $j+1$, $1 \le j \le k$.
Our description of Phase $j+1$ is based on the assumption that Phase j is complete but the game is not finished yet and that the following conditions are true for every $1 \le i \le j$.

Condition 1: ϕ_i^* has a unique extension ϕ_i over the whole X_i that is a partial isomorphism from M to M'. Let $X_i' = \phi_i(X_i)$.

Condition 2: There is a one-to-one correspondence between the partitions $\mathcal{C}^{k+1}(X_{i-1})$ and $\mathcal{C}^{k+1}(X'_{i-1})$ such that, if $C' \in \mathcal{C}^{k+1}(X'_{i-1})$ corresponds to $C \in \mathcal{C}^{k+1}(X_{i-1})$, then $C \equiv_{\phi_{i-1}} C'$ and $|C| = |C'|$.

Condition 3: For every $C \in \mathcal{C}^{k+1}(X_{i-1})$, ϕ_i^* is defined on all but one elements of C. Denote $\tilde{C} = \operatorname{dom}\phi_i^* \cap C$. Then $\phi_i^*(\tilde{C}) \subset C'$, where C' corresponds to C according to Condition 2. Furthermore, ϕ_i takes the single element in $C \setminus \tilde{C}$ to the single element in $C' \setminus \phi_i^*(\tilde{C})$. Thus, $\phi_i(C) = C'$.

For the further references we denote the set $\phi_i(Y_{i-1}) = Y(X'_{i-1})$ by Y'_{i-1} and its subset $\phi_i^*(\tilde{Y}_{i-1})$ by $\tilde{Y}'_{i-1}$.

Condition 1 is true for $i = 1$ because ϕ_1^* is defined on the whole X_1. For the sake of technical convenience, we set $X'_0 = X_0 = \emptyset$. We suppose that $n > k + 1$ (otherwise Theorem 4.1 is trivially true). This implies that $\mathcal{C}^{k+1}(X_0) = \mathcal{C}^{k+1}(X'_0) = \emptyset$ and makes Conditions 2 and 3 for $i = 1$ trivially true. For $i > 1$ Conditions 1–3 follow by induction from Claim C below.

In the sequel we will intensively exploit the following notion. We say that a pair $(a, a') \in V(M) \times V(M')$ is *i-threatening* (for Duplicator) if a and a' are selected by the players in the same round after Phase i and

- $a \notin X_i$ or $a' \notin X'_i$,
- $a \not\equiv_{\phi_i} a'$.

We now start description of the phase. It consists of two parts.

Part 1. As long as no i-threatening pair arises for $1 \le i \le j$, Spoiler selects all but one elements in each class $C \in \mathcal{C}^{k+1}(X_j)$. The set of the vertices selected in C will be denoted by $\tilde{C}$. Furthermore, Spoiler selects all vertices in $X_{j+1} \setminus (X_j \cup Y_j)$. As soon as an i-threatening pair for some $1 \le i \le j$ arises, Spoiler switches to the strategy given by Claim B below and wins in at most $(i-1)(k-1)$ moves.

Part 2. Assume that Part 1 finishes and Duplicator still does not lose. Then, if Spoiler is able to win in at most k next moves irrespective of Duplicator's strategy, he does so and the game finishes. If he is not able to win but able in at most k moves to enforce creating an i-threatening pair for some $i \le j$, he does so and wins in at most $(i-1)(k-1)$ subsequent moves using the strategy of Claim B. Otherwise Phase $j+1$ is complete and the next Phase $j+2$ starts.

End of phase description.

Claim A. Let $i \le k + 1$. Suppose that Phase i is finished and Conditions 1–3 are met for i and all its preceding values. Assume that $a \in V(M)$ and $a' \in V(M')$ are selected by the players in the same round after Phase i and neither of them has been selected before. If

- $a \in X_i$ but $a' \neq \phi_i(a)$

or

- $a' \in X'_i$ but $a \neq \phi_i^{-1}(a')$,

then the pair (a, a') is m-threatening for some $m < i$.

Proof of Claim. Let m, $1 \le m < i$, be the largest index such that neither $a \in X_m$ nor $a' \in X'_m$. Then $a \in X_{m+1}$ or $a' \in X'_{m+1}$. We consider the former case (the analysis of the latter case is symmetric). By Condition 3, $a \in Y_m \setminus \tilde{Y}_m$ and the relation $a \equiv_{\phi_m} x$ holds for the only $x = \phi_{m+1}(a)$. We have $a' \neq \phi_i(a) = \phi_{m+1}(a)$ (the latter equality is due to the uniqueness of the ϕ_i's ensured by Condition 1). Therefore $a \not\equiv_{\phi_m} a'$, which means that (a, a') is m-threatening. ∎

Claim B. Assume that Phase j, $j \le k+1$, finishes, Conditions 1–3 for all $i \le j$ are met, and the game is going on. Let $1 \le i \le j$. As soon as after Phase j an i-threatening pair (a, a') arises, Spoiler is able to win in at most $(i-1)(k-1)$ moves playing all the time, at his own choice, either in M or in M'.

Convention. Given a relation $R = R^M$ of M, we will denote the respective relation $R^{M'}$ by R'.

Proof of Claim. We proceed by induction on i. For $i = 1$ the claim easily follows from Item 3 of Lemma 3.7. Let $i \ge 2$ and assume that the claim is true for all preceding values $1, 2, \ldots, i-1$.

We focus on the case that $a \notin X_i$ (in the case that $a' \notin X'_i$ the proof is given by the symmetric argument). The non-equivalence $a \not\equiv_{\phi_i} a'$ can happen in two situations.

Case 1: $a' \in X'_i$. Clearly, $a \neq \phi_i^{-1}(a')$ and therefore, by Claim A, the pair (a, a') is m-threatening for some $m < i$. By the induction hypothesis, Spoiler is able to win in at most $(m-1)(k-1)$ moves.

Case 2: $a' \notin X'_i$. Then the non-equivalence $a \not\equiv_{\phi_i} a'$ means that there is an l-ary relation of M and $\bar{a} \in (X_i \cup \{a\})^l$ with at least one occurrence of a such that

$$R\bar{a} \neq R'\psi\bar{a}, \tag{23}$$

where ψ is the map defined by $\psi(x) = \phi_i(x)$ for all x in $A = \{a_1, \ldots, a_l\} \setminus \{a\}$ and by $\psi(a) = a'$. Thus, ψ is not a partial isomorphism from M to M'. Hence, if $A \subseteq \operatorname{dom} \phi_i^*$, then Spoiler wins immediately.

Assume that $\hat{A} = A \setminus \operatorname{dom} \phi_i^*$ is nonempty. Spoiler selects all unselected elements in $\hat{A}$, if he wants to play in M, or in $\phi_i(\hat{A})$, if he prefers to play in M'. This takes at most $k-1$ moves. Suppose that Spoiler plays in M (for M' the argument is symmetric). If for every $b \in \hat{A}$ its counterpart in $V(M')$ is $\phi_i(b)$, this is Spoiler's win by (23). If some $b \in \hat{A}$ has the counterpart b' such that $b' \neq \phi_i(b)$, by Claim A there arises an m-threatening pair for some $m < i$. Applying the induction hypothesis for the index m, we conclude that Spoiler is able to win in at most $(m-1)(k-1)$

moves, having made altogether at most $(k-1)+(m-1)(k-1) \le (i-1)(k-1)$ moves. ■

Claim C. Assume that Phase j, $j \le k$, has been finished and Conditions 1–3 for all $i \le j$ are met. Assume furthermore that Part 1 of Phase $j+1$ finishes and the game is still going on. Then either Conditions 1–3 hold true for $i = j+1$ as well or Spoiler is able to win or to create an i-threatening pair for some $i \le j$ in at most k moves with at most one alternation from M to M' (and hence he is able to win in Part 2 of Phase $j+1$).

Proof of Claim. Assuming that Spoiler is unable to win or to create an i-threatening pair, we check Conditions 1–3.

Condition 2. The following two facts take place, for else Spoiler would be able to enforce creating a j-threatening pair in at most one move:

- For every $C' \in \mathcal{C}^{k+1}(X'_j)$ there is $C \in \mathcal{C}^{k+1}(X_j)$ such that $C \equiv_{\phi_j} C'$. (Otherwise Spoiler selects an elements in C' that violates this condition and a j-threatening pair arises whatever Duplicator's response.)
- For every $C \in \mathcal{C}^{k+1}(X_j)$ there is $C' \in \mathcal{C}^{k+1}(X'_j)$ such that $C \equiv_{\phi_j} C'$ and $|C'| \ge |C|-1$. (Otherwise, for some C, $\phi^*_{j+1}(\tilde{C})$ cannot be included into the respective C'. Therefore $c \not\equiv_{\phi_j} \phi^*_{j+1}(c)$ for at least one $c \in \tilde{C}$, providing us with a j-threatening pair.)

Thus, there is a one-to-one correspondence between $\mathcal{C}^{k+1}(X_j)$ and $\mathcal{C}^{k+1}(X'_j)$ such that, for C and C' corresponding to one another, $C \equiv_{\phi_j} C'$, $|C'| \ge |C|-1$, and $\phi^*_{j+1}(\tilde{C}) \subseteq C'$. Moreover, it actually holds $|C'| = |C|$ because, if $|C'| \ge |C|+1$, Spoiler could select 2 vertices in $C' \setminus \phi^*_{j+1}(\tilde{C})$ obtaining a j-threatening pair whatever Duplicator's response.

Conditions 1 and 3. By Condition 1 for $i = j$, the partial isomorphism ϕ^*_{j+1} can be extended on X_j only to ϕ_j and then it remains undefined within X_{j+1} only on $Y_j \setminus \tilde{Y}_j$. Define an extension ϕ_{j+1} of ϕ^*_{j+1} on the whole X_{j+1} so that ϕ_{j+1}

- agrees with ϕ_j on X_j,
- agrees with ϕ^*_{j+1} on $\tilde{Y}_j$, and
- for each $C \in \mathcal{C}^{k+1}(X_j)$, takes the single element in $C \setminus \tilde{C}$ to the single element in $C' \setminus \phi^*_{j+1}(\tilde{C})$, where C' corresponds to C according to Condition 2 that we have already proved.

We have to show that ϕ_{j+1} is a partial isomorphism from M to M' and no other extension of ϕ^*_{j+1} is such.

Assume that ϕ_{j+1} is not a partial isomorphism and get a contradiction to the assumption that Spoiler can in the nearest k moves neither win nor create an i-threatening pair. For some l-ary relation of M and $\bar{a} \in X_{j+1}^l$, we should have

$$R\bar{a} \neq R'\phi_{j+1}\bar{a}. \tag{24}$$

As a consequence, $A = \{a_1, \dots, a_l\}$ is not included into $\operatorname{dom} \phi^*_{j+1}$ for else ϕ^*_{j+1} would not be a partial isomorphism, contradicting the assumption that the game is still going on. Let Spoiler select all elements in $\hat{A} = A \setminus \operatorname{dom} \phi^*_{j+1}$. If for $b \in \hat{A}$ Duplicator always responds with $\phi_{j+1}(b)$, he loses by (24). Otherwise, let b be an element in $\hat{A}$ to which Duplicator responds with $b' \neq \phi_{j+1}(b)$. If $b \in X_j$ or $b' \in X'_j$, then we have $b' \neq \phi_j(b)$ because ϕ_{j+1} extends ϕ_j, . By Claim A, (b, b') is an i-threatening pair for some $i < j$. If $b \in X_{j+1} \setminus X_j$ and $b' \in X'_{j+1} \setminus X'_j$, then $b \not\equiv_{\phi_j} b'$ by Condition 2 proved above and the definition of ϕ_{j+1}. Thus, (b, b') is j-threatening. We have a contradiction in any case and therefore ϕ_{j+1} is a partial isomorphism from M to M' indeed.

To prove the uniqueness of the extension ϕ_{j+1} (i.e., Condition 1), assume that $\hat{\phi}_{j+1}$ is another extension of ϕ^*_{j+1} over X_{j+1} which is a partial isomorphism and differs from ϕ_{j+1} at $b \in Y_j \setminus \tilde{Y}_j$. Let $b' = \phi_{j+1}(b)$ and $b'' = \hat{\phi}_{j+1}(b)$. By Condition 2 proved above,

$$b' \not\equiv_{X'_j} b''. \tag{25}$$

By Condition 1 for $i = j$, $\hat{\phi}_{j+1}$ on X_j coincides with ϕ_j. Thus, the composition $\hat{\phi}_{j+1}\phi^{-1}_{j+1}$ takes b' to b'', extends $\mathrm{id}_{X'_j}$, and is an automorphism of $M'[X'_{j+1}]$. This makes a contradiction to (25). ∎

Claim C implies by an easy induction on j from 1 to $k+1$ that, for each $1 \leq j \leq k$, unless Spoiler wins in Phase j or earlier, Conditions 1–3 assumed in our description of Phase $j+1$ are indeed true. For analysis of the concluding phase, we state simple consequences of Claims A–C.

Claim D. Suppose that Spoiler follows the strategy designed above (Duplicator's strategy does not matter). Assume that Duplicator survives up to Phase $k+1$. Then the following claims are true.

1) Conditions 1–3 hold true for all $i \leq k+1$.
2) When in further play Spoiler selects $v \in V(M) \cup V(M')$, we denote Duplicator's response by $\psi(v)$. As long as there arises no i-threatening pair for any $i \leq k$,

it holds

$$\psi(v) \equiv_{\phi_k} v \ \text{ if } \ v \notin X_k \cup X'_k, \tag{26}$$

$$\psi(v) = \phi_{k+1}(v) \ \text{ if } \ v \in X_{k+1}, \tag{27}$$

$$\psi(v) = \phi^{-1}_{k+1}(v) \ \text{ if } \ v \in X'_{k+1}. \tag{28}$$

(The relations in (26) and (27)–(28) are equivalent on $(X_{k+1} \cup X'_{k+1}) \setminus (X_k \cup X'_k)$.)

Proof of Claim. Item 1 follows from Claim C by an easy inductive argument. Regarding Item 2, note that, if (26) were false, $(v, \psi(v))$ would be a k-threatening pair. If (27) or (28) were false, $(v, \psi(v))$ would be an i-threatening pair for some $i \leq k$ on the account of Claim A. ∎

Concluding Phase (Phase $k+2$).

We here assume that Phases from 1 up to $k+1$ have been finished without Spoiler's win and therefore Items 1 and 2 of Claim D hold true. As soon as there arises an i-threatening pair for some $i \leq k$, Spoiler switches to the strategy given by Claim B and wins in at most $(k-1)^2$ moves. As long as there occurs no such pair, Spoiler follows the strategy described below. The strategy depends on which of the following three cases takes place.

Case 1: There is a one-to-one correspondence between $\mathcal{C}(X_k)$ and $\mathcal{C}(X'_k)$ such that, if C and C' correspond to one another, then $C \equiv_{\phi_k} C'$ and, moreover, $|C| = |C'|$. By Item 1 of Claim D, such correspondence does exist between $\mathcal{C}^{k+1}(X_k)$ and $\mathcal{C}^{k+1}(X'_k)$ in any case.

Let Υ be the set of maps $\phi : V(M') \to V(M)$ such that

- ϕ is one-to-one,
- ϕ extends ϕ^{-1}_{k+1},
- for every $C' \in \mathcal{C}(X'_k)$, we have $\phi(C') \in \mathcal{C}(X_k)$ and $\phi(C') \equiv_{\phi_k} C'$.

Claim E. Assume that ϕ and ψ are in Υ. Let R be an l-ary relation of M. Then $R\phi\bar{a}' = R\psi\bar{a}'$ for all $\bar{a}' \in V(M')^l$.

Proof of Claim. The product $\psi\phi^{-1}$ is a permutation of $V(M)$ that moves only elements in Z. Moreover, $\psi\phi^{-1}$ preserves the partition $\mathcal{C}(X_k) \setminus \mathcal{C}^{k+1}(X_k)$ of Z and therefore $\psi\phi^{-1}$ is decomposed into the product of permutations π_C over $C \in \mathcal{C}(X_k) \setminus \mathcal{C}^{k+1}(X_k)$, where each π_C acts on the respective C. Since every π_C is decomposable into a product of transpositions, we have $\psi\phi^{-1} = \tau_1\tau_2\ldots\tau_t$ with τ_i being a transposition of two elements both in some C. It is easy to see that $\psi\bar{a}' = (\ldots((\phi\bar{a}')^{\tau_t})\ldots)^{\tau_1}$. By Lemma 3.12, each application of τ_i does not change the initial value of $R\phi\bar{a}'$. Therewith we arrive at the desired equality $R\phi\bar{a}' = R\psi\bar{a}'$. ∎

To specify Spoiler's strategy, we fix $\phi \in \Upsilon$ arbitrarily. Since M and M' are nonisomorphic, ϕ is not an isomorphism from M' to M, that is,

$$R\phi\bar{a}' \neq R'\bar{a}' \tag{29}$$

for some l-ary relation R' of M' and $\bar{a}' \in V(M')^l$. This inequality implies that the set $A' = \{a'_1, \ldots, a'_l\}$ is not included into X'_{k+1}. Spoiler selects, one by one, elements of $\hat{A} = A' \setminus \operatorname{range} \phi^*_{k+1}$. For Spoiler's move v, let $\psi(v)$ denote Duplicator's response.

Assume first that

$$\begin{gathered} \psi(v) \equiv_{\phi_k} v \ \text{ whenever } \ v \notin X'_k \\ \text{and} \\ \psi(v) = \phi^{-1}_{k+1}(v) \ \text{ whenever } \ v \in X'_{k+1}. \end{gathered} \tag{30}$$

Due to (30), we are able to extend ψ, initially defined on $\hat{A}$, to a map in Υ. Fix a such extension. By Claim E, $R\phi\bar{a}' = R\psi\bar{a}'$ and, by (29), Spoiler wins. If (30) is violated for some $v \in \hat{A}$, by Item 2 of Claim D this produces an i-threatening pair for $i \le k$ and therefore Spoiler wins in at most $(k-1)^2$ moves, having made altogether at most $k + (k-1)^2$ moves.

Case 2: There is no one-to-one correspondence between $\mathcal{C}(X_k)$ and $\mathcal{C}(X'_k)$ such that, if C and C' correspond to one another, then $C \equiv_{\phi_k} C'$. Spoiler selects an element in C or C' that has no counterpart. If Duplicator responds with a vertex outside $X_k \cup X'_k$, there arises a k-threatening pair. If Duplicator responds with a vertex in $X_k \cup X'_k$, there arises an i-threatening pair for $i < k$ by Item 2 of Claim D. This allows Spoiler to win altogether in at most $1 + (k-1)^2$ moves.

Case 3: There is a one-to-one correspondence between $\mathcal{C}(X_k)$ and $\mathcal{C}(X'_k)$ such that, if C and C' correspond to one another, then $C \equiv_{\phi_k} C'$. However, there are $C \in \mathcal{C}(X_k)$ and $C' \in \mathcal{C}(X'_k)$ such that $C \equiv_{\phi_k} C'$ but $|C| \neq |C'|$.

Call a class $C \in \mathcal{C}(X_k)$ *useful* if $C \equiv_{\phi_k} C'$ but $|C| \neq |C'|$. The description of Case 3 tells us that there is at least one useful class. Actually, since $|V(M)| = |V(M')|$, there are at least two useful classes, C_1 and C_2. Note that $|C_1| + |C_2| \le |Z|$. Without loss of generality, assume that $|C_1| \le |Z|/2$. Let C'_1 be the counterpart of C_1 in $\mathcal{C}(X'_k)$, i.e., $C_1 \equiv_{\phi_k} C'_1$. In the larger of C_1 and C'_1 Spoiler selects $\min\{|C_1|, |C'_1|\} + 1$ elements. Duplicator is enforced to at least once reply not in the smaller class. By Item 2 of Claim D, this produces an i-threatening pair and Spoiler, according to Claim B, wins in at most $(k-1)^2$ subsequent moves, having made altogether at most $|Z|/2 + 1 + (k-1)^2$ moves.

End of description of the concluding phase

4.2. Estimation of the length of the game. If Spoiler follows the above strategy and Duplicator delays his loss as long as possible, the end of the game is always this: Spoiler enforces creating a threatening pair in at most k moves and then wins in at most $(k-1)^2$ next moves using the strategy of Claim B. Let us calculate the smallest possible (optimal for Duplicator) number of elements in M unoccupied till such final stage of the game. The minimum is attained if all Phases from 1 up to $k+2$ are played and in Phase $k+2$ it happens Case 3. Then the number of elements unoccupied in X_{k+1} is equal to

$$\sum_{i=1}^{k} |Y_i \setminus \tilde{Y}_i| = \sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)|.$$

The number of elements unoccupied in Z is at least $|Z| - (|Z|/2+1) = |Z|/2 - 1$. By Lemma 3.13, the total number of unoccupied elements is at least

$$\sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + \frac{|Z|}{2} - 1 > \frac{n}{2k} - \frac{1}{2} - \frac{1}{2k}.$$

Thus, the maximum possible number of occupied elements is less than

$$\left(1 - \frac{1}{2k}\right) n + \frac{1}{2} + \frac{1}{2k}.$$

Summing up, we conclude that our strategy allows Spoiler to win in less that

$$\left(1 - \frac{1}{2k}\right) n + k^2 - k + 2$$

moves. Theorem 4.1 is proved.

4.3. Definability results. A natural question is if our approach applies to defining rather than identifying formulas. In fact, the proof of Theorem 4.1 implies the definability with lower quantifier rank for a quite representative class of structures.

4.3.1. *Definability of irredundant structures.*

DEFINITION 4.2. *If M is a finite structure, let*

$$\sigma(M) = \max\{\,|A| : A \subseteq V(M) \text{ such that } a_1 \sim a_2 \text{ for every } a_1, a_2 \in A\}$$

be the maximum cardinality of a $\sim$-equivalence class in $V(M)$.

If $\sigma(M) = 1$, i.e., no transposition of two elements is an automorphism of M, we call M irredundant.

THEOREM 4.3. *Let M be an irredundant structure of order n with maximum relation arity k. Then*

$$\mathrm{D}_1(M) < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 1.$$

PROOF. It is not hard to see that an irredundant structure whose all relations are unary is definable by a formula with quantifier rank 1. Assume therefore that $k \geq 2$. Notice that Spoiler's strategy described in Section 4.1 applies for any pair of L-structures M and M' of arbitrary orders with the only exception of Case 3 in the concluding Phase $k+2$, where the equality $|V(M)| = |V(M')|$ is supposed. Since the set Z is partitioned into $\sim$-equivalence classes each consisting of at least $k+2$ elements, for an irredundant structure M we have $Z = \emptyset$. Consequently, $V(M) = X_{k+1}$. It follows that either Spoiler wins at latest in Phase $k+1$ or, according to Item 1 of Claim D, there is a partial isomorphism ϕ_{k+1} from M to M' with $\operatorname{dom} \phi_{k+1} = V(M)$.

In the latter case, since M and M' are non-isomorphic, there is at least one element $v \in V(M') \setminus \operatorname{range} \phi_{k+1}$. In the concluding phase of the game Spoiler selects v and, according to Item 2 of Claim D, there arises a k-threatening pair. Spoiler switches to the strategy given by Claim B and wins in at most $(k-1)^2$ moves.

It remains to estimate the length of the game. Similarly to Section 4.2, we conclude that Spoiler needs at most $n - \sum_{i=1}^{k} |\mathcal{C}^{k+1}(X_i)| + k + (k-1)^2$ to win. By estimate (22), where $|Z| = 0$, this number is less than $(1 - \frac{1}{2k})n + k^2 - k + 1$. ⊣

REMARK 4.4. *There are simple examples of irredundant structures M showing a lower bound $\mathrm{D}(M) \geq n/4$. For example, let F be a directed graph on two vertices u and v consisting of a single (directed) edge (uv). Let G be another directed graph on u and v consisting of two edges, (uv) and the loop (uu). Denote the disjoint union of a copies of F and b copies of G by $aF+bG$. It is easy to see that $aF+bG$ is irredundant for any a and b. Directed graphs $M = mF + mG$ and $M' = (m-1)F + (m+1)G$ are non-isomorphic and both have order $4m$. An obvious strategy for Duplicator in the Ehrenfeucht game on M and M' shows that $\mathrm{D}(M, M') \geq m$.*

Theorem 4.3 will be considerably strengthened in the next subsections. In particular, it will be surpassed by Theorem 4.11.

4.3.2. *A further refinement.* As we observed in the proof of Theorem 4.3, Spoiler's strategy designed in Section 4.1 ensures the bound

$$\mathrm{D}_1(M, M') < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2. \tag{31}$$

for M' of *any* order under an additional condition imposed on M. We are able to describe exceptional pairs of non-isomorphic M and M' for which (31) may not hold much more precisely. Assume that M' has order $n' \geq n$. As was already mentioned, the assumption that $n' = n$ is used only in Case 3 of the concluding Phase $k+2$. Turning back to this case, we see that what is actually used is the existence of at least two useful classes in $\mathcal{C}(X_k)$. Thus, (31) may not hold in the only case that there is a unique useful class $C_0 \in \mathcal{C}(X_k)$. Since actually $C_0 \in \mathcal{C}(X_k) \setminus \mathcal{C}^{k+1}(X_k)$, we have $|C_0| \geq k+2$. By Lemma 3.12, the class C_0 consists of pairwise $\sim$-equivalent elements.

Let C_0' be the counterpart of C_0 in $\mathcal{C}(X_k')$, i.e., $C_0' \equiv_{\phi_k} C_0$. Given $B \subseteq C_0'$ with $|B| = |C_0|$, let $M_B' = M'[V(M') \setminus (C_0' \setminus B)]$. Consider an arbitrary map $\phi : V(M_B') \to V(M)$ extending ϕ_{k+1}^{-1}, mapping each $C' \in \mathcal{C}(X_k') \setminus \{C_0'\}$ onto its $\equiv_{\phi_k}$-counterpart in $\mathcal{C}(X_k)$, and mapping B onto C_0. As in Case 1 of Phase $k+2$, we see that Spoiler is able to win within the bound of (31) unless ϕ is an isomorphism from M_B' to M. From here we easily arrive at the following conclusion.

Lemma 4.5. *Let L be a vocabulary with maximum relation arity k. Let M and M' be non-isomorphic L-structures of orders n and n' respectively and $n \leq n'$. Then the bound*

$$\mathrm{D}_1(M, M') < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2$$

may be false only if there is a set $C_0 \subseteq V(M)$ with $|C_0| \geq k+2$ consisting of pairwise $\sim$-equivalent vertices and there is a partial isomorphism ψ from M to M' defined on $V(M) \setminus C_0$ whose any injective extension is a partial isomorphism from M to M'.

In the next subsection we make a constructive interpretation of the condition appearing in the lemma.

4.3.3. *Cloning an element of a structure.* **Notation.** Recall that, given a set V and a function π defined on V, we extend π over V^l, where $l \geq 1$, by $\pi\bar{u} = (\pi(u_1), \ldots, \pi(u_l))$ for any $\bar{u} = (u_1, \ldots, u_l)$ with all u_i in V. In particular, this concerns the case that π is a permutation of elements of V. Recall also that, if $\pi = (v_1 v_2)$ is a transposition, then we may write $\bar{u}^{(v_1 v_2)}$ in place of $\pi\bar{u}$.

Definition 4.6. *Given $v \in V(M)$, let $[v]_M = \{u \in V(M) : u \sim v\}$ be the $\sim$-equivalence class of the element v.*

We now introduce an operation of expanding a class $[v]_M$, i.e., adding to M new elements $\sim$-equivalent to v. This operation was considered in [14] in the particular case of uniform hypergraphs.

Let L be a vocabulary with maximum relation arity k. Below K and M are L-structures, v is an element of M, and t is a non-negative integer.

Definition A The notation $K = M \oplus tv$ means that the following conditions are fulfilled.

A1: $V(M) \subseteq V(K)$ and $|V(K)| = |V(M)| + t$.
A2: $K[V(M)] = M$.
A3: $|[v]_M| \geq k$.
A4: $[v]_K = [v]_M \cup (V(K) \setminus V(M))$.

Definition B The notation $K = M \oplus tv$ means that the following conditions are fulfilled.

B1: $V(M) \subseteq V(K)$ and $|V(K)| = |V(M)| + t$.

B2: There is $C \subseteq [v]_M$ with $|C| \geq k$ such that every injective extension of $\mathrm{id}_{V(M)\setminus C}$ to a map $\psi : V(M) \to V(K)$ is a partial isomorphism from M to K.

Definition C The notation $K = M \oplus tv$ means that the following conditions are fulfilled.

C1: $V(M) \subseteq V(K)$ and $|V(K)| = |V(M)| + t$.

C2: $|[v]_M| \geq k$.

C3: Let R be an l-ary relation in L. If $\bar{u} \in V(M)^l$, then $R^K\bar{u} = R^M\bar{u}$.

C4: Let R be an l-ary relation in L. Assume that $\bar{u} \in V(K)^l$ and the set $\{u_1, \ldots, u_l\} \setminus V(M) = \{w_1, \ldots, w_p\}$ is nonempty. Then $R^K\bar{u} = 1$ iff there are pairwise distinct elements $v_1, \ldots, v_p \in [v]_M \setminus \{u_1, \ldots, u_l\}$ such that $R^M\pi\bar{u} = 1$ for $\pi = (w_1v_1)\cdots(w_pv_p)$.

LEMMA 4.7. *Definitions A, B, and C are equivalent.*

PROOF. *Conditions A1–A4 imply Conditions B1–B2.* Since B1 coincides with A1, we only have to derive B2. We are actually able to prove B2 for an arbitrary $C \subseteq [v]_M$ with $|C| \geq k$ (there is at least one such C by A3). Let ψ be as specified in B2. For any l-ary relation R in L and $\bar{u} \in V(M)^l$, we have to check that $R^M\bar{u} = R^K\psi\bar{u}$. Assume that in $\{\psi(u_1), \ldots, \psi(u_l)\}$ there are p elements from $V(K) \setminus V(M)$ and denote them by $w_1, \ldots, w_p$. Take arbitrary pairwise distinct $v_1, \ldots, v_p \in C \setminus \{\psi(u_1), \ldots, \psi(u_l)\}$. Let $\tilde{u} = \pi\psi\bar{u}$ with $\pi = (w_1v_1)\cdots(w_pv_p)$. By A4, we have $v_i \sim w_i$ in K for all $i \leq p$. It follows that $R^K\psi\bar{u} = R^K\tilde{u}$. Since $\tilde{u} \in V(M)^l$, by A2 we have $R^K\tilde{u} = R^M\tilde{u}$. Notice now that $\tilde{u}$ and $\bar{u}$ coincide at the positions occupied by elements in $V(M) \setminus C$, while elements in C are permuted according to some permutation τ, i.e., $\tilde{u} = \tau\bar{u}$. Since τ is decomposable in a product of transpositions and elements of C are pairwise $\sim$-equivalent in M, we have $R^M\tilde{u} = R^M\bar{u}$, completing derivation of B2.

Conditions B1–B2 imply Conditions C1–C4. For C1 and C2 this is trivial. C3 immediately follows from B2 if we take $\psi = \mathrm{id}_{V(M)}$. Let us focus on C4. Let $\bar{u}$ and $w_1, \ldots, w_p$ be as specified in this condition. Assume first that $R^K\bar{u} = 1$. Take $v_1, \ldots, v_p \in C \setminus \{u_1, \ldots, u_l\}$ being pairwise distinct and define ψ by $\psi(v_i) = w_i$ for $i \leq p$ and $\psi(x) = x$ for all other $x \in V(M)$. Notice that $\psi^{-1}\bar{u} = \pi\bar{u}$ for $\pi = (w_1v_1)\cdots(w_pv_p)$. As ψ is a partial isomorphism by B2, we conclude that $R^M\pi\bar{u} = R^K\bar{u} = 1$. This proves C4 in one direction. Such a way of proving $R^M\pi\bar{u} = R^K\bar{u}$ will be referred to as *ψ-argument*.

For the other direction, assume that $R^M\pi\bar{u} = 1$ for $\pi = (w_1v_1)\cdots(w_pv_p)$ with some $v_1, \ldots, v_p \in [v]_M \setminus \{u_1, \ldots, u_l\}$. If all v_i are in C, the equality $R^K\bar{u} = 1$ follows from the ψ-argument with the same ψ as above. Otherwise, we can replace each v_i with some $v'_i \in C$, where $v'_1, \ldots, v'_p$ are pairwise distinct elements of $C \setminus \{u_1, \ldots, u_l\}$ and $v'_i = v_i$ whenever $v_i \in C$. For no i this replacement changes the initial value of $R^M\pi\bar{u}$ and, after all replacements are done, we have $R^M\pi'\bar{u} = 1$ with $\pi' = (w_1v'_1)\cdots(w_pv'_p)$. Defining ψ' by $\psi'(v'_i) = w_i$ and $\psi'(x) = x$ elsewhere on $V(M)$, we obtain $R^K\bar{u} = R^M\pi'\bar{u} = 1$ by the ψ'-argument.

Conditions C1–C4 imply Conditions A1–A4. Since A1–A3 are virtually the same as C1–C3, our concern is A4. It is easy to see that $[v]_K \cap V(M)$ cannot be larger than $[v]_M$. Therefore, it suffices to show that in K we have $v \sim v'$ for any $v' \in [v]_M \cup (V(K) \setminus V(M))$. Given an l-ary relation R in L and $\bar{u} \in V(K)^l$, we have to check that

$$R^K\bar{u} = R^K\bar{u}^{(vv')}.$$

We do it by routine examination of several cases. Note that, if neither v nor v' occurs in $\bar{u}$, then there is nothing to prove.

To simplify notation, denote

$$\hat{u} = \bar{u}^{(vv')}.$$

Furthermore, let $U = \{u_1, \ldots, u_l\}$ and $U \setminus V(M) = \{w_1, \ldots, w_p\}$. Denote the set of elements in $\hat{u}$ by $\hat{U}$.

Case 1: $v' \in V(K) \setminus V(M)$.

Subcase 1.1: $v \in U$, $v' \in U$.

Assuming $R^K\bar{u} = 1$, we will infer $R^K\hat{u} = 1$. This will give also the converse implication because $\bar{u}$ is supposed arbitrary with occurrences of both v and v' and we hence can take $\hat{u}$ instead of $\bar{u}$. Without loss of generality, assume that $v' = w_p$. By C4, there are $v_1, \ldots, v_p \in [v]_M \setminus U$ such that $R^M\pi\bar{u}$ with $\pi = (w_1v_1)\cdots(w_{p-1}v_{p-1})(v'v_p)$. As easily seen, $\pi\hat{u} = (\pi\bar{u})^{(vv_p)}$. Since $v_p \sim v$ in M, we have $R^M\pi\hat{u} = 1$. Note that $\hat{U} = U$ and hence $v_1, \ldots, v_p \in [v]_M \setminus \hat{U}$. By C4, we conclude that $R^K\hat{u} = 1$, as desired.

Subcase 1.2: $v \in U$, $v' \notin U$.

Note that $\hat{U} \setminus V(M) = \{w_1, \ldots, w_p, v'\}$ and $[v]_M \setminus \hat{U} = ([v]_M \setminus U) \cup \{v\}$. We first assume that $R^K\bar{u} = 1$ and infer from here that $R^K\hat{u} = 1$. Let $v_1, \ldots, v_p$ be as ensured by Condition C4 for $\bar{u}$, that is, $R^M\pi\bar{u} = 1$ with $\pi = (w_1v_1)\cdots(w_pv_p)$. Let $\pi' = \pi(v'v)$. As easily seen, $\pi'\hat{u} = \pi\bar{u}$. Thus, $R^M\pi'\hat{u} = R^M\pi\bar{u} = 1$ and, by C4, we conclude that $R^K\hat{u} = 1$.

We now assume that $R^K\hat{u} = 1$ and have to infer $R^K\bar{u} = 1$. According to C4, there are pairwise distinct $v'_1, \ldots, v'_{p+1} \in [v]_M \setminus \hat{U}$ such that $R^M\pi'\hat{u} = 1$ with $\pi' = (w_1v'_1)\cdots(w_pv'_p)(v'v'_{p+1})$. Choose pairwise distinct $v_1, \ldots, v_p$ in $\{v'_1, \ldots, v'_{p+1}\} \setminus \{v\}$

and apply to $\bar{u}$ the substitution $\pi = (w_1v_1)\cdots(w_pv_p)$. It is not hard to see that $\pi\bar{u} = \tau\pi'\hat{u}$ for τ being a permutation of the set $V = \{v, v'_1, \ldots, v'_p, v'_{p+1}\}$ taking v'_i to v_i for $i \le p$ and v'_{p+1} to v. A such τ exists because elements in $\{v'_1, \ldots, v'_{p+1}\}$ and in $\{v_1, \ldots, v_p, v\}$ are pairwise distinct (the fact that the two sets may intersect does not matter). Since τ is decomposable in a product of transpositions of two elements from V and elements in V are pairwise $\sim$-equivalent in M, we have $R^M\pi\bar{u} = R^M\pi'\hat{u} = 1$. By C4, we conclude that $R^K\bar{u} = 1$, as desired.

Subcase 1.3: $v \notin U$, $v' \in U$.

This subcase reduces to Subcase 1.2 by considering $\hat{u}$ in place of $\bar{u}$.

Case 2: $v' \in [v]_M$.

Since in this case v and v' are interchangeable, it suffices to assume that $v \in U$ and prove that $R^K\bar{u} = 1$ implies $R^K\hat{u} = 1$. Note that $\hat{U} \setminus V(M) = \{w_1, \ldots, w_p\}$.

Subcase 2.1: $v' \in U$.

Note that $[v]_M \setminus \hat{U} = [v]_M \setminus U$. Let $v_1, \ldots, v_p \in [v]_M \setminus U$ be as ensured by Condition C4 for $\bar{u}$, i.e., $R^M\pi\bar{u} = 1$ with $\pi = (w_1v_1)\cdots(w_pv_p)$. Applying the same π to $\hat{u}$, we see that $\pi\hat{u} = (\pi\bar{u})^{(vv')}$. As $v \sim v'$ in M, we have $R^M\pi\hat{u} = R^M\pi\bar{u} = 1$ and hence, by C4, we obtain $R^K\hat{u} = 1$.

Subcase 2.2: $v' \notin U$.

Note that $[v]_M \setminus \hat{U} = (([v]_M \setminus U) \setminus \{v'\}) \cup \{v\}$. Let $v_1, \ldots, v_p$ and π be as in Subcase 2.1. The difference is that now the containment $v' \in \{v_1, \ldots, v_p\}$ is possible. For $i \le p$, set

$$v'_i = \begin{cases} v_i & \text{if } v_i \ne v' \\ v & \text{if } v_i = v' \end{cases}$$

and apply to $\hat{u}$ the substitution $\pi' = (w_1v'_1)\cdots(w_pv'_p)$. It is not hard to see that $\pi'\hat{u} = \tau\pi\bar{u}$ for τ being a permutation of the set $\{v, v_1, \ldots, v_p, v'\}$ taking v_i to v'_i for all $i \le p$ and v to v'. Similarly to the second part of Subcase 1.2, we conclude that $R^M\pi'\hat{u} = R^M\pi\bar{u} = 1$ and, by C4, we obtain $R^K\hat{u} = 1$. ⊣

LEMMA 4.8. *Let L be a vocabulary with maximum relation arity k. Let M be an L-structure, $v \in V(M)$ with $|[v]_M| \ge k$, and $t \ge 0$. Then an L-structure K such that $K = M \oplus tv$ exists and is unique up to an isomorphism.*

PROOF. The existence follows from Definition C. To obtain K, we add t new elements to $V(M)$, keep all relations of M on $V(M)$, and add new relations involving at least one new element, being guided by Condition C4.

To prove the uniqueness, we use Definition B. Assume that $K_1 = M \oplus tv$ and $K_2 = M \oplus tv$ according to this definition. Let $\phi : V(K_1) \to V(K_2)$ be an arbitrary one-to-one map whose restriction on $V(M)$ is $\mathrm{id}_{V(M)}$. We claim that ϕ is an isomorphism from K_1 to K_2. Given an l-ary relation R in L and $\bar{u} \in V(K_1)^l$, we have to check that $R^{K_1}\bar{u} = R^{K_2}\phi\bar{u}$. The case that $\bar{u} \in V(M)^l$ is trivial. Suppose that $\{u_1, \dots, u_l\} \setminus V(M) = \{w_1, \dots, w_p\}$ is nonempty. Note that $\{\phi(u_1), \dots, \phi(u_l)\} \setminus V(M) = \{\phi(w_1), \dots, \phi(w_p)\}$ and $\{u_1, \dots, u_l\} \cap V(M) = \{\phi(u_1), \dots, \phi(u_l)\} \cap V(M)$. Let $v_1, \dots, v_p$ be pairwise distinct elements in C that do not occur in $\bar{u}$ and hence in $\phi\bar{u}$. Define ψ_1 by $\psi_1(v_i) = w_i$ for $i \le p$ and $\psi_1(x) = x$ for all other x in $V(M)$. Define ψ_2 similarly with the difference that $\psi_2(v_i) = \phi(w_i)$ for $i \le p$. Obviously, $\psi_2^{-1}\phi\bar{u} = \psi_1^{-1}\bar{u}$. By B2, ψ_1 and ψ_2 are partial isomorphisms from M to K_1 and K_2 respectively. Therefore

$$R^{K_1}\bar{u} = R^M\psi_1^{-1}\bar{u} = R^M\psi_2^{-1}\phi\bar{u} = R^{K_2}\phi\bar{u}.$$

The proof is complete. ⊣

With using Definition B, the following lemma is a direct consequence of Lemma 4.5.

Lemma 4.9. *Let L be a vocabulary with maximum relation arity k. Let M and M' be non-isomorphic L-structures of orders n and n' respectively and $n \le n'$. Then the bound*

$$\mathrm{D}_1(M, M') < \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2$$

may be false only if $M' = M^* \oplus (n' - n)v$ for some structure M^* isomorphic with M and $v \in V(M^*)$.

4.3.4. *An upper bound for* $\mathrm{D}(M)$. The following result was obtained in [14] for graphs with the proof easily adaptable for any structures (see Lemma 4.2 and Remark 4.9 in [14]).

Lemma 4.10. ([14]) *Let M be a structure of order n with maximum relation arity k, v be an element of M with $|[v]_M| = s \ge k$, and $M' = M \oplus tv$ with $t \ge 1$. Then*

$$s + 1 \le \mathrm{D}(M, M') \le \mathrm{D}_1(M, M') \le s + k - 1 + \frac{n+1}{s+1}.$$

Putting Lemmas 4.9 and 4.10 together, we immediately obtain an upper bound for $\mathrm{D}(M)$. Recall that $\sigma(M) = \max_{v \in V(M)} |[v]_M|$.

Theorem 4.11. *For a structure M of order n with maximum relation arity k, we have*

$$\mathrm{D}_1(M) \le \max\left\{ \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2,\ \sigma(M) + k \right\}.$$

Proof. Given M, let us summarize upper bounds we have for $\mathrm{D}_1(M, M')$ for various M' non-isomorphic with M. Denote

$$u_{k,n} = \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2 \quad \text{and} \quad f(s) = \left\lfloor s + k - 1 + \frac{n+1}{s+1} \right\rfloor.$$

If $M' = M^* \oplus tv$ for M^* an isomorphic copy of M, then

$$\mathrm{D}_1(M, M') \le \max_{1 \le s \le \sigma(M)} f(s) \tag{32}$$

by Lemma 4.10. Similarly, if $M = M^* \oplus tv$ for M^* an isomorphic copy of M', then

$$\mathrm{D}_1(M, M') \le \max_{1 \le s \le \sigma(M')} f(s),$$

which is within the bound (32) because in this case $\sigma(M') \le \sigma(M)$. For all other M' we have

$$\mathrm{D}_1(M, M') < u_{k,n}$$

by Lemma 4.9.

Notice now that

$$\max_{1 \le s \le \sigma(M)} f(s) \le \max\{f(1), f(\sigma(M))\}.$$

Furthermore,

$$f(\sigma(M)) \le \begin{cases} f(1) & \text{if } \sigma(M) \le (n-1)/2, \\ \sigma(M) + k & \text{if } \sigma(M) \ge n/2, \end{cases}$$

and $f(1) < u_{k,n}$. Summing up, we conclude that

$$\max_{M'} \mathrm{D}_1(M, M') \le \max\{u_{k,n},\ \sigma(M) + k\}.$$

By Lemma 2.2, the proof is complete. ⊣

Note that, given M, the number $\sigma(M)$ is efficiently computable in the sense that computing $\sigma(M)$ reduces to verification if a transposition is an automorphism of the structure. Thus, Theorem 4.11 provides an efficiently computable non-trivial upper bound for $\mathrm{D}_1(M)$, whereas it seems plausible that the exact value of $\mathrm{D}(M)$ is incomputable.

We also can restate the obtained bounds as a dichotomy result telling us that either we have the bound $\mathrm{D}_1(M, M') < (1 - \frac{1}{2k})n + k^2 - k + 2$ or else M has a simple, easily recognizable property and, moreover, for all such exceptional M we are able to easily compute $\mathrm{D}(M)$ within an additive constant. Results of this sort are obtained in [14] for structures with maximum relation arity 2 and k-uniform hypergraphs.

THEOREM 4.12. *Let M be a structure of order n with maximum relation arity k. If*

$$\sigma(M) \le \left(1 - \frac{1}{2k}\right) n + (k-1)^2 + 1, \tag{33}$$

we have

$$\mathrm{D}_1(M) \le \left(1 - \frac{1}{2k}\right) n + k^2 - k + 2. \tag{34}$$

Otherwise we have

$$\sigma(M) + 1 \le \mathrm{D}\,(M) \le \mathrm{D}_1(M) \le \sigma(M) + k. \tag{35}$$

PROOF. If the condition (33) is met, the bound (34) follows directly from Theorem 4.11. If (33) does not hold, the upper bound in (35) again follows from Theorem 4.11. The lower bound in (35) follows from Lemma 4.10 as $\mathrm{D}\,(M) \ge \mathrm{D}\,(M, M \oplus 1v) \ge \sigma(M) + 1$, where $v \in V(M)$ is such that $|[v]_M| = \sigma(M)$ and hence $|[v]_M| > k$. ⊣

§5. Identifying finite structures by Bernays-Schönfinkel formulas.

THEOREM 5.1. *Let L be a vocabulary with maximum relation arity k. If M is an L-structure of order n, then*

$$\mathrm{BS}\,(M) < \left(1 - \frac{1}{2k^2 + 2}\right) n + k. \tag{36}$$

If $k = 1$, a stronger bound $\mathrm{BS}\,(M) \le n/2 + 1$ holds true.

The case of $k = 1$ is easy and included for the sake of completeness. The upper bound of $n/2 + 1$ matches, up to an additive constant of 1, a simple lower bound of $n/2$ attainable by structures with a single unary relation. The proof of Theorem 5.1 for the case that $k \ge 2$ takes the rest of this section.

5.1. Notation. In addition to the notation introduced in Section 2.1, we will denote $[k] = \{1, 2, \ldots, k\}$. If $\bar{z} = (z_1, \ldots, z_l)$ and τ is a map from $[k]$ to $[l]$, then $\bar{z}^\tau = (z_{\tau(1)}, \ldots, z_{\tau(k)})$.

Recall that, given a partial isomorphism $\phi : X \to X'$ from an L-structure M to another L-structure M', we have defined a relation $\equiv_\phi$ between elements in $\overline{X}$ and elements in $\overline{X'}$ (see Definition 3.6). Definition 3.8 extends this relation over classes in $\mathcal{C}(X)$ and $\mathcal{C}(X')$. We will need yet another extension of $\equiv_X$ over subsets of $\overline{X}$ and $\overline{X'}$. Let $U \subseteq \overline{X}$ and $U' \subseteq \overline{X'}$. We will write $U \cong_\phi U'$ if ϕ extends to an isomorphism from $M[X \cup U]$ to $M'[X' \cup U']$.

We define $\mathrm{BS}_q(M)$ similarly to $\mathrm{BS}\,(M)$ with the only additional requirement that an identifying Bernays-Schönfinkel formula has at most q universal quantifiers. It is clear that $\mathrm{BS}\,(M) \le \mathrm{BS}_{q+1}(M) \le \mathrm{BS}_q(M)$.

5.2. A couple of useful formulas. If $\bar{x} = (x_1, \ldots, x_l)$ is a sequence of variables, let

$$\mathrm{Dist}(\bar{x}) = \bigwedge_{1 \le i < j \le l} x_i \ne x_j.$$

Let M be a finite structure over vocabulary L and $\bar{a}$ be a sequence of l pairwise distinct elements of $V(M)$. Then it is easy to construct a first order formula $\mathrm{Iso}_{M,\bar{a}}(x_1,\dots,x_l)$ such that, for every L-structure M' and $\bar{a}' \in V(M')^l$, $M',\bar{a}' \models \mathrm{Iso}_{M,\bar{a}}(\bar{x})$ iff the component-wise correspondence between $\bar{a}$ and $\bar{a}'$ is a partial isomorphism between M and M'. Specifically, assume that $L=(R_1,\dots,R_m)$, where R_i has arity k_i. Then

$$\mathrm{Iso}_{M,\bar{a}}(\bar{x}) = \mathrm{Dist}(\bar{x}) \wedge \bigwedge_{i=1}^{m}\Big(\bigwedge_{\tau} \Big\{ R_i(\bar{x}^\tau) \,\Big|\, \tau : [k_i] \to [l],\ R_i^M(\bar{a}^\tau)=1 \Big\} \wedge \bigwedge_{\tau} \Big\{ \neg R_i(\bar{x}^\tau) \,\Big|\, \tau : [k_i] \to [l],\ R_i^M(\bar{a}^\tau)=0 \Big\} \Big).$$

5.3. The first way of identification. In this section we will exploit the relation $\sim$ on $V(M)$ defined in Section 3.1 and the invariant $\sigma(M)$ introduced in Definition 4.2.

PROPOSITION 5.2. *Let L be a vocabulary with maximum relation arity k. For every L-structure M of order n, we have*

$$\mathrm{BS}_k(M) \le n + k - \sigma(M).$$

PROOF. Suppose that $\sigma(M)=k+d$ with $d\ge 1$ (if $\sigma(M)\le k$, the proposition is trivial). Let A be a $\sim$-equivalence class of elements of $V(M)$ such that $|A|=\sigma(M)$. Denote $B=\overline{A}$ and fix orderings $A=\{a_1,\dots,a_{k+d}\}$ and $B=\{b_1,\dots,b_{n-k-d}\}$. Set $\bar{a}=(a_1,\dots,a_k)$. We suggest the following formula Φ_M to identify M:

$$\Phi_M = \exists y_1 \dots \exists y_{n-k-d} \forall x_1 \dots \forall x_k \Psi_M(\bar{y},\bar{x}),$$

where

$$\Psi_M(\bar{y},\bar{x}) = \mathrm{Iso}_{M,\bar{b}}(\bar{y}) \wedge \big(\mathrm{Dist}(\bar{y},\bar{x}) \to \mathrm{Iso}_{M,\bar{b},\bar{a}}(\bar{y},\bar{x})\big)\,.$$

Claim A. $M' \models \Phi_M$ iff there is a partial isomorphism $\phi : B \to B'$ from M to M' such that every injective extension of ϕ over $B\cup\{a_1,\dots,a_k\}$ is a partial isomorphism from M to M'. ∎

Claim B. $M \models \Phi_M$.

Proof of Claim. On the account of Claim A, it suffices to show that the extension ϕ of id_B by $\phi(a_1)=a_{i_1},\dots,\phi(a_k)=a_{i_k}$, where $i_1,\dots,i_k$ is an arbitrary sequence of pairwise distinct indices in $[k+d]$, is a partial automorphism of M. This follows from the fact that every permutation of A, in particular, that taking each a_j for $j\le k$ to a_{i_j}, is decomposed into a product of transpositions $(a_p a_q)$ with $1\le p<q\le k+d$. (Recall that the latter are automorphisms of M). ∎

Claim C. If an L-structure M' has order n and $M' \models \Phi_M$, then M and M' are isomorphic.

Proof of Claim. Let ϕ and B' be as in Claim A. Fix an ordering $a'_1, \ldots, a'_{k+d}$ of the set $A' = V(M') \setminus B'$. According to Claim A, for every sequence $i_1, \ldots, i_k$ of pairwise distinct indices in $[k+d]$, the extension of ϕ by $\phi(a_j) = a'_{i_j}$ for $j \le k$ is a partial isomorphism from M to M'. From the proof of Claim B we know an analog of this fact for M itself: for every sequence $i_1, \ldots, i_k$ of pairwise distinct indices in $[k+d]$, the extension ψ of id_B by $\psi(a_j) = a_{i_j}$ for $j \le k$ is a partial automorphism of M. It follows, in particular, that for every sequence $1 \le i_1 < \ldots < i_k \le k+d$, the extension of ϕ by $\phi(a_{i_j}) = a'_{i_j}$ for $j \le k$ is a partial isomorphism from M to M'. Extend ϕ over the whole $V(M)$ by $\phi(a_i) = a'_i$ for all $i \le k+d$. We conclude that the restriction of ϕ on every k-element subset of $V(M)$ is a partial isomorphism from M to M'. Since every relation of M has arity at most k, ϕ is an isomorphism from M to M'. ■ ⊣

5.4. The second way of identification.

Definition 5.3. *A set $B \subseteq V(M)$ is called a* base *of a structure M if the relations $\equiv_B$ and $\sim$ coincide on $\overline{B}$. The* fineness *of a base B is defined by $f(B) = \max\{\,|C| : C \in \mathcal{C}(B)\}$. Furthermore, let $\rho(B) = |B| + \max\{f(B)+1, k\}$.*

We define $\rho(M)$ to be the minimum $\rho(B)$ over all bases B of M.

Proposition 5.4. $\mathrm{BS}\,(M) \le \rho(M)$.

Proof. Given a base B of M, we construct a Bernays-Schönfinkel formula Φ_M with $\rho(B)$ quantifiers that identifies M. Let $p = |B|$ and $q = \max\{f(B)+1, k\}$. Assume that $p + q < n$ for otherwise we are done. Denote $A = \overline{B}$ and fix orderings $A = \{a_1, \ldots, a_{n-p}\}$ and $B = \{b_1, \ldots, b_p\}$. We set

$$\Phi_M = \exists y_1 \ldots \exists y_p \forall x_1 \ldots \forall x_q \Psi_M(\bar y, \bar x),$$

where

$$\Psi_M(\bar y, \bar x) = \mathrm{Iso}_{M,\bar b}(\bar y) \wedge \left(\mathrm{Dist}(\bar y, \bar x) \to \bigvee_{\substack{\tau:[q]\to[n-p] \\ \tau \text{ is injective}}} \mathrm{Iso}_{M,\bar b,\bar a^\tau}(\bar y, \bar x) \right).$$

Claim A. Let M' be another L-structure, $\bar b' = (b'_1, \ldots, b'_p)$ be a sequence of elements of $V(M')$, and $A' = V(M') \setminus \{b'_1, \ldots, b'_p\}$. Then

$$M', \bar b' \models \forall x_1 \ldots \forall x_q \Psi_M(\bar y, \bar x)$$

holds iff

- the component-wise correspondence ϕ between $\bar{b}$ and $\bar{b}'$ is a partial isomorphism from M to M' and
- for every $U' \subseteq A'$ with at most q elements there is a $U \subseteq A$ such that $U \cong_\phi U'$.

The proof is fairly obvious. The claim immediately implies that $M \models \Phi_M$.

Claim B. If $M' \models \Phi_M$ and M' has order n, then M and M' are isomorphic.

Proof of Claim. Let $\bar{b}' = (b'_1, \ldots , b'_p)$ be such that

$$M', \bar{b}' \models \forall x_1 \ldots \forall x_q \Psi_M(\bar{y}, \bar{x}).$$

Set $B' = \{b'_1, \ldots , b'_p\}$. By the definition of Ψ_M, there is a partial isomorphism $\phi : B \to B'$ from M to M'. By Claim A, for every $a' \in A'$ there is $a \in A$ such that $a \equiv_\phi a'$. Hence for every $C' \in \mathcal{C}(B')$ there is $C \in \mathcal{C}(B)$ such that $C \equiv_\phi C'$. Moreover, for every $C' \in \mathcal{C}(B')$ and the respective $C \in \mathcal{C}(B)$ it holds $|C| \geq |C'|$ (if $|C'| > |C|$, then for any $(|C| + 1)$-element set $U' \subseteq C'$ the second condition in Claim A fails). Since $|A| = |A'|$ or, in other terms, $\sum_{C\in\mathcal{C}(B)} |C| = \sum_{C'\in\mathcal{C}(B')} |C'|$, for every C' it actually holds the equality $|C| = |C'|$. Thus, we have a one-to-one correspondence between $\mathcal{C}(B)$ and $\mathcal{C}(B')$ such that, if $C \in \mathcal{C}(B)$ and $C' \in \mathcal{C}(B')$ correspond to one another, then $C \equiv_\phi C'$ and $|C| = |C'|$.

We are now prepared to exhibit an isomorphism from M' to M. Fix an arbitrary extension ψ of ϕ^{-1} to a one-to-one map from $V(M')$ to $V(M)$ taking each C' to the respective C. We will show that ψ is an isomorphism. Let R' be an l-ary relation of M' and R be the respective relation of M. Given an arbitrary l-tuple $\bar{u}' \in V(M')^l$, we have to prove that

$$R\psi\bar{u}' = R'\bar{u}'. \tag{37}$$

Denote $U' = \{u'_1, \ldots , u'_l\}$. Let $\psi_{U'}$ be the extension of ϕ^{-1} to a partial isomorphism from M' to M with $U' \subseteq \operatorname{dom} \psi_{U'}$ whose existence is guaranteed by Claim A. We have

$$R\psi_{U'}\bar{u}' = R'\bar{u}'.$$

To prove (37), it suffices to prove that

$$R\psi_{U'}\bar{u}' = R\psi\bar{u}'. \tag{38}$$

We proceed similarly to the proof of Claim E in Section 4.1. By Item 3 of Lemma 3.7, the partial map $\psi_{U'}$ takes an element in a class C' to an element in the respective class C. Suppose that $\psi_{U'}$ is extended over the whole $V(M')$ with the latter condition obeyed. Since both $\psi_{U'}$ and ψ extend ϕ^{-1}, the product $\psi_{U'}\psi^{-1}$ moves only elements in A. Since both ψ and $\psi_{U'}$ take an element in a class C' to an element in the respective class C, the map $\psi_{U'}\psi^{-1}$ preserves the partition $\mathcal{C}(B)$ of A. It follows that $\psi_{U'}\psi^{-1}$ is decomposed into the product of permutations π_C over $C \in \mathcal{C}(B)$, where each π_C acts on the respective C. Since every π_C is decomposable into a product of transpositions, we have $\psi_{U'}\psi^{-1} = \tau_1\tau_2\ldots\tau_t$ with τ_i being a transposition of two elements both in some C. It is easy to see that $\psi_{U'}\bar{u}' = (\ldots((\psi\bar{u}')^{\tau_t})\ldots)^{\tau_1}$. By Lemma 3.12, each application of τ_i does not change the initial value of $R\psi\bar{a}'$. Therewith (38) is proved. ■ ⊣

REMARK 5.5. *One can show that* $\rho(M)$ *provides us with an upper bound not only for* $\mathrm{BS}(M)$ *but also for* $\mathrm{D}_1(M)$.

5.5. The third way of identification. Yet another way of identification that we here suggest is actually not new being a specification of Proposition 5.4 in the preceding section.

DEFINITION 5.6. *If* M *is a finite structure, let*

$$\delta(M) = \max\{\,|A| : A \subseteq V(M) \text{ such that } a_1 \not\equiv_{\overline{A}} a_2 \text{ for every } a_1, a_2 \in A\}\,.$$

It is not hard to see that, in other terms, $\delta(M) = \max_{X \subseteq V(M)} |\mathcal{C}(X)|$.

PROPOSITION 5.7. *Let* L *be a vocabulary with maximum relation arity* $k \geq 2$. *For every* L*-structure* M *of order* n, *we have*

$$\mathrm{BS}_k(M) \leq n + k - \delta(M).$$

PROOF. As easily seen, if $A \subseteq V(M)$ is such that $a_1 \not\equiv_{\overline{A}} a_2$ for every $a_1, a_2 \in A$, then $\overline{A} = V(M) \setminus A$ is a base of M with fineness $f(\overline{A}) = 1$. Since $k \geq 2$, we have $\max\{f(\overline{A}) + 1, k\} = k$ and therefore $\rho(M) \leq n + k - \delta(M)$. Thus, the proposition directly follows from Proposition 5.4. We only have to note that the identifying formula constructed in the proof of Proposition 5.4 has $\max\{f(\overline{A}) + 1, k\} = k$ universal quantifiers. ⊣

5.6. Putting it together. We now complete the proof of Theorem 5.1. Assume that $k \geq 2$. We will employ all three possibilities of identifying M given by Propositions 5.7, 5.2, and 5.4. Using the last possibility, we will use the set X_{k+1} defined by Definition 3.11 that is a base of M according to Lemma 3.12.

By the bound (10) of Lemma 3.13 and the fact that $|\mathcal{C}(X)| \leq \delta(M)$ for every $X \subseteq V(M)$, we have

$$|X_{k+1}| = n - |Z| \leq 2k^2\delta(M) - (k-1). \tag{39}$$

We now consider two cases.

Case 1: $Z = \emptyset$. By (39) we have $\delta(M) \geq \frac{n+k-1}{2k^2}$. By Proposition 5.7, this implies that

$$\mathrm{BS}(M) < \left(1 - \frac{1}{2k^2}\right) n + k.$$

Case 2: $Z \neq \emptyset$. In this case for the fineness of the base X_{k+1} we have $f(X_{k+1}) \geq k+2$. Using (39), we obtain

$$\begin{aligned}\rho(X_{k+1}) &\leq 2k^2\delta(M) - (k-1) + \max\{\,|C| : C \in \mathcal{C}(X_{k+1})\} + 1\\ &\leq 2k^2\delta(M) + \sigma(M) + 2 - k.\end{aligned}$$

Let $\lambda(M) = \max\{\delta(M), \sigma(M)\}$. By Propositions 5.7, 5.2, and 5.4, we have

$$\begin{aligned}\mathrm{BS}\,(M) &\leq \min\{n+k-\delta(M), n+k-\sigma(M), 2k^2\delta(M) + \sigma(M) + 2 - k\}\\ &\leq \min\{n+k-\lambda(M), (2k^2+1)\lambda(M) + 2 - k\}\\ &\leq \max_{1\leq\lambda\leq n} \min\{n+k-\lambda, (2k^2+1)\lambda + 2 - k\}\\ &\leq \left(1 - \frac{1}{2k^2+2}\right) n + k - \frac{k-1}{k^2+1} < \left(1 - \frac{1}{2k^2+2}\right) n + k.\end{aligned}$$

Since the latter bound holds in both the cases, the proof of Theorem 5.1 is for $k \geq 2$ complete.

In the case of $k = 1$ we use Propositions 5.2 and 5.4. We use the fact that, for a structure M with all relations unary, the empty set is a base and $\rho(\emptyset) = \sigma(M) + 1$. We therefore have $\mathrm{BS}\,(M) \leq \min\{n+1-\sigma(M), \sigma(M)+1\} \leq n/2 + 1$.

§6. Identifying finite structures by Bernays-Schönfinkel formulas with bounded number of universal quantifiers. Recall that $\mathrm{BS}_q(M)$ denotes the minimum total number of quantifiers in a Bernays-Schönfinkel formula identifying M with at most q universal quantifiers. We now address the asymptotics of the maximum value of $\mathrm{BS}_q(M)$ over structures of order n under the condition that q is bounded by a constant. We first observe that less than k universal quantifiers are rather useless for identification of a structure with maximum relation arity k.

PROPOSITION 6.1. *If M is a structure of order n with maximum relation arity k and $n \geq k$, then* $\mathrm{BS}_{k-1}(M) = n$.

PROOF. We have to show that no formula $\Phi = \exists y_1 \ldots \exists y_p \forall x_1 \ldots \forall x_q \Psi(\bar{y}, \bar{x})$ with Ψ quantifier-free, $q \leq k-1$, and $p + q \leq n - 1$ can identify M. Suppose that

$$M, \bar{b}, \bar{a} \models \Psi(\bar{y}, \bar{x}) \tag{40}$$

for some $\bar{b} \in V(M)^p$ and all $\bar{a} \in V(M)^q$. Let $A = V(M) \setminus \{b_1, \ldots, b_p\}$. Since $q+1 \leq k$, $q+1 \leq n-p \leq |A|$, and $n \geq k$, there is a k-element $U \subseteq V(M)$ such that $|U \cap A| \geq q+1$. Let $u_1, \ldots, u_k$ be an arbitrary ordering of U. Let R be a k-ary relation of M. Define a relation R' so that $R'\bar{u} \neq R\bar{u}$ and R' coincides with R elsewhere. Let M' be the modification of M with R' instead of R. Clearly, M' and M are non-isomorphic. It is easy to see that $M', \bar{b}, \bar{a} \models \Psi(\bar{y}, \bar{x})$ for the same $\bar{b}$ as in (40) and all $\bar{a} \in V(M')^q$. Therefore $M' \models \Phi$ and Φ fails to identify M. ⊣

If at least k universal quantifiers are available, some saving on the number of quantifiers is possible: It turns out that $\mathrm{BS}_k(M) < n - \sqrt{n} + k^2 + k$ and this bound cannot be improved much if we keep the number of universal quantifiers constant.

THEOREM 6.2. *Let* $\mathrm{BS}_q(n,k)$ *denote the maximum* $\mathrm{BS}_q(M)$ *over structures* M *of order* n *and maximum relation arity* k*. Then*

$$\mathrm{BS}_k(n,k) < n - \sqrt{n} + k^2 + k.$$

On the other hand, if n *is a square, then*

$$\mathrm{BS}_q(n,k) \ge n - (q-1)\sqrt{n} + q$$

for every $q \ge 2$ *and* $k \ge 2$*.*

The upper bound of Theorem 6.2 is provable by the techniques from Section 5. Let M be a structure of order n with maximum relation arity k. By Propositions 5.7 and 5.2,

$$\mathrm{BS}_k(M) \le n + k - \max\{\delta(M), \sigma(M)\}.$$

It remains to prove the following bound.

LEMMA 6.3. $\max\{\delta(M), \sigma(M)\} > \sqrt{n} - k^2$.

PROOF. By the bound (10) of Lemma 3.13,

$$n + k - 1 \le 2k \sum_{i=1}^{k-1} |\mathcal{C}^{k+1}(X_i)| + (k+1)|\mathcal{C}^{k+1}(X_k)| + (k-1)|\mathcal{C}(X_k)| + |Z|.$$

We bound each term $|\mathcal{C}(X)|$ from above by $\delta(M)$. Furthermore, we bound $|Z|$ from above by the number of $\equiv_{X_{k+1}}$-equivalence classes inside Z multiplied by the maximum number of elements in such a class. By Lemma 3.12 it follows that $|Z| \le \delta(M)\sigma(M)$. We therefore conclude that

$$n + k - 1 \le \delta(M)(2k^2 + \sigma(M)).$$

This implies

$$\max\{\delta(M), \sigma(M)\} \ge \min_{1 \le \sigma \le n} \max\left\{\sigma, \frac{n+k-1}{2k^2+\sigma}\right\} > \sqrt{n} - k^2,$$

as required. ⊣

REMARK 6.4. *The bound of Lemma 6.3 is essentially optimal because, for any graph* G *of order* m^2 *whose vertex set is partitioned into* m $\sim$*-equivalence classes of* m *element each, it holds* $\sigma(G) = m$ *and* $\delta(G) \le m$*. Such* G *can be constructed from any graph* H *of order* m *whose automorphism group contains no transposition by replacing each vertex* $v \in V(H)$ *with* m *pairwise (non-)adjacent vertices* $\sim$*-related to* v *in* H*.*

We now prove the lower bound of Theorem 6.2. It suffices to do it for graphs. The example of G with large $\mathrm{BS}_q(G)$ will be the same as in Remark 6.4. This example can be lifted to a higher arity k by adding $k-2$ dummy coordinates to the adjacency relation with no affect to its truth value.

PROPOSITION 6.5. *Let G_m be graph of order m^2 whose vertex set is partitioned into m $\sim$-equivalence classes of m element each. Let $q \geq 2$. Then $\mathrm{BS}_q(G_m) \geq m^2-(q-1)m+q$.*

PROOF. It is enough to show that, if G_m is identified by a Bernays-Schönfinkel formula Φ with q universal quantifiers, then Φ contains at least $m^2-(q-1)m$ existential quantifiers. If $q \geq m+1$, this is trivial. Assume that $q \leq m$.

Suppose on the contrary that G_m is identified by a Bernays-Schönfinkel formula $\Phi = \exists y_1 \ldots \exists y_p \forall x_1 \ldots \forall x_q \Psi(\bar{y}, \bar{x})$ with $p < m^2-(q-1)m$. Let $\bar{b} \in V(G_m)^p$ be such that $G_m, \bar{b} \models \forall x_1 \ldots \forall x_q \Psi(\bar{y}, \bar{x})$. Equivalently,

$$G_m, \bar{b}, \bar{a} \models \Psi(\bar{y}, \bar{x}) \text{ for all } \bar{a} \in V(G_m)^q. \tag{41}$$

Let $A = V(G_m) \setminus \{b_1, \ldots, b_p\}$. We have $|A| \geq (q-1)m+1$. The condition imposed on G_m implies that there are two $\sim$-equivalence classes, C_1 and C_2, such that $|A \cap C_1| \geq q$ and $|A \cap C_2| \geq 1$. Let us modify G_m by removing one vertex from $A \cap C_2$ and adding a new vertex v' to C_1 so that $v' \sim v$ for all $v \in C_1$. The modified graph, G', is clearly non-isomorphic to G_m. We show that, nevertheless, $G' \models \Phi$.

It suffices to show that $G', \bar{b}, \bar{a}' \models \Psi(\bar{y}, \bar{x})$ for every $\bar{a}' \in V(G')^q$. In view of (41), we are done if for every $\bar{a}' \in V(G')^q$ we are able to find an $\bar{a} \in V(G_m)^q$ such that the component-wise correspondence between $\bar{b}, \bar{a}$ and $\bar{b}, \bar{a}'$ is a partial isomorphism between G_m and G'. If $\bar{a}'$ does not contain any occurrence of v', we obviously can take $\bar{a} = \bar{a}'$. If $\bar{a}'$ contains an occurrence of v', let v be a vertex in $A \cap C_1$ that does not occur in $\bar{a}'$ and let $\bar{a}$ be the result of substituting v in place of v' everywhere in $\bar{a}'$. It is not hard to see that the obtained $\bar{a}$ is as required. ⊣

§7. The case of graphs. For a binary structure M, Theorem 4.1 implies $\mathrm{I}(M) < 0.75n+4$ and Theorem 5.1 implies $\mathrm{BS}(M) < 0.9n+2$. In the case of graphs, both these bounds can be improved. In [14] we obtain an almost optimal bound $\mathrm{I}(G) \leq (n+3)/2$ (there are simple examples of graphs with $\mathrm{I}(G) \geq (n+1)/2$). Combining the approach from [14] and the techniques from Section 5, we are able to prove a better bound for $\mathrm{BS}(G)$ as well. We are also interested in knowing the smallest n starting from which for G of order n we have the bound at least $\mathrm{BS}(G) \leq n-1$, an improvement on the trivial bound of n.

THEOREM 7.1. *Let G be a graph of order n.*

1) *We have* $\mathrm{BS}(G) \leq 3n/4+3/2$.

2) *If* $n \ge 5$, *we have* $\mathrm{BS}_2(G) \le n-1$ *with the only exception of the graph* H *on 5 vertices with 2 adjacent edges for which, nevertheless, we have* $\mathrm{BS}_3(H) \le 4$.

PROOF. Given a graph G, let $X = E(\emptyset)$, where the transformation E is introduced in Section 3.2. We state two properties of the X established in [14]:

Property 1: $|\mathcal{C}(X)| \ge |X| + 1$.

Property 2: Let $Y = Y(X)$ and $Z = V(G) \setminus (X \cup Y)$. Every class in $\mathcal{C}(X \cup Y)$ consists of pairwise $\sim$-equivalent vertices.

Note that $|\mathcal{C}(X)| \le \delta(G)$. By Property 1 we conclude that

$$|X| + |Y| \le |X| + |\mathcal{C}(X)| \le 2|\mathcal{C}(X)| - 1 \le 2\delta(G) - 1. \tag{42}$$

Property 2 means that $X \cup Y$ is a base of G.

We now consider two cases.

Case 1: $Z = \emptyset$. In this case $n = |X| + |Y|$. By (42), $\delta(G) \ge (n+1)/2$. Using Proposition 5.7, we obtain $\mathrm{BS}_2(G) \le n/2 + 3/2$.

Case 2: $Z \ne \emptyset$. In this case $\rho(X \cup Y) \le |X| + |Y| + \sigma(G) + 1$. By (42) we have $\rho(X \cup Y) \le 2\delta(G) + \sigma(G)$. Denote $\lambda(G) = \max\{\delta(G), \sigma(G)\}$. By Propositions 5.7, 5.2, and 5.4, we have

$$\begin{aligned}
\mathrm{BS}\,(G) &\le \min\{n + 2 - \delta(G), n + 2 - \sigma(G), 2\delta(G) + \sigma(G)\} \\
&\le \min\{n + 2 - \lambda(G), 3\lambda(G)\} \\
&\le \max_{1 \le \lambda \le n} \min\{n + 2 - \lambda, 3\lambda\} = 3n/4 + 3/2.
\end{aligned}$$

Since this bound holds true in both the cases, Item 1 of the theorem is proved.

To prove Item 2, we estimate $\max\{\delta(G), \sigma(G)\}$. Since $n = |X| + |Y| + |Z| \le 2\delta(G) - 1 + \delta(G)\sigma(G)$, we have

$$n + 1 \le \delta(G)(2 + \sigma(G)). \tag{43}$$

It follows that

$$\max\{\delta(G), \sigma(G)\} \ge \min_{1 \le c \le n} \max\left\{c, \frac{n+1}{2+c}\right\} = \sqrt{n+2} - 1$$

and hence

$$\max\{\delta(G), \sigma(G)\} \ge 3 \tag{44}$$

whenever $n > 7$.

Claim A. The bound (44) holds for all G of order 6 or 7.

Proof of Claim. This claim is proved by the direct brute force analysis. We have $\delta(\overline{G}) = \delta(G)$ and $\sigma(\overline{G}) = \sigma(G)$, where $\overline{G}$ denotes the complement of a graph G. Hence, for order 6, it suffices to consider graphs with at most 7 edges. For order 7 the number of cases is much larger; the complete analysis can be found in [15]. ∎

Thus, if G has order at least 6, we have the bound (44) and the theorem follows from Propositions 5.7 and 5.2. For graphs of order 5 the estimate (44) holds with the only exception for the specified graph H. This graph is identified by formula

$$\exists y_1 \forall x_1 \forall x_2 \forall x_3 \left(\mathrm{Dist}(y_1, x_1, x_2, x_3) \to \neg E(x_1, x_2) \wedge \bigvee_{i=1}^{3} E(y_1, x_i) \wedge \bigvee_{i=1}^{3} \neg E(y_1, x_i) \right),$$

where E is the adjacency relation. ⊣

REMARK 7.2. *Item 2 of Theorem 7.1 does not hold true for graphs of order* $n = 4$*: It is not hard to prove that* $\mathrm{BS}\,(F) = 4$ *for the graph* F *on 4 vertices with 1 edge.*

REMARK 7.3. *In* [11] *we address the first order definability of a random graph* G *on* n *vertices. It is proved that, with probability* $1 - o(1)$*,*

$$\log_2 n - 2\log_2\log_2 n \le \mathrm{I}\,(G) \le \log_2 n - \log_2\log_2 n + \log_2\log_2\log_2 n + O(1).$$

One of the ingredients of the proof is that, with high probability, $\delta(G) \ge n - (2 + o(1))\log_2 n$*. Since* $\mathrm{I}\,(G) \le \mathrm{BS}_2(G) \le n + 2 - \delta(G)$*, we conclude that, with high probability,*

$$\log_2 n - 2\log_2\log_2 n \le \mathrm{BS}_2(G) \le (2 + o(1))\log_2 n.$$

§8. Open problems.

1. Let $\mathrm{I}\,(n,k)$ (resp. $\mathrm{I}_l(n,k)$; $\mathrm{BS}\,(n,k)$) be the maximum $\mathrm{I}\,(M)$ (resp. $\mathrm{I}_l(M)$; $\mathrm{BS}\,(M)$) over structures of order n with maximum relation arity k. We now know that

$$\begin{aligned} \tfrac{n}{2} \le \mathrm{I}\,(n,k) \le \mathrm{I}_1(n,k) \le \mathrm{BS}\,(n,k) < (1 - \tfrac{1}{2k^2+2})n + k \\ \text{and } \ \mathrm{I}_1(n,k) < (1 - \tfrac{1}{2k})n + k^2 - k + 2. \end{aligned} \tag{45}$$

Note that $\mathrm{I}\,(n,k) \le \mathrm{I}\,(n,k+1)$ and that the lower bound of $n/2$ is actually for $\mathrm{I}\,(n,1)$. Make the gap between the lower and upper bounds in (45) closer.

The case of $k = 2$ is essentially solved in [14], where the bounds

$$\frac{n+1}{2} \le \mathrm{I}\,(n,2) \le \mathrm{I}_1(n,2) \le \frac{n+3}{2}$$

are proved. If $k = 3$, we are able to improve on (45) by showing that $\mathrm{I}_1(n,3) \le \frac{2}{3}n + O(1)$ (in [14] this bound was obtained for 3-uniform hypergraphs).

2. Can one prove a non-trivial upper bound for $\mathrm{I}_0(n,k)$? The weakest question is if $\mathrm{I}_0(n,k) \le n-1$. It is easy to show that $\mathrm{I}_0(n,1) \le (n+1)/2$. In [14] we prove that $\mathrm{I}_0(G) \le (n+5)/2$ for graphs of order n.

3. What happens if we restrict the number of existential rather than universal quantifiers in an identifying Bernays-Schönfinkel formula?

REFERENCES

[1] J.-Y. Cai, M. Fürer, N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica* 12:389–410 (1992).

[2] H.-D. Ebbinghaus, J. Flum. *Finite Model Theory.* Springer Verlag, 2nd rev. ed. (1999).

[3] A. Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fundam. Math.* 49:129–141 (1961).

[4] R. Fagin. Finite-model theory — a personal perspective. *Theoretical Computer Science* 116:3–31 (1993).

[5] R. Fraïssé. Sur quelques classifications des systems de relations. *Publ. Sci. Univ. Alger* 1:35–182 (1954).

[6] M. Grohe, Fixed-point logics on planar graphs. In: *Proc. of the Ann. Conf. on Logic in Computer Science* 6–15 (1998).

[7] M. Grohe, Isomorphism testing for embeddable graphs through definability. In: *Proc. of the 32nd ACM Ann. Symp. on Theory of Computing (STOC)* 63–72 (2000).

[8] N. Immerman. *Descriptive complexity.* Springer-Verlag (1999).

[9] N. Immerman, D. Kozen. Definability with bounded number of bound variables. *Information and Computation* 83:121–139 (1989).

[10] N. Immerman, E. Lander, Describing graphs: a first-order approach to graph canonization. In: *Complexity Theory Retrospective*, A. Selman Ed., Springer-Verlag, 59–81 (1990).

[11] J. H. Kim, O. Pikhurko, J. Spencer, O. Verbitsky. How complex are random graphs in first order logic? Submitted (2003).

[12] E. Pezzoli. Computational complexity of Ehrenfeucht-Fraïssé games on finite structures. In: *Proc. of the CSL'98 Conf.*, G. Gottlob, K. Seyr Eds. Lecture Notes in Computer Science 1584, Springer-Verlag, 159–170 (1999).

[13] O. Pikhurko, J. Spencer, O. Verbitsky. Succinct definitions in first order graph theory. In preparation (2003).

[14] O. Pikhurko, H. Veith, O. Verbitsky. First order definability of graphs: tight bounds on quantifier rank. Submitted (2003). E-print `http://arxiv.org/abs/math.CO/0311041`

[15] O. Pikhurko, O. Verbitsky. Descriptive complexity of finite structures: saving the quantifier rank. (2003). E-print `http://arxiv.org/abs/math.LO/0305244`

[16] J. Spencer. *The strange logic of random graphs.* Springer Verlag (2001).

DEPARTMENT OF MATHEMATICAL SCIENCES, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA 15213-3890.

URL: `http://www.math.cmu.edu/~pikhurko/`

E-mail: `pikhurko@andrew.cmu.edu`

DEPARTMENT OF MECHANICS AND MATHEMATICS, KYIV UNIVERSITY, UKRAINE.

E-mail: `oleg@ov.litech.net`