Complexity Results for First-Order Two-Variable Logic with Counting*

Leszek Pacholski
Institute of Computer Science
Wrocław University
pacholsk@tcs.uni.wroc.pl

Wiesław Szwast Lidia Tendera
Institute of Mathematics
Opole University
[szwast,tendera]@math.uni.opole.pl

Abstract

Let C_p^2 denote the class of first order sentences with two variables and with additional quantifiers "there exists exactly (at most, at least) i", for $i \leq p$, and let C^2 be the union of C_p^2 taken over all integers p. We prove that the satisfiability problem for C_1^2 sentences is NEXPTIME-complete. This strengthens the results by E. Grädel, Ph. Kolaitis and M. Vardi [15] who showed that the satisfiability problem for the first order two-variable logic L^2 is NEXPTIME-complete and by E. Grädel, M. Otto and E. Rosen [16] who proved the decidability of C^2. Our result easily implies that the satisfiability problem for C^2 is in non-deterministic, doubly exponential time. It is interesting that C_1^2 is in NEXPTIME in spite of the fact, that there are sentences whose minimal (and only) models are of doubly exponential size.

It is worth noticing, that by a recent result of E. Grädel, M. Otto and E. Rosen [17], extensions of two-variables logic L^2 by a week access to cardinalities through the Härtig (or equicardinality) quantifier is undecidable. The same is true for extensions of L^2 by very week forms of recursion.

The satisfiability problem for logics with a bounded number of variables has applications in artificial intelligence, notably in modal logics (see e.g. [22]), where counting comes in the context of graded modalities and in description logics, where counting can be used to express so-called number restrictions (see e.g. [8]).

1 Introduction

Let L^2 denote the class of first order sentences with two variables over a relational vocabulary, and let C_p^2 denote L^2 extended with additional quantifiers "there exists exactly (at most, at least) i", for $i \leq p$. Finally, let C^2 be the union of C_p^2 taken over all integers p. We prove that the problem of satisfiability of sentences of C_1^2 is NEXPTIME-complete.

Problems concerning decidability of restricted classes of quantificational formulas have been studied since the second decade of this century by many logicians including W. Ackermann, P. Bernays, K. Gödel, L. Kalmár, M. Schönfinkel, T. Skolem, H. Wang [1, 2, 5, 11, 12, 24, 33, 34, 35, 37] and many others. In the late twenties and in the thirties (see [7] and [19] for more informations) the study of classification of solvable classes of prenex formulas was one of the most active areas of logic. Now, after the works of Y. Gurevich [18], M. Rabin [30], S. Shelah [32] and W. Goldfarb [14] the classification of prenex classes has been completed. Accounts of the classical results in this area can be found in several books [3, 7, 9, 25]. More

*The results included in section 4 have been published as a part of [29].

recent results have been obtained by H.R. Lewis and W. Goldfarb [13, 14, 26]. A short survey of the research in this area can be found in [19] (see also the introduction to [15]).

In 1962, in a short note, D. Scott [31] proved that the satisfiability problem for L^2 was decidable. His proof was based on a reduction of this problem to the problem of satisfiability of sentences in the Gödel class with equality. Later, in 1975, M. Mortimer gave another proof of decidability by proving that L^2 has a finite model property. When in 1984 G.D. Goldfarb [14] found a counterexample to the claim, that the Gödel class with equality had a decidable satisfiability problem, the very short and elegant proof by D. Scott lost its validity. In 1980 H. Lewis [27] proved that the satisfiability problem for L^2 was NEXPTIME-hard. The complexity of an algorithm which could be extracted from the Mortimer's work was doubly exponential. Recently, E. Grädel, Ph. Kolaitis and M. Vardi [15] have closed the gap by providing a very elegant proof that the satisfiability problem for L^2 was in NEXPTIME. Later we found another proof [36] of the same result. Our proof was not as nice as the one in [15], but we hoped it could be extended to get the complexity bounds for C^2.

In [16] E. Grädel, M. Otto and E. Rosen established decidability of the satisfiability problem for C^2. They proved that the set of sentences which have infinite models was recursive, which implied the above mentioned result. No complexity estimates could be obtained from their proof.

In this paper we prove that the satisfiability problem for C^2_1 is in NEXPTIME, so by the result H. Lewis [27] it is NEXPTIME-complete. By the reduction of C^2 to C^2_1 given in [16] this implies that C^2 is in 2-NEXPTIME. Although our strict upper bound applies only to C^2_1 we believe that we have developed techniques that can be used to close the gap for the entire class C^2.

Our approach is in a very remote way based on the ideas of Mortimer. A very simple cardinality argument shows that Mortimer's notion of a *star* could not be used to give a NEXPTIME decision procedure. This led to a weakening of this notion to the notion of a *constellation*. As the first application of this notion we gave in [36] another proof of the result of Grädel, Kolaitis and Vardi [15]. There we have also used a stronger notion of a normal form - going further than Grädel, Otto and Rosen in [16] - a *constellation form*, in which additionally, constant symbols do not appear. The proof in [36] is "syntactic", however, in the case of L^2, the "syntactic" structure coding a model is almost equivalent to a model. This changes dramatically when we move to C^2, and allows for a concise description of models that can be even infinite.

In contrast to [16] our basic notions are almost entirely syntactic. We like the feudal terminology of [16] and we treat *kings* of [16] with proper care and respect. However, *kings* in our sense have other virtues besides belonging to a finite set. Population of our kings is always at most doubly exponential in the size of the language. On the other hand, it is easy to give examples of models whose sets of kings in the sense of [16] have, for a language of bounded size, arbitrary large cardinality. This seems to suggest that the method of [16] could not easily be adapted to give complexity bounds.

To get our result we analyze the structure of the feudal court. We have a few kings and kings are characterized by the fact, that they are connected between themselves using only *counting types*. Instead of a more or less uniform court we have a hierarchy V_i, for $i < 2^{n^2}$ of vassals, each of which may be a sovereign of perhaps several vassals in V_{i+1}. The union V of all V_i, for $i < 2^{n^2}$ is included in the set of *kings* in the sense of [16] and provides information sufficient to reconstruct a model and thus gives rise a 2-NEXPTIME algorithm for C^2_1, and a 3-NEXPTIME algorithm for C^2. Of course, we can not easily improve the above bounds, since we can provide a sentence (see Proposition 4.21) of C_1^2 of size n whose unique model coincides with V and has cardinality $O(2^{2^n})$.

To push the lower bound down we had to provide a finer analysis. We have noticed that although the number of vassals in a model can be large (doubly exponential), the number of vassals that are different from the point of view of relations between themselves is smaller (exponential). In more technical terms a potential model is described by a set of indexed constellations and numbers of elements that realize these constellations. Roughly speaking, an indexed constellation in addition to information on two-types realized by pairs containing a given element carries, for certain two-types *requests* for partner constellations - constellations that should realize, together with the given constellation, these two-types. Moreover, we show that the model is composed of some number of parts (only one of them can be infinite), which can be treated separately and independently during construction of the model. To check if the parts can be constructed we use several graph-theoretical results concerning the existence of Hamiltonian cycles, matchings and bipartition.

It is worth noticing, that by a recent result of E. Grädel, M. Otto and E. Rosen [17], extensions of two-variables logic L^2 by a weak access to cardinalities through the Härtig (or equicardinality) quantifier is undecidable. The same is true for extensions of L^2 by very weak forms of recursion.

The satisfiability problem for logics with a bounded number of variables has applications in artificial intelligence, notably in modal logics (see e.g. [22]) where counting comes in the context of graded modalities and in description logics, where counting can be used to express so-called number restrictions (see e.g. [8]). More information on applications and relation of two-variables logics to modal logics is given in [15].

2 Preliminaries

Throughout the paper we are concerned mainly with signatures that consist of unary and binary predicate letters without Boolean predicates, function symbols and constants. This restriction allows to simplify definitions and technical proofs. We would, however, like to emphasize that it is easy to adapt all notions used in this paper and to modify the proofs in order to obtain the same results also for the full first-order two-variable logic with counting, including predicate letters of higher arity and constants (see e.g. [15] for a proof that predicate letters of higher arity can be eliminated).

We assume that the reader is familiar with standard notions of logic and with basic concepts of computational complexity theory. In this paper, $\mathcal{L}$-structures are denoted by Gothic capital letters and their universes by corresponding Latin capitals. Furthermore, if a structure $\mathfrak{A}$ is fixed, then its substructure with the universe denoted by a Latin capital is denoted by the corresponding Gothic capital.

By L^2 we denote the class of first order sentences with two variables over a relational vocabulary, and by C_p^2 we denote L^2 extended by additional quantifiers of the form $\exists^{=i}$, $\exists^{\leq i}$ or $\exists^{\geq i}$ (there exists exactly, at most, at least i), for $i \leq p$. Finally, C^2 is the union of C_p^2 taken over all integers p.

Let $\mathcal{L}$ be a relational vocabulary with unary and binary predicate letters only. A *1-type* $t(x)$ is a maximal consistent set of atomic and negated atomic formulas of the language $\mathcal{L}$ in the variable x. A *2-type* $t(x, y)$ is a maximal consistent set of atomic and negated atomic formulas of the language $\mathcal{L}$ in the variables x, y, such that $(x \neq y) \in t(x, y)$. A type t is often identified with the conjunction of formulas in t. For a 2-type $t(x,y)$ we denote by $t(x,y)\restriction\{x\}$ the unique 1-type $t(x)$ included in $t(x,y)$ and we denote by t^* the type dual to t, that is the type obtained from t by replacing each occurrence of the variable x by y and each occurrence of y by x. If $\mathfrak{A}$ is an $\mathcal{L}$-structure with the universe A, and if $a, b \in A$, then we denote by $tp^{\mathfrak{A}}(a,b)$ the unique type realized by the pair $\langle a,b\rangle$ in $\mathfrak{A}$.

Recall that for any integer function $t(n)$, NTIME($t(n)$) is the class of all decision problems that can be solved by a non-deterministic Turing machine in time $t(n)$, where n is the length of the input. We put

$$\text{NEXPTIME} = \bigcup_p \text{NTIME}(2^{p(n)}),$$

$$\text{2-NEXPTIME} = \bigcup_p \text{NTIME}(2^{2^{p(n)}}),$$

where p is a polynomial.

3 On L^2 case

In this section we consider the satisfiability problem for L^2, the first-order logic with two-variables and without counting quantifiers. We give an algorithm solving this problem which runs in non-deterministic exponential time. As we have mentioned in the Introduction, it follows from the paper of M. Mortimer [28] that the satisfiability problem for L^2 can be solved by a non-deterministic algorithm in doubly exponential time. An algorithm whose complexity matches the NEXPTIME lower bound given by H. Lewis [27] was presented in a very nice paper by E. Grädel, Ph. Kolaitis and M. Vardi [15]. This algorithm and the bound that follow from the Mortimer's work depend on the bounds on the cardinality of a minimal model of an L^2 sentence. Our algorithm in contrast to the above, does not exploit the bounded model property of L^2.

This section is a modification of [36] and it is included here following a suggestion of one of the referees in order to introduce and explain the techniques used later for logic with counting.

Our approach in a remote way is based on Mortimer's notion of a *star* [28], a *star* being an arbitrary set of two-types with a consistent *center*. The notion of a star was a very convenient technical tool to describe a finite structure and to check, with the help of Ehrenfeucht games of depth two [10], that this structure is a model of an L^2 sentence. Unfortunately, the Mortimer's notion of a star cannot be directly used to give a NEXPTIME decision procedure since the cardinality of a star is exponential and the number of possible stars is doubly exponential in the number of predicate letters in the signature.

We weaken the notion of a star to a notion of a *small constellation* that we introduce after a close analysis of L^2 sentences from the point of view of their satisfiability. As in other related papers [31, 15] we use a variant of a notion of a normal form of first-order sentences. Our notion is called a *constellation form* and it allows to introduce the notion of a small constellation in a very natural way. Unlike a star, a small constellation is of linear size and it contains only these two-types that describe a relation of a given point to a witness that must exist in a model of an L^2 sentence.

We also introduce a notion of a *small galaxy* as a set of small constellations that can be modeled in a first order structure and we prove that an L^2-sentence is satisfiable if and only if there exists a small galaxy (Theorem 3.5). A small galaxy has only exponential size.

As the next step we give necessary and sufficient conditions for a set of small constellations to form a small galaxy (Definition 3.12, Theorem 3.13). In the proof of Theorem 3.13 we use notions of special and replicable constellations which are analogous to Mortimer's notions of asymmetric and symmetric stars. These notions are crucial for our analysis of models for L^2-sentences. As a result we get a nondeterministic exponential upper bound for the satisfiability problem for L^2-sentences (Corollary 3.14).

3.1 Small constellations, small galaxies and satisfiability

Let $\mathcal{R} \subseteq \mathcal{L}$ be a set of binary predicate letters, $\mathcal{R} = \{R_1, \ldots, R_m\}$.

Definition 3.1 *An $\mathcal{L}$-sentence Φ is in* constellation form *if*

$$\Phi = \forall x \forall y \phi(x, y) \wedge \bigwedge_{1 \leq i \leq m} \forall x \exists y R_i(x, y),$$

where ϕ is quantifier-free.

This definition may seem too strong. The second part of the formula seems to suggest that all elements are similar from the point of view of $\mathcal{R}$. Note however, that we do not require that $x \neq y$, therefore for an element x, by $R_i(x, x)$ we can code those relations R_i, for which the existential quantifier of the second part of Φ does not apply.

Let $\mathcal{A}$ be a set of 2-types closed under operation * and let $\mathcal{A}^+ = \{t \in \mathcal{A} : R_i(x, y) \in t$, for some $i \leq m\}$.

Definition 3.2 *Let $S = \{s_0, s_1, \ldots, s_k\}$, where $0 \leq k \leq m$, s_0 is a 1-type and, if $k > 0$ then $s_1, \ldots, s_k \in \mathcal{A}^+$. Define*
$center(S) = \bigwedge_{0 \leq i \leq k} s_i \restriction \{x\}$.
The set S is a small $\mathcal{A}$-$\mathcal{R}$-constellation *if the following conditions hold:*
1) $center(S) = s_0$,
2) for every $R_i \in \mathcal{R}$, if $R_i(x, x) \notin center(S)$ then there exists j, $1 \leq j \leq k$, such that $R_i(x, y) \in s_j$,

Notice that the notion of a small $\mathcal{A}$-$\mathcal{R}$-constellation depends on a set $\mathcal{A}$ of 2-types and a set $\mathcal{R}$ of binary predicate symbols.

Definition 3.3 *Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. An element $a \in A$* realizes *a small $\mathcal{A}$-$\mathcal{R}$-constellation $S = \{s_0, \ldots, s_k\}$ if $tp^{\mathfrak{A}}(a, a) = s_0$, for each $b \in A$, $tp^{\mathfrak{A}}(a, b) \in \mathcal{A}$, and there exists a sequence $b_1, \ldots, b_k$ of elements of A such that $tp^{\mathfrak{A}}(a, b_i) = s_i$, $0 < i \leq k$.*
A small $\mathcal{A}$-$\mathcal{R}$-constellation S is realized *in $\mathfrak{A}$ if there exists $a \in A$ which realizes S.*

Note that if an element $a \in \mathfrak{A}$ realizes a small $\mathcal{A}$-$\mathcal{R}$-constellation then $\mathfrak{A} \models \bigwedge_{1 \leq i \leq m} \exists y R_i(a, y)$.

Definition 3.4 *Let $\mathcal{S}$ be a set of small $\mathcal{A}$-$\mathcal{R}$-constellations. A structure $\mathfrak{A}$* realizes *$\mathcal{S}$ if every element $a \in A$ realizes a small $\mathcal{A}$-$\mathcal{R}$-constellation $S \in \mathcal{S}$, and every small $\mathcal{A}$-$\mathcal{R}$-constellation $S \in \mathcal{S}$ is realized by an element $a \in A$.*
The set $\mathcal{S}$ is a small galaxy *if there is a structure $\mathfrak{A}$ such that $card(A) > 1$, and $\mathfrak{A}$ realizes $\mathcal{S}$.*

The following theorem gives a necessary and sufficient condition for satisfiability of sentences in constellation form.

Theorem 3.5 *Let $\mathcal{R} = \{R_1, \ldots, R_m\} \subseteq \mathcal{L}$ and let Φ be an $\mathcal{L}$-sentence in constellation form,*

$$\Phi = \forall x \forall y \phi(x,y) \wedge \bigwedge_{1 \le i \le m} \forall x \exists y R_i(x,y).$$

Put $\mathcal{A} = \{t : t(x,y) \text{ is a 2-type over } \mathcal{L} \text{ and } t(x,y) \to \phi(x,y)\}$.

Then Φ has a model with at least two-element universe if and only if there exists a set $\mathcal{S}$ of small $\mathcal{A}$-$\mathcal{R}$-constellations which is a small galaxy.

Proof. ($\Rightarrow$) Let $\mathfrak{A} \models \Phi$ and $card(A) > 1$. Since $\mathfrak{A} \models \forall x \forall y \phi(x,y)$, the set $\mathcal{A}$ is closed under the operation *. Moreover, $\mathfrak{A} \models \bigwedge_{1 \le i \le m} \forall x \exists y R_i(x,y)$ implies that every element of A realizes at least one small $\mathcal{A}$-$\mathcal{R}$-constellation. Let $\mathcal{S} = \{S : S$ is a small $\mathcal{A}$-$\mathcal{R}$-constellation and S is realized in $\mathfrak{A}\}$. By Definitions 3.4, $\mathfrak{A}$ realizes $\mathcal{S}$.

($\Leftarrow$) Let $\mathcal{S}$ be a small galaxy and assume $\mathfrak{A} \models \mathcal{S}$. Let $a \in A$. By Definition 3.4, a realizes a small $\mathcal{A}$-$\mathcal{R}$-constellation $S \in \mathcal{S}$, $S = \{s_0, \ldots, s_k\}$. This implies that $tp^{\mathfrak{A}}(a,a) = s_0$, and there exists a sequence $b_1, \ldots, b_k$ of distinct elements of A such that $b_i \neq a$, for $i = 1, \ldots, k$, and

1. $tp^{\mathfrak{A}}(a, b_i) = s_i$, for $i = 1, \ldots, k$,
2. $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}$, for $b \in \mathcal{A}$.

So, by Definition 3.2, the elements $b_1, \ldots, b_k$ witness that the part $\bigwedge_{1 \le i \le m} \exists y R_i(x,y)$ of Φ holds for a. Moreover, for every $b \in A, b \neq a$, $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}$, and so $\mathfrak{A} \models \phi(a,b)$. Therefore $\mathfrak{A} \models \Phi$.

□

3.2 The reduction

The following reduction theorem is essentially due to Scott [31]. It has been also used in [28] and [15]. We present a slightly modified version of the theorem given in [15].

Theorem 3.6 *There exists a polynomial time algorithm which, given an L^2 sentence Ψ over an arbitrary relational vocabulary, constructs a sentence Φ in constellation form with the following properties:*

1. *Ψ is satisfiable if and only if Φ is satisfiable.*
2. *Every predicate letter occuring in Φ has arity at most 2.*
3. *If n is the length of Ψ, then Φ contains $O(n)$ different predicate letters and has length $O(n \log n)$.*

3.3 The small galaxy theorem

In this section we fix $\mathcal{R} = \{R_1, \ldots, R_m\} \subseteq \mathcal{L}$, and a set $\mathcal{A}$ of 2-types closed under the operation *.

To simplify terminology in this subsection we write 'constellation' instead of 'small $\mathcal{A}$-$\mathcal{R}$-constellation' and 'galaxy' instead of 'small galaxy'.

By Theorem 3.6 and Theorem 3.5 the satisfiability problem for L^2 sentences can be reduced to the problem of finding an appropriate galaxy. In this subsection we shall give syntactic conditions that are necessary and sufficient for a set of constellations to be a galaxy.

Definition 3.7 *Let S, T be constellations and let $t(x,y) \in \mathcal{A}$. S* is connectable to *T* by *$t(x,y)$ if $center(S) \subseteq t(x,y)$ and $center(T) \subseteq t^*(x,y)$.*

We say that S is connectable to *T if there is a type $t(x,y) \in \mathcal{A}$ such that S is connectable to T by $t(x,y)$.*

Proposition 3.8 *Let $\mathcal{S}$ be a galaxy and $S \in \mathcal{S}$. Then the following conditions are equivalent.*

1. *There is a structure $\mathfrak{A}$ which realizes $\mathcal{S}$, and S is realized in $\mathfrak{A}$ by at least two element.*
2. *S is connectable to S.*

Proof. Let $\mathcal{S}$ be a galaxy, $S \in \mathcal{S}$ and let $\mathfrak{B}$ be a structure such that $\mathfrak{B} \models \mathcal{S}$. To prove the implication (1) $\Rightarrow$ (2), assume that S is realized in $\mathfrak{A}$ by two elements a and b. Let $t(x,y) = tp^{\mathfrak{A}}(a,b)$. Since $\mathfrak{A} \models \mathcal{S}$, we have $t(x,y) \in \mathcal{A}$. Of course, $center(S) \subseteq t(x,y)$ and $center(S) \subseteq t^*(x,y)$.

Now, we shall prove that (2) $\Rightarrow$ (1). Let $t \in \mathcal{A}$ be such that $center(S) \subseteq t(x,y)$ and $center(S) \subseteq t^*(x,y)$. Let $b \in B$ realize S in $\mathfrak{B}$. We claim that there exists an extension $\mathfrak{A}$ of $\mathfrak{B}$ such that $A = B \cup \{a\}$, where $a \notin B$ and a realizes S. Indeed, $\mathfrak{A}$ can be obtained from $\mathfrak{B}$ by putting $A = B \cup \{a\}$, $tp^{\mathfrak{A}}(a,b) = t(x,y)$, and $tp^{\mathfrak{A}}(a,c) = tp^{\mathfrak{A}}(b,c)$, for every $c \in B$. $\square$

The proposition above motivates the following definition.

Definition 3.9 *A constellation S is* replicable *if S is connectable to S. Otherwise, the constellation S is* special.

Let $\mathcal{S}$ be a galaxy, and let $\mathfrak{A}$ satisfy $\mathcal{S}$. In the universe A of $\mathfrak{A}$ we can distinguish the set $K \subseteq A$ consisting of all elements which realize special constellations. Elements of the set K are called *kings*. A *noble* is an element of the set $N = \bigcup_{a \in K}\{b_1, \ldots, b_k \in A : k \leq m$ and $\{tp^{\mathfrak{A}}(a), tp^{\mathfrak{A}}(a,b_1), \ldots, tp^{\mathfrak{A}}(a,b_k)\} \in \mathcal{S}\}$. Nobles are those elements of the universe that are necessary for the existence of kings. Define the *court* $C = K \cup N$. Note that $card(C) \leq (m+1)card(K)$. There may also be *plebeians* – elements outside the court; they are not necessary for the kings but perhaps some nobles may need them. Plebeians may also depend on kings to survive.

Remark. The notion of a king in a structure has been used in many places. For example, Yu. Gurevich and S. Shelah have used this notion in [20] to show that their proof of the solvability of the Gödel class without equality could not be generalized to the case with equality. E. Grädel, Ph. Kolaitis and M. Vardi have also used this notion in [15]. We would like to point out that although in this paper the kings are defined in terms of constellations, they have the same meaning as in [15].

Definition 3.10 *Denote by $Sp(\mathcal{S})$ the subset of $\mathcal{S}$ consisting of all special constellations, and by $Rp(\mathcal{S})$ the set $\mathcal{S} \setminus Sp(\mathcal{S})$.*

The following simple observation establishes relations between the notions defined above.

Proposition 3.11 *Let $\mathcal{S}$ be a galaxy, and let $\mathfrak{A}$ realizes $\mathcal{S}$. Then there exist sets K and C such that the following conditions hold.*

1. *$K \subseteq C \subseteq A$, $card(K) \leq card(Sp(\mathcal{S}))$ and, $card(C) \leq (m+1)card(K)$.*
2. *Every element $a \in K$ realizes a constellation $S \in Sp(\mathcal{S})$ in $\mathfrak{A}{\restriction}C$.*

3. Every constellation $S \in Sp(\mathcal{S})$ is realized by an element $a \in K$ in $\mathfrak{A} \restriction C$.

4. For every $S, T \in Rp(\mathcal{S})$, S is connectable to T.

Proof. Immediate. $\square$

One can easily check that the converse to the above proposition does not hold. For example, let

$$
\begin{aligned}
\mathcal{L} &= \mathcal{R} = \{R_1, R_2\},\\
\mathcal{A} &= \{t_1, t_1^*, t_2, t_2^*, t_3\},\\
s_0(x) &= R_1(x,x) \wedge R_2(x,x),\\
t_0(x) &= \neg R_1(x,x) \wedge \neg R_2(x,x),\\
t_1 &= t_0(x) \wedge R_1(x,y) \wedge \neg R_2(x,y) \wedge R_1(y,x) \wedge R_2(y,x) \wedge s_0(y),\\
t_2 &= t_0(x) \wedge \neg R_1(x,y) \wedge R_2(x,y) \wedge R_1(y,x) \wedge R_2(y,x) \wedge s_0(y),\\
t_3 &= t_0(x) \wedge \neg R_1(x,y) \wedge \neg R_2(x,y) \wedge \neg R_1(y,x) \wedge \neg R_2(y,x) \wedge t_0(y),\\
\mathcal{S} &= \{S, T\}, \text{ where } S = \{s_0\} \text{ and } T = \{t_0, t_1, t_2\}.
\end{aligned}
$$

It is easy to see that the constellation S is special and T is replicable. One can check that if we define $K = \{a\}$, $C = K$, $tp^{\mathfrak{A}}(a) = s_0$, then conditions (1)–(3) of Proposition 3.11 hold and, since T is connectable to T by t_3, condition (4) holds too. Unfortunately, the constellation T can not be realized in any structure, since to realize T we need two elements b_1 and b_2 such that $tp^{\mathfrak{A}}(b_1) = s_0$, $tp^{\mathfrak{A}}(b_2) = s_0$, and $tp^{\mathfrak{A}}(b_1, b_2) \in \mathcal{A}$, which is not possible. Therefore, $\mathcal{S}$ is not a galaxy.

Now, we shall extend the set of conditions given in Proposition 3.11 to a set of conditions that will imply that a set $\mathcal{S}$ of constellations is a galaxy.

Definition 3.12 *Let $\mathcal{S}$ be a set of constellations. A* small representation *of $\mathcal{S}$ is a system*

$$\langle K, C, I, F, G \rangle,$$

where K and C are sets, I, F, G are functions such that $I : C \to \mathcal{S}$, $F : C \times C \to \mathcal{A}$, $G : Rp(\mathcal{S}) \times K \to \mathcal{A}$, and the following conditions hold.

(s1) $K \subseteq C$, $card(K) \le card(Sp(\mathcal{S}))$, and $card(C) \le (m+1)card(K)$.

(s2) $I(K) = Sp(S)$, $I(C \setminus K) \subseteq Rp(\mathcal{S})$,
$F(a,a) = F(a,b)\restriction\{x\}$, and for every $a \ne b$ $F(a,b) = F(b,a)^*$.

(s3) For every $a \in K$, and every $t \in I(a)$ there is an element $c \in C$ such that $t = F(a,c)$.

(s4) For every $b \in C \setminus K$, and every $t \in I(b)$ if there is no $c \in C$ such that $t = F(b,c)$, then there is a constellation $T \in Rp(\mathcal{S})$ such that $I(b)$ is connectable to T by t.

(s5) For every $S, T \in Rp(\mathcal{S})$, S is connectable to T.

(s6) For every $S \in Rp(\mathcal{S})$, and every $a \in K$, S is connectable to $I(a)$ by $G(S,a)$.

(s7) For every $S \in Rp(\mathcal{S})$, and every type $t(x,y) \in S$ if there is no $a \in K$ such that $G(S,a) = t(x,y)$, then there is a constellation $T \in Rp(\mathcal{S})$ such that S is connectable to T by t.

Conditions (s1), (s2) and (s3) say that the set C is a universe of a structure in which all special constellations are realized. In other words, kings are provided with all they need to survive. Condition (s4) ensures that every noble can find enough plebeians around him. Condition (s5) says that plebeians can live together in one society and, by condition (s6), the society is ruled by kings. Condition (s7) states that plebeians can get what they need – if not from kings, then from somewhere else.

Theorem 3.13 (Small Galaxy Theorem) *A set of constellations $\mathcal{S}$ is a galaxy if and only if there exists a small representation of $\mathcal{S}$.*

Proof. ($\Rightarrow$) Assume that $\mathcal{S}$ is a galaxy and $\mathfrak{A}$ realizes $\mathcal{S}$. Let K be the set of kings in $\mathfrak{A}$, and let C be the court in $\mathfrak{A}$. For every $a \in C$ choose a constellation $S \in \mathcal{S}$ which is realized by a, and put $I(a) = S$. For every $a, b \in C$, put $F(a, b) = tp^{\mathfrak{A}}(a, b)$. For every constellation $S \in Rp(\mathcal{S})$ find an element $b \in A$ which realizes S, and for every $a \in K$ put $G(S, a) = tp^{\mathfrak{A}}(b, a)$.

It is easy to check that the system $\langle K, C, I, F, G\rangle$ is a small representation of $\mathcal{S}$.

($\Leftarrow$) Let $\mathcal{S}$ be a set of constellations, and let $\langle K, C, I, F, G\rangle$ be a small representation of $\mathcal{S}$.

We shall construct a structure $\mathfrak{A}$ realizing $\mathcal{S}$ such that the universe A of $\mathfrak{A}$ contains C, every $a \in K$ realizes $I(a)$ in $\mathfrak{A}{\restriction}C$, and $tp^{\mathfrak{A}}(a, b) = F(a, b)$, for each pair $\langle a, b\rangle$ of elements of C.

The construction proceeds in steps. The number of step can be infinite. In each step new elements are added to the universe. A new element is added when there is a request to satisfy a constellation, say S. Whenever an element a is added to satisfy S, I is extended by putting $I(a) = S$. An element a such that $I(a) = S$ is *inactivated* after adding enough elements to witness that a realizes S. An unordered pair of elements will be *reserved*, when a type to be realized by this pair has been designated.

In every step of the construction the universe of the part of the structure $\mathfrak{A}$ defined so far is finite. We also assume that there is a fixed linear ordering $<$ of the universe, and each new element added to the universe is greater then all old elements.

Let $\mathcal{S} = \{S_1, \ldots, S_k\}$.

Stage 1.

1. Let $A = C$.
2. For every $a, b \in C$, put $tp^{\mathfrak{A}}(a, b) = F(a, b)$ (cf. (s2)).
3. For every $a \in K$, inactivate a.
4. For every $a, b \in C$, reserve $\{a, b\}$.
5. For every $S \in Rp(\mathcal{S})$ such that $I(b) \neq S$, for each $b \in C$, add a new element d to A and put $I(d) = S$.

   Stage 2.
6. Let b be the first active (i.e yet not inactivated) element of A.

   Note that $I(b) \in Rp(\mathcal{S})$. Indeed, $b \notin K$, so either $b \in C \setminus K$, and so $I(b) \in Rp(\mathcal{S})$, by (s2), or b has been added to A in steps 5, 7(a)ii or 9(b), and whenever we add a new element b to the universe we always put $I(b) \in Rp(\mathcal{S})$.
7. If $b \in C \setminus K$ then
   (a) for every $t \in I(b)$ if there is no element $c \in C$ such that $t = F(b, c)$ do
      i. using (s4) find $T \in Rp(\mathcal{S})$ such that $I(b)$ is connectable to T by t,

ii. add a new element d to A;
iii. put $I(d) = T$, and $tp^{\mathfrak{A}}(b, d) = t$, reserve $\{b, d\}$;

(b) inactivate b and go to 6.

8. Using (s6), for every $a \in K$, put $tp^{\mathfrak{A}}(b, a) = G(I(b), a)$.
   Note that, $b \notin C$, so no pair $\{a, b\}$, with $a \in K$, has been reserved earlier.
9. For every $t \in I(b)$, if there is no $c \in A$ such that $\{c, b\}$ is reserved and $tp^{\mathfrak{A}}(c, b) = t^*$, do
   (a) by (s7) find $T \in Rp(\mathcal{S})$ such that $I(b)$ is connectable to T by t.
   Note that, by step 8, there is no element $a \in K$ such that $t = G(I(b), a)$.
   (b) add a new element d to A;
   (c) put $I(d) = T$, $tp^{\mathfrak{A}}(b, d) = t$, and reserve $\{b, d\}$;
   (d) for every $a < b$, if $\{a, b\}$ is not reserved then using (s5) find $t \in \mathcal{A}$ such that $I(b)$ is connectable to $I(a)$ by t, put $tp^{\mathfrak{A}}(b, a) = t$ and reserve $\{b, a\}$.
10. Inactivate b and go to 6.

We shall now show that $\mathfrak{A}$ realizes $\mathcal{S}$. First, let us note that every pair of distinct elements of A realizes in $\mathfrak{A}$ a two-type of $\mathcal{A}$ (see steps 2, 7(a)iii, 8, 9(c), 9(d)).

New elements are added at the end of the fixed ordering, and in step 6 we always consider the first active element, therefore every element $a \in A$ will eventually be inactivated. We claim, that when an element a is inactivated then a realizes a constellation of $\mathcal{S}$ in $\mathfrak{A}$. In fact an element inactivated in step 3, by (s2) and (s3) of Definition 3.12, realizes a special constellation of $\mathcal{S}$. Before an element b is inactivated in step 7(b), in step 7(a) every type of $I(b)$ has been realized by a pair $\langle b, a\rangle$ for some $a \in A$. Similarly, step 9 ensures that the element inactivated in step 10 realizes its constellation.

Finally, by step 5 every constellation of $\mathcal{S}$ is realized in $\mathfrak{A}$. □

Now, let us consider the cardinality of the structure constructed by the algorithm described above. If $Rp(\mathcal{S}) = \emptyset$ then only the first stage of the algorithm is performed and we get a structure with the universe K. We also get a finite structure if no new elements are added in step 7(a)i. In this case $I(C) = \mathcal{S}$, and the function F is defined in such a way that no noble element needs a plebeian. In other cases we get an infinite structure. The construction could be modified in such a way that it will stop after a bounded number of steps. However, we omit this modification, since the construction described above is better suited for generalization to logic with counting.

3.4 Complexity

Corollary 3.14 *There is a nondeterministic algorithm with time complexity $O(2^{cn^2})$, for some constant c, which, given an L^2-sentence Φ, decides if Φ is satisfiable.*

Remark. In [36], using more complicated techniques, we gave a similar algorithm with time complexity $O(2^{cn})$. Here we provide a simplified version only, since it is easier to understand and better explains the methods used in the main part of this paper.

Proof. Let Φ be an L^2 sentence of length n. In the first step we use the polynomial time algorithm of Theorem 3.6 to get a sentence Ψ in constellation form

$$\Psi = \forall x \forall y \phi(x, y) \wedge \bigwedge_{1 \leq i \leq m} \forall x \exists y R_i(x, y)$$

which is satisfiable if and only if Φ is satisfiable. Moreover, Ψ has at most $p = O(n)$ predicate letters, and has length $O(n \log n)$.

Then we use Theorem 3.5. We build a set $\mathcal{A}$ in time $O(2^{O(p)})$, and, in time $O((2^{4p})^m) = O(2^{O(n^2)})$, we guess a set $\mathcal{S}$ of small $\mathcal{A}$-$\mathcal{R}$-constellations.

Next, we use Theorem 3.12 and we guess sets K and C and functions I, F and G. Since $card(K) \leq 2^{O(n^2)}$, and $card(C) \leq (m+1)card(K)$ we can do this in time $O(2^{O(n^2)})$.

Finally, we accept Ψ after checking whether $\langle K, C, I, F, G\rangle$ is a small representation of $\mathcal{S}$. This can also be done in time $O(2^{O(n^2)})$. $\square$

4 Double exponential algorithm

4.1 Constellations, galaxies and satisfiability

Let $\mathcal{R} = \{R_1, \ldots, R_m\} \subseteq \mathcal{L}$ be the set of binary predicate letters.

Definition 4.1 *An $\mathcal{L}$-sentence Φ is in* constellation form *if*

$$\Phi = \forall x \forall y \phi(x,y) \wedge \bigwedge_{1\leq i\leq m} \forall x \exists^{=m_i} y R_i(x,y),$$

where ϕ is quantifier-free. Φ is in $\exists^{=1}$-constellation form *if $m_i = 1$ for each $i \leq m$.*

As Definition 3.1, the definition above may seem too strong, since the second part of the formula seems to suggest that all elements are similar from the point of view of $\mathcal{R}$. However, as before, the fact whether $R_i(x,x)$ holds is used to code those relations R_i for which the counting quantifier does not apply.

Let $\mathcal{A}$ be a set of 2-types closed under operation *.

Definition 4.2 $\mathcal{A} = \mathcal{A}^{\leftrightarrow} \dot{\cup} \mathcal{A}^{\leftarrow} \dot{\cup} \mathcal{A}^{\rightarrow} \dot{\cup} \mathcal{A}^{-}$, *where*

$\mathcal{A}^{\leftrightarrow} = \{t \in \mathcal{A} :$ *there are* $i, j \leq m$ *such that* $R_i(x,y) \in t$ *and* $R_j(y,x) \in t\}$,

$\mathcal{A}^{\leftarrow} = \{t \in \mathcal{A} : t \notin \mathcal{A}^{\leftrightarrow}$ *and there exists* $i \leq m$ *such that* $R_i(y,x) \in t\}$,

$\mathcal{A}^{\rightarrow} = \{t \in \mathcal{A} : t \notin \mathcal{A}^{\leftrightarrow}$ *and there exists* $i \leq m$ *such that* $R_i(x,y) \in t\}$,

$\mathcal{A}^{-} = \{t \in \mathcal{A} :$ *for every* $i \leq m, \neg R_i(x,y) \in t$ *and* $\neg R_i(y,x) \in t\}$.

In the definition above $\mathcal{A}^{\leftrightarrow}$, $\mathcal{A}^{\leftarrow}$ and $\mathcal{A}^{\rightarrow}$ represent *counting types.* Since R_i appears in the second part of the formula Φ in constellation form, it follows that $R_i(x,y) \in t$ implies that for (a,b) and (a,b') realizing t we always have $b = b'$.

Definition 4.3 *Let $S = \{s_0, s_1, \ldots, s_k\}$, where $k \geq 0$, s_0 is a 1-type and, if $k > 0$ then $s_1, \ldots, s_k \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\rightarrow}$. Define*

$center(S) = \bigwedge_{0\leq i\leq k} s_i \restriction \{x\}$.

The set S is an $\mathcal{A}$-$\mathcal{R}$-constellation *if the following conditions hold:*

1) $center(S) = s_0$,

2) for every $R_i \in \mathcal{R}$, if $R_i(x,x) \notin center(S)$ then there is exactly one j, $1 \leq j \leq k$, such that $R_i(x,y) \in s_j$,

3) for every $R_i \in \mathcal{R}$, if $R_i(x,x) \in center(S)$ then for every j, $1 \leq j \leq k$, $R_i(x,y) \notin s_j$.

Notice that the notion of an $\mathcal{A}$-$\mathcal{R}$-constellation depends on fixed sets $\mathcal{A}$ of 2-types and $\mathcal{R}$ of binary predicate symbols. Moreover, the number of two-types in a constellation does not exceed $card(\mathcal{R})$. It does not follow from Definition 4.3 that each constellation contains a counting type. There may be constellations S such that $center(S) = \{R_i(x,x) : R_i \in \mathcal{R}\}$. In fact $center(S)$ codes the relations in $\mathcal{R}$ which are not used in S in the context of counting.

Definition 4.4 *Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. An element $a \in A$* realizes *an $\mathcal{A}$-$\mathcal{R}$-constellation $S = \{s_0, \ldots, s_k\}$ if $tp^{\mathfrak{A}}(a,a) = s_0$, and there exists a unique sequence $b_1, \ldots, b_k \in A$ that $tp^{\mathfrak{A}}(a,b_i) = s_i$, $1 \leq i \leq k$, and for every $b \in A$, $b \neq a$, $b \neq b_i$, $1 \leq i \leq k$, we have $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$. An $\mathcal{A}$-$\mathcal{R}$-constellation S is* realized *in $\mathfrak{A}$ if there exists an element $a \in A$ which realizes S.*

For $a \in A$, we write $C_a^{\mathfrak{A}}$ to denote the unique $\mathcal{A}$-$\mathcal{R}$-constellation realized by a.

Definition 4.5 *Let $\mathcal{S}$ be a set of $\mathcal{A}$-$\mathcal{R}$-constellations. A structure $\mathfrak{A}$* realizes *$\mathcal{S}$, if every element in A realizes an $\mathcal{A}$-$\mathcal{R}$-constellation and every constellation in $\mathcal{S}$ is realized in $\mathfrak{A}$.*
A set $\mathcal{S}$ of $\mathcal{A}$-$\mathcal{R}$-constellations is a galaxy *if there is a structure $\mathfrak{A}$ such that $card(A) > 1$, and $\mathfrak{A}$ realizes $\mathcal{S}$.*

The following theorem gives a necessary and sufficient condition for satisfiability of sentences in $\exists^{=1}$-constellation form.

Theorem 4.6 *Let $\mathcal{R} = \{R_1, \ldots, R_m\} \subseteq \mathcal{L}$, and let Φ be an $\mathcal{L}$-sentence in $\exists^{=1}$-constellation form,*

$$\Phi = \forall x \forall y \phi(x,y) \wedge \bigwedge_{1 \leq i \leq m} \forall x \exists^{=1} y R_i(x,y).$$

Put $\mathcal{A} = \{t : t(x,y)$ is a 2-type over $\mathcal{L}$ and $t(x,y) \rightarrow \phi(x,y)\}$.

Then Φ has a model with at least two-elements if and only if there exists a set of $\mathcal{A}$-$\mathcal{R}$-constellations which is a galaxy.

Proof. ($\Rightarrow$) Assume that $\mathfrak{A} \models \Phi$ and $card(A) > 1$. Since $\mathfrak{A} \models \forall x \forall y \phi(x,y)$, the set $\mathcal{A}$ is closed under *. Since $\mathfrak{A} \models \bigwedge_{1 \leq i \leq m} \forall x \exists^{=1} y R_i(x,y)$, every element of A realizes some $\mathcal{A}$-$\mathcal{R}$-constellation. Therefore $\mathcal{S} = \{C_a^{\mathfrak{A}} : a \in A\}$ is a galaxy.

($\Leftarrow$) Let $\mathcal{S}$ be a galaxy and assume that $\mathfrak{A}$ realizes $\mathcal{S}$. Let $a \in A$. By Definition 4.5, a realizes an $\mathcal{A}$-$\mathcal{R}$-constellation $S \in \mathcal{S}$, $S = \{s_0, \ldots, s_k\}$. This implies that $tp^{\mathfrak{A}}(a,a) = s_0$, and that there exists a sequence $b_1, \ldots, b_k$ of distinct elements of A such that $b_i \neq a$, for $i = 1, \ldots, k$, and

1. $tp^{\mathfrak{A}}(a,b_i) = s_i$, for $i = 1, \ldots, k$,
2. $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-} \subset \mathcal{A}$, for each $b \in \mathcal{A}$, such that $b \neq a$ and $b \neq b_i$, $i = 1, \ldots, k$,.

Therefore by Definition 4.3, the elements $b_1, \ldots, b_k$ witness that the part $\bigwedge_{1 \leq i \leq m} \exists^{=1} y R_i(x,y)$ of Φ holds for $x = a$. Moreover, for every $b \in A, b \neq a$, $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}$, and so $\mathfrak{A} \models \phi(a,b)$. Hence, $\mathfrak{A} \models \Phi$. □

4.2 The Reduction

The following theorem has been shown in [16].

Theorem 4.7 *There is a recursive reduction* NF *from C^2-sentences to C^2-sentences in normal form over an extended vocabulary, which is sound for satisfiability: Φ is satisfiable if and only if* NF(Φ) *is satisfiable.*

In the above theorem the normal form is slightly weaker than our $\exists^{=1}$-constellation form. The difference is that in the $\exists^{=1}$-constellation form the quantifier free part of the sentences with prefix $\forall\exists^{=1}$ is atomic, whereas in the normal form in then sense of [16] it could be any quantifier free two-variable formula. This additional condition can be easily met by introducing new relation symbols for quantifier free formulas, and adding $\forall\forall$-sentences defining the newly introduced symbols.

From the proof of Theorem 4.7 given in [16] the following corollaries can be derived.

Corollary 4.8 *There exists a polynomial time algorithm which, given a C^2_1 sentence Ψ over a relational vocabulary, constructs a sentence Φ in $\exists^{=1}$-constellation form with the following properties:*

1. *Ψ is satisfiable if and only if Φ is satisfiable.*
2. *Every predicate letter occuring in Φ has arity at most 2.*
3. *If n is the length of Ψ, then Φ contains $O(n)$ different predicate letters and has length $O(n \log n)$.*

The reduction for the full logic C^2 is more expensive.

Corollary 4.9 *There exists an exponential time algorithm which, given a C^2 sentence Ψ over a relational vocabulary, constructs a sentence Φ in $\exists^{=1}$-constellation form with the following properties:*

1. *Ψ is satisfiable if and only if Φ is satisfiable.*
2. *Every predicate letter occuring in Φ has arity at most 2.*
3. *If n is the length of Ψ, then Φ contains $O(2^n)$ different predicate letters and has length $O(2^{O(n)})$.*

The exponential increase of the length of the sentence Φ given by the algorithm in Corollary 4.9 is caused by the necessity to introduce as many new predicate letters as the maximal integer which appear as an index of a counting quantifier. If integers are represented in binary we have to introduce $O(2^n)$ new predicate letters for a sentence of length n. We do not know any better reduction and this is the main reason, why we can not improve the upper complexity bound for the satisfiability problem for the full C^2 from double to single exponential.

4.3 The Galaxy Theorem

In this subsection we fix $\mathcal{R} = \{R_1, \ldots, R_m\} \subseteq \mathcal{L}$, and a set $\mathcal{A}$ of 2-types closed under *. Henceforth, whenever the sets $\mathcal{A}$ and $\mathcal{R}$ are fixed, we write 'a constellation' instead of 'an $\mathcal{A}$-$\mathcal{R}$-constellation'.

So far we have shown that the satisfiability problem for C_1^2 sentences can be transformed to the problem of finding an appropriate galaxy. In this section we shall formulate syntactic conditions which are necessary and sufficient for a set of constellations to form a galaxy, but before doing that, in order to acquaint the reader with our basic technic and to provide a better background for the proof of the main result of this section, we shall state and prove some basic properties of constellations.

At the beginning we introduce a syntactic notion of *connectability* of two constellations. This definition says that two constellations are connectable by a 2-type t if t is a connective type for them, that is t contains the centers of both constellations and either t is non-counting, or t and t^* are distributed between these two constellations. In other words, this notion provides a necessary condition for two constellations to be realizable in the same structure.

The notion of connectability, together with the notions of constellation and galaxy, plays a crucial role in this section and is basic in the whole paper. An easy observation (Proposition 4.14) shows that in a specific situation this notion suffices to formulate very simple conditions that allows to solve the satisfiability problem. This "specific" situation can be described in both semantic and syntactic terms: there is a structure in which every constellation is realized infinitely many times, or every two constellations are connectable by a non-counting type. Intuitively it means that there are no privileged elements in the structure.

Next, we consider the case when there are some privileged elements in a model. We prove that if a constellation S is realized in a structure sufficiently often then we can build a structure in which S appears infinitely many times (Lemma 4.15). Constellations that can be realized infinitely often are easy to deal with, in contrast with those that always appear only finitely many times.

Lemma 4.16 plays a crucial role in the proof of the main result of this section — the Galaxy Theorem. It says that every galaxy can be partitioned into two sets: constellations which can be realized by at most r elements and constellations which can be realized by infinitely many elements. The integer r is bounded by an exponential function of the number of constellations in a given galaxy. To prove this lemma, for a structure $\mathfrak{A}$ realizing the given galaxy, we define a sequence of sets $V_1 \subset V_2 \subset \ldots \subset V_{p-1}$ of subsets of A. The set V_1 consists of lords, that is of elements of A which realize constellations appearing in $\mathfrak{A}$ very rarely – less than 2m+1 times. Every set V_{i+1}, for $i > 1$, besides members of V_i, contains elements that are vassals of elements of V_i. They realize constellations appearing in $\mathfrak{A}$ not very often with respect to the cardinality of the set V_i of sovereigns of the elements of V_{i+1}. In this way we obtain a finite hierarchy of elements of A and so, a hierarchy of elements of the galaxy — constellations realized by elements of appropriate V_i. This hierarchy does not necessarily include all constellations.

All the results mentioned above give several necessary conditions for a set of constellations to be a galaxy. As the next step we introduce the notion of a *finite representation of* a set of constellations (Definition 4.17), and we prove the Galaxy Theorem (Theorem 4.18) which says that the problem whether a set of constellations $\mathcal{S}$ is a galaxy can be reduced to the problem whether there exists a finite representation of $\mathcal{S}$.

Since the components of a finite representation are either finite sets of bounded cardinality or functions from such sets into some fixed finite sets, and since the conditions on the components are easily[1] computable, the Galaxy Theorem forms a basis for a decision procedure for the satisfiability problem for C_1^2 (Corollary 4.20 in 4.4).

[1] In this section "easily" means in double exponential time.

We begin the technical part of this section with some additional definitions.

Definition 4.10 *Let S, T be constellations, and let $t(x,y) \in \mathcal{A}$. S is* connectable to T by $t(x,y)$ *if $center(S) \subseteq t(x,y)$, $center(T) \subseteq t^*(x,y)$ and,*

1. *$t \in S$ and $t^* \in T$ if $t \in \mathcal{A}^{\leftrightarrow}$,*
2. *$t \in S$ if $t \in \mathcal{A}^{\rightarrow}$,*
3. *$t^* \in T$ if $t \in \mathcal{A}^{\leftarrow}$.*

Definition 4.11 *Let $\mathcal{S}$ be a galaxy, and assume that $\mathfrak{A}$ realizes $\mathcal{S}$. Define a function $rank_{\mathfrak{A}} : \mathcal{S} \to \mathbb{N} \cup \{\infty\}$ putting $rank_{\mathfrak{A}}(S) = card(\{a \in A : C_a^{\mathfrak{A}} = S\})$.*

We write $rank(\mathcal{S}) = \infty$ if there is a structure $\mathfrak{B}$ realizing $\mathcal{S}$ such that $min_{S \in \mathcal{S}}(rank_{\mathfrak{B}}(S)) > 2m+1$.

Lemma 4.12 *Assume that $\mathfrak{A}$ is a structure which realizes $\mathcal{S}$. Let $S, T \in \mathcal{S}$. If $rank_{\mathfrak{A}}(S) > 2m+1$, and $rank_{\mathfrak{A}}(T) > 2m+1$, then there exist $a, b \in A$ such that $C_a^{\mathfrak{A}} = S$, $C_b^{\mathfrak{A}} = T$, and $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^-$.*

Proof. Let $X = \{a \in A : C_a^{\mathfrak{A}} = S\}$, $Y = \{a \in A : C_a^{\mathfrak{A}} = T\}$, and assume that $card(X) \geq card(Y) > 2m+1$.

By Definition 4.4, for every $a \in X$ ($a \in Y$) there is at most m distinct elements b such that $tp^{\mathfrak{A}}(a,b) \in S$ ($tp^{\mathfrak{A}}(a,b) \in T$, respectively). So, the number of pairs $\langle a, b\rangle$ such that $a \in X$, $b \in Y$ and $tp^{\mathfrak{A}}(a,b) \in S$ or $tp^{\mathfrak{A}}(b,a) \in T$ does not exceed $m \cdot card(X) + m \cdot card(Y) \leq 2m \cdot card(X)$. On the other hand, the number of pairs $\langle a, b\rangle$ such that $a \in X$ and $b \in Y$ is $card(X) \cdot card(Y) > (2m+1)card(X)$. □

Corollary 4.13 *Let $\mathcal{S}$ be a galaxy with $rank(\mathcal{S}) = \infty$. Then there exists a structure $\mathfrak{B}$ realizing $\mathcal{S}$ such that $rank_{\mathfrak{B}}(S) = \infty$, for each $S \in \mathcal{S}$.*

Proof. Assume that $\mathfrak{A}$ realizes $\mathcal{S}$, $S \in \mathcal{S}$, and $rank_{\mathfrak{A}}(S) = n$. We claim that there is an extension $\mathfrak{B}$ of $\mathfrak{A}$, such that $\mathfrak{B}$ realizes $\mathcal{S}$, and $rank_{\mathfrak{B}}(S) > n$. By Lemma 4.12, for all constellations $S, T \in \mathcal{S}$, there exists a type $t(x,y) \in \mathcal{A}^-$ such that S is connectable to T by $t(x,y)$. Let $\mathfrak{A}'$ be a structure isomorphic to $\mathfrak{A}$ such that $A \cap A' = \emptyset$. Define $B = A \cup A'$, and let $\mathfrak{B} \restriction A = \mathfrak{A}$, $\mathfrak{B} \restriction A' = \mathfrak{A}'$. Now, for every $a \in A$, and every $a' \in A'$ find $t(x,y) \in \mathcal{A}^-$ such that $C_a^{\mathfrak{A}}$ is connectable to $C_{a'}^{\mathfrak{A}'}$ by $t(x,y)$, and put $tp^{\mathfrak{B}}(a,a') = t(x,y)$. □

Proposition 4.14 *The following conditions are equivalent:*

1. *$rank(\mathcal{S}) = \infty$*
2. *(a) for every $S \in \mathcal{S}$, and every $s(x,y) \in S$, there exists $T \in \mathcal{S}$ such that S is connectable to T by $s(x,y)$,*
   (b) for every $S, T \in \mathcal{S}$, S is connectable to T by some $t(x,y) \in \mathcal{A}^-$.

Proof. (1) $\Rightarrow$ (2). Condition (a) follows from Definition 4.5 and condition (b) – from Lemma 4.12.

(2) $\Rightarrow$ (1). We shall give an algorithm which constructs a structure $\mathfrak{A}$ realizing $\mathcal{S}$. In the process of construction new elements will be added to the universe, some elements of the universe will be inactivated and some unordered pairs of elements will be reserved. An

element a will be inactivated when the constellation S that had been earlier assigned to a has been built, i.e. when elements which witness that a realizes S have been added. An unordered pair $\{a,b\}$ will be reserved, when the type realized by $\{a,b\}$ has been defined. Moreover, a function $I : A \mapsto \mathcal{S}$ will be defined in such a way that $I(a) = C_a^{\mathfrak{A}}$, for every $a \in A$.

In every step of the construction the part of the model defined so far $\mathfrak{A}$ will be finite. We assume that a linear ordering $<$ of the universe is given such that a new element added to the universe is always greater then the old elements.

Let $\mathcal{S} = \{S_1, \ldots, S_k\}$.

1. Let $A = \{a_1, \ldots, a_k\}$. Put $I(a_i) = S_i$, $i = 1, \ldots, k$.
2. Let $a \in A$ be the first active (not yet inactivated) element.
3. For every $t_i \in I(a)$, if there is no element $b \in A$ such that $\{a,b\}$ is reserved, and $tp^{\mathfrak{A}}(a,b) = t_i$, then
   (a) add a new element b_i to A,
   (b) put $tp^{\mathfrak{A}}(a,b_i) = t_i$,
   (c) find a constellation $T \in \mathcal{S}$ such that S is connectable to T by t_i,
   (d) put $I(b_i) = T$, and reserve $\{a,b_i\}$.
4. For every $c < a$ put $tp^{\mathfrak{A}}(a,c) = t \in \mathcal{A}^-$ such that $I(a)$ is connectable to $I(c)$ by t.
5. Inactivate a.
6. Go to 2.

If $min_{S\in\mathcal{S}}(rank_{\mathfrak{A}}(S)) \leq 2m+1$, perform the operations from the proof of Corollary 4.13. □

Lemma 4.15 *Assume that $\mathfrak{A}$ realizes $\mathcal{S}$. Let V be a finite subset of A and let $\mathcal{S}' = \{C_a^{\mathfrak{A}} : a \in A \setminus V\}$. If $\mathcal{S}' \cap \{C_a^{\mathfrak{A}} : a \in V\} = \emptyset$, and for every $a \in A \setminus V$, $rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) > max(card(V) \cdot m, 2m+1)$, then there is a structure $\mathfrak{B}$ realizing $\mathcal{S}$, such that for every $S \in \mathcal{S}'$ $rank_{\mathfrak{B}}(S) = \infty$, and $rank_{\mathfrak{B}}(S) = rank_{\mathfrak{A}}(S)$, for every $S \in \mathcal{S} \setminus \mathcal{S}'$.*

Proof. Let $\mathfrak{A}$ realize $\mathcal{S}$.

An iterative application of the following algorithm applied to every $S \in \mathcal{S}'$ yields a structure $\mathfrak{B}$ such that $rank_{\mathfrak{B}}(S) = \infty$, for every $S \in \mathcal{S}'$, and $rank_{\mathfrak{B}}(S) = rank_{\mathfrak{A}}(S)$, for every $S \in \mathcal{S} \setminus \mathcal{S}'$ (inactivation, reserving elements and the function I play the same role as in the proof of Proposition 4.14). At the beginning, put $\mathfrak{A}'$=$\mathfrak{A}$.

1. Let $A'' = A' \cup \{x\}$.
2. For every $a \in A'$ put $I(a) = C_a^{\mathfrak{A}'}$, and inactivate a.
3. Put $I(x) = S$.
4. Let x be the first active element of A''.
5. Find $a \in A \setminus V$ such that $C_a^{\mathfrak{A}} = I(x)$, and $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^- \cup \mathcal{A}^{\rightarrow}$, for every $b \in V$. Such an element a exists, since there are at most $m \cdot card(V)$ elements $c \in A \setminus V$ such that $tp^{\mathfrak{A}}(c,b) \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\leftarrow}$.
6. For every $t_i \in S$
   (a) if there is $b \in V$ such that $tp^{\mathfrak{A}}(a,b) = t_i$ then put $tp^{\mathfrak{A}}(x,b) = t_i$, and reserve $\{x,b\}$ else

(b) if there is no element $d \in A''$ such that $\{x, d\}$ is reserved and $tp^{\mathfrak{A}''}(x, d) = t_i$, then add a new element b_i to A'',
put $tp^{\mathfrak{A}}(x, b_i) = t_i$, reserve $\{x, b_i\}$,
find $a_i \in A \setminus V$ such that $tp^{\mathfrak{A}}(a, a_i) = t_i$, and put $I(b_i) = I(a_i)$.

An element a_i can be found since $C_a^{\mathfrak{A}} = S$ and therefore there is an element $c_i \in A$ such that $tp^{\mathfrak{A}}(a, c_i) = t_i$. Since $c_i \in A \setminus V$, and $\mathfrak{A}$ realizes $\mathcal{S}$ we have $I(c_i) = C_{c_i}^{\mathfrak{A}} \in \mathcal{S}'$.)

7. For every $c < x$, if $\{c, x\}$ is not reserved, put $tp^{\mathfrak{A}''}(x, c) = t \in \mathcal{A}^-$ such that $I(x)$ is connectable to $I(c)$ in $\mathfrak{A}$ by t, and reserve $\{x, c\}$.
(By Lemma 4.12, for every $S, T \in \mathcal{S}'$, S is connectable to T in $\mathfrak{A}$ by some $t \in \mathcal{A}^-$.)
8. Inactivate x.
9. Go to 4.

One application of the above algorithm to the constellation $S \in \mathcal{S}'$ and the structure $\mathfrak{A}'$ expands the structure $\mathfrak{A}'$ to a structure $\mathfrak{A}''$ such that $rank_{\mathfrak{A}''}(S) > rank_{\mathfrak{A}'}(S)$.

In step 6, when the types $tp^{\mathfrak{A}''}(x, b)$ are defined, where $b \in V$, the constellation realized by b does not change, since $tp^{\mathfrak{A}''}(x, b) \in \mathcal{A}^{\rightarrow}$. Also in step 7, the constellations realized by the elements $c < x$ are not changed since only types in $\mathcal{A}^-$ are used.

Every $x \in A''$ is eventually inactivated since new elements b_i are added at the end of the ordering. When an element x is inactivated it is ensured that for every $c < x$, $tp^{\mathfrak{A}''}(c, x)$ is defined, and $C_x^{\mathfrak{A}''} \in \mathcal{S}$. □

Lemma 4.16 *Let $\mathcal{S}$ be a galaxy. There is a constant r, $r = O(m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$, and there exists a structure $\mathfrak{B}$ realizing $\mathcal{S}$ such that $rank_{\mathfrak{B}}(S) < r$ or $rank_{\mathfrak{B}}(S) = \infty$, for every $S \in \mathcal{S}$.*

Proof. Let $\mathfrak{A}$ realize $\mathcal{S}$. It suffices to define $V \subseteq A$ of appropriate cardinality which satisfies the conditions of Lemma 4.15.

The set V will be constructed in stages.

Stage 1. Let $V_1 = \{a \in A : rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) \leq 2m + 1\}$.
Note that if $V_1 = \emptyset$ then by Corollary 4.13, there is a structure $\mathfrak{B}$ such that for every $S \in \mathcal{S}$, $rank_{\mathfrak{B}}(S) = \infty$. In this case only stages 1 and 2 are performed.

Stage i. $(i > 1)$

1. If $rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) > card(V_{i-1}) \cdot m$, for every $a \in A \setminus V_{i-1}$,
then put $V_i = V_{i-1}$ and **stop**.
2. Put $V_i = V_{i-1} \cup \{a \in A \setminus V_{i-1} : rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) \leq card(V_{i-1}) \cdot m\}$.
3. Go to Stage $i + 1$.

Note that there is a stage i such that $V_i = V_{i-1}$. Indeed, for every stage i, let $C(V_i) = \{S \in \mathcal{S} :$ there is $a \in V_i$ such that $C_a^{\mathfrak{A}} = S\}$. Hence, for every $i > 1$, if $V_i \neq V_{i-1}$ then $C(V_i) \supset C(V_{i-1})$. So, since $\mathcal{S}$ is finite, the number p of stages performed is less or equal $card(\mathcal{S})$. Put $V = V_p$.

Now, we estimate $card(V)$. We have $card(V_1) \leq (2m + 1) \cdot card(\mathcal{S})$, and, for $i > 1$,

$$card(V_i) \leq card(V_{i-1}) + m \cdot card(V_{i-1}) \cdot (1 + m \cdot card(\mathcal{S})).$$

If we put $q = 1 + m \cdot card(\mathcal{S})$, then we have $card(V_1) \leq 3q^p$. Moreover, for every $a \in V$, $rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) \leq card(V)$, and for every $a \in A \setminus V, rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) > card(V) \cdot m$. Put $r = 3 \cdot (1 + m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$. This by Lemma 4.15, finishes the proof. □

Now, we are ready to introduce the main definition of this section.

Definition 4.17 *Let $\mathcal{S}$ be a set of constellations. A* finite representation of $\mathcal{S}$ *is a system*

$$\langle \mathcal{S}_1, V, C, I, F, G \rangle,$$

where $\mathcal{S}_1$ is a set of constellations , V and C are sets, I, F, G are functions such that
$I : C \mapsto \mathcal{S}, \quad F : C \times C \to \mathcal{A}, \quad G : (\mathcal{S} \setminus \mathcal{S}_1) \times V \to \mathcal{A},$
and the following conditions hold

(f1) $\mathcal{S}_1 \subseteq \mathcal{S}$, $V \subseteq C$, *and* $card(C) \leq m \cdot (2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$,

(f2) $I(V) = \mathcal{S}_1$, $I(C \setminus V) \subseteq \mathcal{S} \setminus \mathcal{S}_1$,
$F(a,a) = F(a,b)\restriction\{x\}$, *and for every* $a \neq b$, $F(a,b) = F(b,a)^*$,
$G : (\mathcal{S} \setminus \mathcal{S}_1) \times V \to \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{-}$,

(f3) For every $b \in C$ *define* $D(b) = \{F(b,c) : c \in C, c \neq b, F(b,c) \in \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}\}$. *Then*

   (a) for every $b \in C$, *and every* $t \in D(b)$ *there is exactly one* $c \in C, c \neq b$ *such that* $F(b,c) = t$,

   (b) $D(a) = I(a)$, *for every* $a \in V$,

   (c) for every $b \in C \setminus V$ *we have* $D(b) \subseteq I(b)$, *and for every* $t \in I(b) \setminus D(b)$ *there is* $T \in \mathcal{S} \setminus \mathcal{S}_1$ *such that* $I(b)$ *is connectable to* T *by* t,

(f4) for every $S, T \in \mathcal{S} \setminus \mathcal{S}_1$, S *is connectable to* T *by some* $t \in \mathcal{A}^{-}$,

(f5) for every $S \in \mathcal{S} \setminus \mathcal{S}_1$ *we have* $\{G(S,a) \in \mathcal{A}^{\rightarrow} : a \in V\} \subseteq S$, *and for every* $a \in V$, S *is connectable to* $I(a)$ *by* $G(S,a)$

(f6) for every $S \in \mathcal{S} \setminus \mathcal{S}_1$, *and every* $t \in S$, *if* $t \in \mathcal{A}^{\rightarrow}$ *and there is no* $T \in \mathcal{S} \setminus \mathcal{S}_1$ *such that* S *is connectable to* T *by* t *then there is a unique* $a \in V$ *such that* $G(S,a) = t$,

(f7) for every $S \in \mathcal{S} \setminus \mathcal{S}_1$, *and every* $t \in S$, *if there is no* $a \in V$ *such that* $G(S,a) = t$ *then there is* $T \in \mathcal{S} \setminus \mathcal{S}_1$ *such that* S *is connectable to* T *by* t.

We say that $\mathcal{S}$ is finitely representable, *if there is a finite representation of $\mathcal{S}$.*

Let us note that the notion of a finite representation is almost identical with the notion of small representation (Definition 3.12). The role of replicable small constellations is taken here by constellations in $\mathcal{S} \setminus \mathcal{S}_1$.

Theorem 4.18 (Galaxy Theorem) *A set of constellations $\mathcal{S}$ is a galaxy if and only if $\mathcal{S}$ is finitely representable.*

Proof. ($\Rightarrow$) Let $\mathcal{S}$ be a galaxy. Use Lemma 4.16 to get a structure $\mathfrak{A}$ and a constant r such that $\mathfrak{A}$ realizes $\mathcal{S}$, and for every $S \in \mathcal{S}$, $rank_{\mathfrak{A}}(S) < r$ or $rank_{\mathfrak{A}}(S) = \infty$. Put
$\mathcal{S}_1 = \{S \in \mathcal{S} : rank_{\mathfrak{A}}(S) < r\}$,
$V = \{a \in A : rank_{\mathfrak{A}}(C_a^{\mathfrak{A}}) < r\}$,
$C = V \cup \{a \in A :$ there is $b \in V$ such that $tp^{\mathfrak{A}}(b,a) \in \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}\}$.
Note that if $S \in \mathcal{S} \setminus \mathcal{S}_1$ then $rank_{\mathfrak{A}}(S) = \infty$. For every $a \in V$, put $I(a) = C_a^{\mathfrak{A}}$. For every $a, b \in C, a \neq b$, put $F(a,b) = tp^{\mathfrak{A}}(a,b)$. For every $S \in \mathcal{S} \setminus \mathcal{S}_1$ find $a \in A \setminus C$ such that $C_a^{\mathfrak{A}} = S$, and for every $c \in V$ put $G(S,c) = tp^{\mathfrak{A}}(a,c)$.
It is easy to check that conditions (f1)-(f7) of Definition 4.17 hold.

($\Leftarrow$) Let $\langle \mathcal{S}_1, V, C, I, F, G \rangle$ be a finite representation of $\mathcal{S}$.

Case 1. $\mathcal{S}_1 = \emptyset$. By condition (f2), $V = \emptyset$. Consequently conditions (f7) and (f4) are equivalent to conditions (a) and (b) of Proposition 4.14.

Case 2. $\mathcal{S}_1 = \mathcal{S}$. By condition (f2), $V = C$. Therefore, by conditions (f1)-(f3), we can define $\mathfrak{B}$ realizing $\mathcal{S}$ with universe V in which $tp^{\mathfrak{B}}(a, b) = F(a, b)$, for every $a, b \in V$.

Case 3. $\mathcal{S}_1 \neq \emptyset$ and $\mathcal{S}_1 \neq \mathcal{S}$. We shall construct a structure $\mathfrak{A}$ realizing $\mathcal{S}$ with the universe A ($A \supseteq C$). In our infinite construction, inactivation and reservation have the same role as in the previous algorithms. Additionally, function I will be extended to all elements of A in such a way that for every $b \in A$, $I(b) = C_b^{\mathfrak{A}}$. In each step of construction the universe of partially defined model $\mathfrak{A}$ will be finite, and we assume that there is a fixed linear ordering on the universe such that any new element added to the universe is greater then the old ones.

Stage 1.

1. Let $A = C$.
2. For every $a, b \in C$, put $tp^{\mathfrak{A}}(a, b) = F(a, b)$ (cf. (f2)).
3. For every $a \in V$, inactivate a.
4. For every $a, b \in C$, reserve $\{a, b\}$.
5. For every $S \in \mathcal{S} \setminus \mathcal{S}_1$, if there is no $b \in C$ such that $I(b) = S$, then add a new element d to A and put $I(d) = S$.

Stage 2.

6. Let b be the first active element of A (note that $I(b) \in \mathcal{S} \setminus \mathcal{S}_1$).
7. If $b \in C$ then
   (a) for every $t \in I(b) \setminus D(b)$ do
      i. find $T \in \mathcal{S} \setminus \mathcal{S}_1$ such that $I(b)$ is connectable to T by t (use (f3-c)),
      ii. add a new element d to A and put $I(d) = T$,
      iii. put $tp^{\mathfrak{A}}(b, d) = t$ and reserve $\{b, d\}$,
   (b) inactivate b and go to 6.
8. For every $a \in V$, put $tp^{\mathfrak{A}}(b, a) = G(I(b), a)$ (use (f5) and (f6)).
9. For every $t \in I(b)$, if there is no $c \in A$ such that $\{c, b\}$ is reserved, and $tp^{\mathfrak{A}}(c, b) = t^*$ then
   (a) find $T \in \mathcal{S} \setminus \mathcal{S}_1$ which is connectable to $I(b)$ by t^* (use (f7)),
   (b) add a new element d to A, and put $I(d) = T$,
   (c) put $tp^{\mathfrak{A}}(b, d) = t$, and reserve $\{b, d\}$.
10. For every $a < b$, if $\{a, b\}$ is not reserved then using (f4)) find $t \in \mathcal{A}^-$ such that $I(b)$ is connectable to $I(a)$ by t, put $tp^{\mathfrak{A}}(b, a) = t$ and reserve $\{b, a\}$.
11. Inactivate b and go to 6.

After performing stage 1, every $a \in V$ realizes the constellation $I(a) \in \mathcal{S}$ in the partially defined structure $\mathfrak{A}$, by f(2) every constellation $S \in \mathcal{S}_1$ is realized by some $a \in V$, and only elements of V have been inactivated. Moreover, for every $S \in \mathcal{S}$, there is $b \in A$ such that $I(b) = S$.

The role of stage 2 is to realize all constellations of $\mathcal{S} \setminus \mathcal{S}_1$ by elements of A. Step 7 is executed if, at stage 1, some types between the chosen b and the other elements of A were defined using function F. For every type of $I(b)$ that has not been defined, a new element d is added to A, and some $T \in \mathcal{S} \setminus \mathcal{S}_1$ is put as $I(d)$. So, only constellations of $\mathcal{S} \setminus \mathcal{S}_1$ have to be realized in the next steps. In step 10, when the types between an element b and smaller, already inactivated, elements are defined, the constellation realized by the earlier elements are not changed because only types in $\mathcal{A}^-$ are used.

Every $b \in A$ is eventually inactivated since new elements are added at the end of the ordering. When an element b is inactivated it is ensured that $C_b^{\mathfrak{A}} \in \mathcal{S}$. □

Corollary 4.19 *If $\langle \mathcal{S}_1, V, C, I, F, G \rangle$ is a finite representation of $\mathcal{S}$ then there exists a structure $\mathfrak{A}$ realizing $\mathcal{S}$, such that $A = C \cup B$, for every $a \in B$, $rank_{\mathfrak{A}}(C_b^{\mathfrak{A}}) = \infty$, and conditions (f1)-(f7) hold.*

Proof. (Sketch) Take $\mathfrak{A}$ given by part ($\Leftarrow$) of the proof of Theorem 4.18. □

4.4 Complexity

In this subsection, using the Galaxy Theorem proved in the previous subsection, we provide an algorithm solving the satisfiability problem for $\mathcal{C}_1^2$. This algorithm works in nondeterministic, double exponential time. In the next section, using more sophisticated techniques, we will show that this bound can be improved.

Corollary 4.20 SAT($\mathcal{C}_1^2$) $\in$ 2-NEXPTIME.

Proof. We describe a nondeterministic algorithm which for every sentence $\Phi \in \mathcal{C}_1^2$ decides if Φ is satisfiable, and works in time doubly exponential with respect to the length of Φ.

Let Φ be a $\mathcal{C}_1^2$-sentence of length n. In the first step we use the polynomial time algorithm from Corollary 4.8 to obtain a sentence Ψ in $\exists^{=1}$-constellation form

$$\Psi = \forall x \forall y \phi(x, y) \wedge \bigwedge_{1 \le i \le m} \forall x \exists^{=1} y R_i(x, y)$$

which is satisfiable if and only if Φ is satisfiable. Moreover Ψ has at most $p = O(n)$ predicate letters, and has length $O(n \log n)$.

Then we use Theorem 4.6. We build the set $\mathcal{A}$ in time $O(2^{4p})$, and we guess a set $\mathcal{S}$ of $\mathcal{A}$-$\mathcal{R}$-constellations. Note that $card(\mathcal{A}) \le 2^{4p}$, and $card(\mathcal{S}) \le (2^{4p})^m$, where $m = card(\mathcal{R})$ is the number of existential quantifiers in Ψ. Therefore $\mathcal{S}$ can be guessed in time $(2^{4p})^m \cdot m \cdot 4p = O(2^{O(n^2)})$.

Next, we apply Theorem 4.18 and guess sets $\mathcal{S}_1$, V, and C, as well as functions I, F, and G as in Definition 4.17. Since $\mathcal{S}_1 \subseteq \mathcal{S}$, and $card(V) \le card(C) \le m \cdot (2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$ we can guess the components in time:

$$\begin{array}{rcl} \mathcal{S}_1 & — & O(card(\mathcal{S})) = O(2^{O(n^2)}), \\ V \text{ and } C & — & O(m(2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}) = O(2^{2^{O(n^2)}}), \\ I, F & — & O((card(C)^2) = O(2^{2^{O(n^2)}}), \\ G & — & O(card(\mathcal{S} \setminus \mathcal{S}_1) \cdot card(V)) = O(2^{2^{O(n^2)}}). \end{array}$$

So, the time required for this step is bounded by $O(2^{2^{cn^2}})$, for some constant c.

Finally, we check whether the system $\langle \mathcal{S}, \mathcal{S}_1, V, C, I, F, G \rangle$ is a finite representation of $\mathcal{S}$. It is easy to see that this can also be done in time $O(2^{2^{cn^2}})$. □

4.5 An example

It is well-known that the class $\mathcal{C}_1^2$ admits axioms of infinity, i.e. there are satisfiable sentences of $\mathcal{C}_1^2$ that have only infinite models. Using the notion of a finite representation, in the proof of Corollary 4.20 we have described an algorithm solving the satisfiability problem for sentences in constellation form, which did not depend on constructing a complete model.

The size of the finite representation $\langle \mathcal{S}_1, V, C, I, F, G\rangle$ of a set of constellations $\mathcal{S}$ depends mainly on the cardinality of the set C. It is bounded in Definition 4.17 by a number that is exponential with respect to the number of constellations in $\mathcal{S}$ and double exponential with respect to the number of predicate letters in the signature.

Below we give an example Φ of a sentence in $\mathcal{C}_1^2$ which has finite models, and is such that for every finite representation $\langle \mathcal{S}_1, V, C, I, F, G\rangle$ of the set of constellations realized in a model of Φ, the cardinality of C is doubly exponential. In this example, following the idea of H. Lewis's proof [27] that NEXPTIME is reducible to the monadic Gödel class, we use a consize representation of the successor relation between encodings of natural numbers that is reminiscent to that used by N. Jones and A. Selman in [23].

Let n be a positive integer.

Let $\mathcal{L} = \{B_1, \ldots, B_n, C_0, C_1, \ldots, C_n, \mathit{Root}, \mathit{Leaf}, \mathit{Left}, \mathit{Right}, \mathit{In}, R\}$, where B_i, C_i, *Root*, *Leaf* are monadic predicate letters and *Left*, *Right*, *In*, R are binary predicate letters. The sentence Φ will describe the unique model (up to isomorphism) that is a full binary tree of height $2^n - 1$.

The sentence Φ is a conjunction of the following sentences.

$$
\begin{aligned}
&\forall x \exists^{=1} y\ R(x,y),\\
&\forall x \exists^{=1} y\ \mathit{Left}(x,y),\\
&\forall x \exists^{=1} y\ \mathit{Right}(x,y),\\
&\forall x \exists^{=1} y\ \mathit{In}(x,y),\\
&\forall x \forall y\ \mathit{Root}(x) \wedge \mathit{Root}(y) \rightarrow x = y,\\
&\forall x \forall y\ R(x,y) \rightarrow \mathit{Root}(y),\\
&\forall x \forall y\ \neg[\mathit{Left}(x,y) \wedge \mathit{Right}(x,y)] \vee \mathit{Leaf}(x),\\
&\forall x\ \mathit{Leaf}(x) \rightarrow [\mathit{Left}(x,x) \wedge \mathit{Right}(x,x)],\\
&\forall x \forall y\ \mathit{In}(x,y) \rightarrow [\neg \mathit{Leaf}(y) \wedge (\mathit{Left}(y,x) \vee \mathit{Right}(y,x))\\
&\qquad \vee \mathit{Root}(x) \wedge \mathit{Root}(y)],\\
&\forall x\ \mathit{Root}(x) \leftrightarrow \textstyle\bigwedge_{0 \le i < n} \neg B_i(x),\\
&\forall x\ \mathit{Leaf}(x) \leftrightarrow \textstyle\bigwedge_{0 \le i < n} B_i(x),\\
&\forall x\ C_0(x) \wedge [\textstyle\bigwedge_{0 \le i < n} (C_i(x) \leftrightarrow (C_{i-1}(x) \wedge B_i(x)))],\\
&\forall x \forall y\ [\neg \mathit{Leaf}(x) \wedge (\mathit{Left}(x,y) \vee \mathit{Right}(x,y))] \rightarrow\\
&\qquad \textstyle\bigwedge_{0 \le i < n} [B_i(y) \leftrightarrow \neg(B_i(x) \leftrightarrow C_{i-1}(x))].
\end{aligned}
$$

The sentence Φ is a slight modification of the example given in [29]. A similar example can also be found in [16]. It is worth noticing that Φ is in $\exists^{=1}$-constellation form. We have here $\mathcal{R} = \{\mathit{In}, \mathit{Left}, \mathit{Right}, R\}$.

Proposition 4.21 *The sentence Φ is satisfiable and, if $\mathfrak{A}$ realizes Φ then $card(\mathfrak{A}) = 2^{2^n} - 1$.*

Proof. Let, for every d, $0 \le d \le 2^n - 1$, Level_d denote the unique 1-type over the set $\{B_1, \ldots, B_n\}$ such that $B_i(x) \in \mathit{Level}_d$ if and only if the i-th bit of d in the binary notation is 1.

It is easy to see that a full binary tree $\mathfrak{T}$ (see Fig. 0) is the unique model of Φ with the interpretations for the predicate letters such that for every $a, b \in \mathfrak{T}$

$Root(a)$	iff	a is the root of $\mathfrak{T}$,
$Leaf(a)$	iff	a is a leaf of $\mathfrak{T}$,
$Left(a,b)$	iff	b is the immediate left successor of a or $a = b$ is a leaf of $\mathfrak{T}$,
$Right(a,b)$	iff	b is the immediate right successor of a or $a = b$ is a leaf of $\mathfrak{T}$,
$In(a,b)$	iff	b is the immediate predecessor of a or $a = b$ is the root of $\mathfrak{T}$,
$Level_d(a)$	iff	the distance from the root to a is equal to d.

Since the remaining predicates are explicitly defined by Φ, their interpretations can be derived from the interpretations above.

Note that for every d, $0 \le d \le 2^n - 1$, there is $a \in T$ such that $Level_d(a)$, and for every $a \in T$, $Leaf(a)$ if and only if $Level_{2^n-1}(a)$. □

5 The main result

The main result of this paper is the following theorem.

Theorem 5.1 SAT($\mathcal{C}_1^2$) $\in$ NEXPTIME.

We begin this section by providing some intuition arising from a close analysis of the example given in Subsection 4.5. Then we define a notion of a *concise representation* of a set of constellations which will play a similar role to the notion of finite representation but will require less space. Finally, we show how to use this notion to get a nondeterministic decision procedure working in exponential time, and solving the satisfiability problem for C_1^2. In the last step we use graph-theoretical notions and results given in section 6.

5.1 Example continued

In this subsection we want to provide some intuition on how to improve the double exponential upper complexity bound for C_1^2. This will be done by discussing in greater detail the example from Subsection 4.5 of the sentence Φ that describes a binary tree of exponential height.

Let us first examine the types and constellations realized in the model of Φ (see Fig. 0). For every pair of elements x and y such that y is an immediate successor of x, x and y are joined with a thin or a thick line depending on whether $Left(x,y)$ or $Right(x,y)$ holds and then also, $In(y,x)$ holds. Moreover, every element x of the tree should in the picture be joined to the root by a line representing $R(x,\text{root})$.

For every element x, the unique 1-type realized by x contains positive formulas of the form $B_i(x)$ for those and only those B_i-s which are listed on the right margin. The values of C_i-s on x are determined by the values of B_i-s. If an element x is neither the root nor a leaf then the 1-type realized by x does not contain any positive appearance of other predicate letters.

Below, when describing types, we list only atomic formulas with both x and y, omitting the remaining two-variable conjuncts which are negations of atomic formulas that are not listed. The elements on the same level $d > 0$ of the tree realize constellations of two kinds with the same center. For $d = 2, 3 \ldots, 2^n - 3$ we have the following constellations, each containing exactly four 2-types

$S = \{Left(y,x) \wedge In(x,y), Left(x,y) \wedge In(y,x), Right(x,y) \wedge In(y,x), R(x,y)\}$,

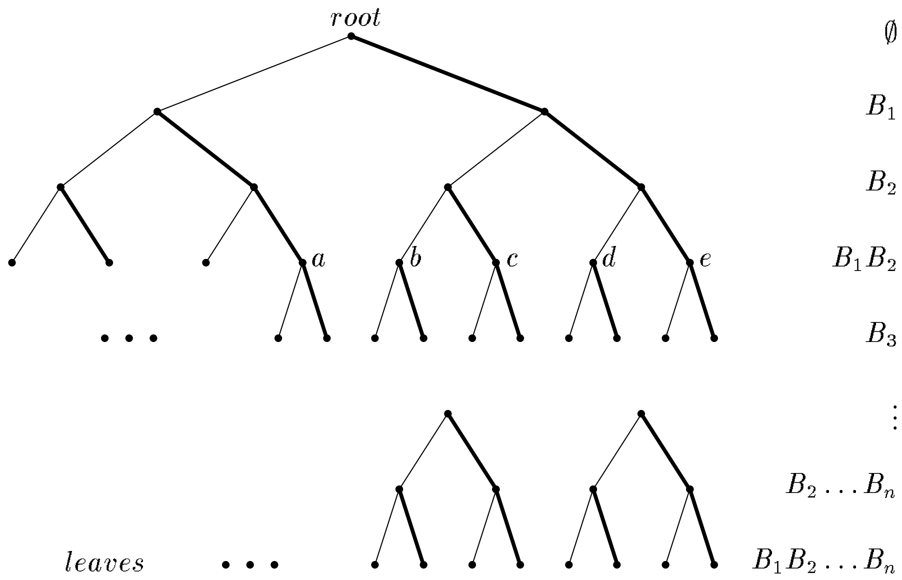

Figure 0: The model for Φ

$T = \{Right(y,x) \wedge In(x,y), Left(x,y) \wedge In(y,x), Right(x,y) \wedge In(y,x), R(x,y)\}$.

So, elements denoted by a, c and e realize the constellation T, and the constellation S is realized by b and d.

The constellations realized on the first level include exactly three 2-types:

$S = \{Left(y,x) \wedge In(x,y) \wedge R(x,y), Left(x,y) \wedge In(y,x), Right(x,y) \wedge In(y,x)\}$,

$T = \{Right(y,x) \wedge In(x,y) \wedge R(x,y), Left(x,y) \wedge In(y,x), Right(x,y) \wedge In(y,x)\}$.

The root and the leaves realize constellations containing exactly two 2-types. The root realizes the constellation

$S = \{Left(x,y) \wedge In(y,x) \wedge R(y,x), Right(x,y) \wedge In(y,x) \wedge R(y,x)\}$

and $\{In(x,x), R(x,x)\} \subset center(S)$.

If x is a leaf then

$S = \{Left(y,x) \wedge In(x,y), R(x,y)\}$,

$T = \{Right(y,x) \wedge In(x,y), R(x,y)\}$,

and $\{Left(x,x), Right(x,x)\} \subset center(S) = center(T)$.

Note that since elements on different levels of the tree realize distinct constellations, the number of constellations realized in $\mathfrak{T}$ is exponential with respect to the number of predicate letters in $\mathcal{L}$. Moreover, the number of vassals, $card(V)$, is exponential with respect to the number of constellations realized in $\mathfrak{T}$. So, the number of elements that are indistinguishable from the point of view of constellation they realize can be double exponential.

One could imagine that in order to check whether a sentence in $\exists^{=1}$-constellation form is satisfiable it is not necessary to have the complete submodel with the universe C defined by the finite representation but it should be sufficient to know which constellations are realized in the submodel, and in which number. It is, however, hard to adapt this idea directly.

Note that some elements that realize the same constellation in a given model can be distinguished by taking into account constellations that are realized by partners of the constellations – elements connected to them with a counting type. For example, elements a and c

of the tree shown in Fig. 0 realize the same constellation but they can be distinguished, since the predecessor of a realizes a constellation of kind T whereas the predecessor of c realizes a constellation of kind S. Elements a and e, however, remain indistinguishable even if we take into account the additional information.

The above remarks suggest that in order to push the complexity down, a potential model can be described by a set of *indexed* constellations, and numbers of elements that realize these constellations. Roughly speaking, an indexed constellation in addition to the information on two-types realized by an element, carries requests for partner constellations that should realize, together with the host, the two-types of the host constellation.

5.2 Concise representation

At the end of section 4.3 using the Galaxy Theorem which allows to transform the problem whether a set of constellations is a galaxy into the problem whether the same set is finitely representable, we gave an algorithm solving the satisfiability problem for C_1^2. As it was shown in the previous subsection, the size of a finite representation can be exponential with respect to the number of constellations.

In this section we shall define the notion of a concise representation of a set of constellations which will play a similar role to finite representation but will use only polynomial space with respect to the number of constellations.

We need several additional notions, the most important of which are the notion of an *indexed constellation* (Definition 5.5) and of a *$\mathcal{X}$-rnk-model* (Definition 5.9). An indexed constellation is a pair $\langle S, f\rangle$, where S is a constellation and f is a function that associates a constellation T to each two-type of S. This definition allows to control not only which constellation S is realized by an element a, but also which constellations are realized in the neighborhood of a, that is by elements that together with a realize two-types of S.

Definition 5.9 describes a model very precisely. It says which indexed constellations are realized, and in which amount. Additionally, it allows to partition a model into parts, each part containing elements realizing the same indexed constellation, and it specifies two-types that can be realized by elements from these parts.

The first easy fact proved here (Proposition 5.10) gives several necessary conditions for a set of constellations to be a galaxy. These conditions are described in terms of new notions introduced below. We hope that through studying this easy proposition the reader will get familiar with the complex terminology and notation use here. It should also provide a good background for the most important notion of concise representation.

Lemma 5.12 is an analogue of the Galaxy Theorem, and one could think that it could form a basis to formulate another algorithm for the satisfiability problem for C_1^2, as in section 4.3. However, although the space needed to write a concise representation is small, and most of the conditions of the definition of concise representation are easily[2] computable, condition (c5), however, seems to require still double exponential time since it requires checking whether there exists a model of double exponential cardinality, which in addition satisfies some conditions. As a first step towards removing this difficulty we prove the Decomposition Theorem (Lemma 5.15) that shows that such a model is composed of a certain number of parts which can be treated separately and independently. Unfortunately, to check if the parts can be constructed we need several technical lemmas.

[2] Here, "easily" means in exponential time

Let $\mathcal{R} \subseteq \mathcal{L}$ be a fixed set of predicate letters with $card(\mathcal{R}) = m$. Let $\mathcal{A}$ be a fixed set of 2-types closed under the operation *, and let $\mathcal{S}$ be a set of constellations $\mathcal{S} = \{S_1, \ldots, S_w\}$.

Definition 5.2 *Let $S \in \mathcal{S}$. A set S' of types is a* sub-constellation of S *if $S' \subseteq S$ and $center(S) \in S'$.*

Note that a sub-constellation S' of S is a constellation (cf. Definition 4.3) only if $S' = S$.

Definition 5.3 *Let $\mathfrak{A}$ be an $\mathcal{L}$-structure, and let $S' = \{s_0, s_1, \ldots, s_l\}$ be a sub-constellation of S, for some $S \in \mathcal{S}$. An element $a \in A$* realizes S' *if $tp^{\mathfrak{A}}(a,a) = s_0$, and there exists a unique sequence $b_1, \ldots, b_l \in A$ such that $tp^{\mathfrak{A}}(a, b_i) = s_i$, $0 < i \leq l$, and $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$, for each $b \in A$, $b \neq a$, $b \neq b_i$, $0 < i \leq l$. A sub-constellation S' is* realized *in $\mathfrak{A}$ if there exists $a \in A$ which realizes S'.*

Definition 5.4 *Let $\mathcal{S}'$ be a set of sub-constellations. A structure $\mathfrak{A}$ realizes $\mathcal{S}'$, if every sub-constellation $S' \in \mathcal{S}'$ is realized in $\mathfrak{A}$, and every element $a \in A$ realizes a sub-constellation of $\mathcal{S}'$.*

Definition 5.5 *Let $S \in \mathcal{S}$. An* indexed constellation S^f *is a pair $\langle S, f \rangle$, where $S \in \mathcal{S}$, and $f : S \setminus \{center(S)\} \to \mathcal{S}$ is a function such that, for every $s \in S$, S is connectable to $f(s)$ by s.*

We denote by $\mathcal{S}_{ind}$ the set of all indexed constellations of $\mathcal{S}$.

Definition 5.6 *Let $\mathfrak{A}$ be an $\mathcal{L}$-structure, and let $a \in A$ realize a constellation of $\mathcal{S}$. Assume that for every $b \in A$, $b \neq a$, if $tp^{\mathfrak{A}}(a,b) \in C_a^{\mathfrak{A}}$ then b realizes a constellation of $\mathcal{S}$.*

We denote by $ind_a^{\mathfrak{A}}$ the function $ind_a^{\mathfrak{A}} : C_a^{\mathfrak{A}} \setminus center(C_a^{\mathfrak{A}}) \to \mathcal{S}$ such that for every $b \in A$, $b \neq a$, if $tp^{\mathfrak{A}}(a,b) \in C_a^{\mathfrak{A}}$ then $ind(tp^{\mathfrak{A}}(a,b)) = C_b^{\mathfrak{A}}$.

An element a of $\mathfrak{A}$ realizes an indexed constellation S^f *if $C_a^{\mathfrak{A}} = S$, and $ind_a^{\mathfrak{A}} = f$.*

Some explanation of Definitions 5.5 and 5.6 was already given the previous section. Consider again the example of Subsection 4.5. The elements a, c and e (see Fig. 0) realize the same constellation, however a and c realize different indexed constellations, whereas a and e realize the same indexed constellation.

Definition 5.7 *Let $\mathcal{T}, \mathcal{U} \subseteq \mathcal{S}$. A set $\mathcal{X}$, $\mathcal{X} \subseteq \mathcal{S}_{ind}$, is an* indexing of $\mathcal{T}$ restricted to $\mathcal{U}$ *if for every $S \in \mathcal{T}$ there is a function f such that $S^f \in \mathcal{X}$, and for every $S^f \in \mathcal{X}$ we have $S \in \mathcal{T}$, and $f : S \setminus \{center(S)\} \to \mathcal{U}$.*

We say that a set $\mathcal{X}$, $\mathcal{X} \subseteq \mathcal{S}_{ind}$, is an indexing of $\mathcal{T}$, *if $\mathcal{X}$ is an indexing of $\mathcal{T}$ restricted to $\mathcal{S}$.*

*A pair $\langle \mathcal{X}, rnk \rangle$ is a rnk-*indexing *of $\mathcal{T}$ if $\mathcal{X}$ is an indexing of $\mathcal{T}$, and rnk is a function such that $rnk : \mathcal{X} \to \mathbb{N}^+$.*

Note that if $\langle \mathcal{X}, rnk \rangle$ is a rnk-indexing of $\mathcal{T}$, $\mathcal{U} \subseteq \mathcal{T}$, $\mathcal{X}' = \{U^f : U^f \in \mathcal{X}$ and $U \in \mathcal{U}\}$ and $rnk' = rnk \restriction \mathcal{X}'$, then $\langle \mathcal{X}', rnk' \rangle$ is a rnk'-indexing of $\mathcal{U}$.

Let $\mathcal{X} \subseteq \mathcal{S}_{ind}$, $\mathcal{U} \subseteq \mathcal{S}$ and $T^f \in \mathcal{X}$. Denote by $T^f \restriction \mathcal{U}$ the sub-constellation $= \{s \in T : f(s) \in \mathcal{U}\} \cup \{center(T)\}$ of T.

Definition 5.8 *Let $\langle \mathcal{X}, rnk \rangle$ be a rnk-indexing of $\mathcal{T}$, and let A be a finite set. A function $lab : A \xrightarrow{onto} \mathcal{X}$ is called a rnk-*labeling of A, *if for every $T^f \in \mathcal{X}$, $card(\{a \in A : lab(a) = T^f\}) = rnk(T^f)$.*

Let $\langle \mathcal{X}, rnk \rangle$ be a rnk-indexing of $\mathcal{T}$, and let A be a finite set. If lab is a rnk-labeling of A then, for every $T_i \in \mathcal{T}$, we put $A_i^{lab} = \{a \in A : lab(a) = T_i^f$, for some f such that $T_i^f \in \mathcal{X}\}$.

Definition 5.9 *Let $\mathcal{X} \subseteq \mathcal{S}_{ind}$ and let $\langle \mathcal{X}, rnk \rangle$ be a rnk-indexing of $\mathcal{T}$. An $\mathcal{L}$-structure $\mathfrak{A}$ is a $\mathcal{X}$-rnk-*model for $\mathcal{T}$ ($\mathfrak{A} \models_{\mathcal{X}}^{rnk} \mathcal{T}$) *if and only if there exists a rnk-labeling lab of A such that for every A_i^{lab}, A_j^{lab}, and every $a \in A_i^{lab}$, a realizes the sub-constellation $lab(a)\restriction\{T_j\}$ in the substructure of $\mathfrak{A}$ restricted to $\{a\} \cup A_j^{lab}$.*

The notions of an indexed constellation, and of a $\mathcal{X}$-rnk-model are fundamental in our proof of the single exponential upper bound on the complexity of SAT($\mathcal{C}_1^2$). The intuitions behind the above definitions are explained by the next proposition.

Proposition 5.10 *If $\mathcal{S}$ is a galaxy then there exist a structure $\mathfrak{A}$, a set $C \subseteq A$, subsets $\mathcal{S}_1, \mathcal{S}_2$ of $\mathcal{S}$, $\mathcal{X} \subseteq \mathcal{S}_{ind}$, and a function $rnk : \mathcal{X} \to \{1, \ldots, card(C)\}$, such that $\mathfrak{A}$ realizes $\mathcal{S}$, $card(C) \leq m(2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$, and the following conditions hold*

(1) $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$, $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, where $\mathcal{X}_1$ is an indexing of $\mathcal{S}_1$ restricted to $\mathcal{S}_1 \cup \mathcal{S}_2$ and $\mathcal{X}_2$ is an indexing of $\mathcal{S}_2$ restricted to $\mathcal{S}$, $\langle \mathcal{X}, rnk \rangle$ is an rnk-indexing of $\mathcal{S}_1 \cup \mathcal{S}_2$,

(2) for every $a \in C$, $C_a^{\mathfrak{A}} \in \mathcal{S}_1 \cup \mathcal{S}_2$,

(3) for every $a \in A$, if $C_a^{\mathfrak{A}} \in \mathcal{S}_1$ then $a \in C$ and, for every $a \in A$ and every $S \in \mathcal{S}_1$, if $C_a^{\mathfrak{A}} = S$ then $C_a^{\mathfrak{C}} = S$,

(4) $\mathfrak{C} \models_{\mathcal{X}}^{rnk} \mathcal{S}_1 \cup \mathcal{S}_2$,

(5) for every $S \in \mathcal{S} \setminus \mathcal{S}_1$, $rank_{\mathfrak{A}}(S) = \infty$.

Proof. Let $\mathcal{S}$ be a galaxy, and let $\langle \mathcal{S}_1, V, C, I, F, G \rangle$ be a finite representation of $\mathcal{S}$ which exists by Theorem 4.18. Let $\mathfrak{A}$ be a structure realizing $\mathcal{S}$ whose existence follows from Corollary 4.19. The domain of the structure $\mathfrak{A}$ is divided into two parts B and C with $B = A \setminus C$, and $V \subset C$.

Let $\mathcal{S}_1 = \{S \in \mathcal{S} : S = C_a^{\mathfrak{A}}$, for some $a \in V\}$,
$\mathcal{S}_2 = \{S \in \mathcal{S} : S = C_a^{\mathfrak{A}}$, for some $a \in C \setminus V\}$,
$\mathcal{X}_1 = \{C_a^{\mathfrak{A},f} : a \in V, f = ind_a^{\mathfrak{A}}\}$,
$\mathcal{X}_2 = \{C_a^{\mathfrak{A},f} : a \in C \setminus V, f = ind_a^{\mathfrak{A}}\}$, $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$,
and for every $S^f \in \mathcal{X}$, let $rnk(S^f) = card(\{a \in C : S = C_a^{\mathfrak{A}}$ and $f = ind_a^{\mathfrak{A}}\}$.

Assume that $\mathcal{S}_1 = \{S_1, \ldots, S_x\}$, $\mathcal{S}_2 = \{S_{x+1}, \ldots, S_y\}$, and $\mathcal{X} = \{\langle S_1, f_{11} \rangle, \ldots, \langle S_1, f_{1,v_1} \rangle, \langle S_2, f_{21} \rangle, \ldots, \langle S_2, f_{2,v_2} \rangle, \ldots, \langle S_y, f_{y1} \rangle, \ldots, \langle S_y, f_{y,v_y} \rangle\}$, where $v_i = card(\{f_{ij} : S_i^{f_{ij}} \in \mathcal{X}\})$, $1 \leq i \leq y$.

We have partitioned the set C into sets $C_1, \ldots, C_y$ in such a way that for every $a \in C$, if $a \in C_i$ then $C_a^{\mathfrak{A}} = S_i$ (see Figure 1). Furthermore, every set C_i is partitioned into classes of elements realizing the same indexed constellations $\langle S_i, f_{ij} \rangle$. Moreover, for every $a \in C_i$, if $C_i \subseteq V$ then $C_a^{\mathfrak{C}} = S_i$. This means that for every $a \in V$, for every $b \in B$, $tp^{\mathfrak{A}}(a, b) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$ ($\notin \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}$) which is denoted in Fig. 1 by the slashed arrows.

Define a rnk-labeling lab of C letting $lab(c) = S^f$, where $S = C_c^{\mathfrak{A}}$ and $f = ind_c^{\mathfrak{A}}$.

It is easy to check that conditions (1)–(5) hold. □

The main idea of the proof of Theorem 5.1 is to replace in Proposition 5.10 the condition *there exists a structure* $\mathfrak{A}$, by something easier to verify, and to substitute the implication by an equivalence. To do this we add several additional conditions, which are easily computable.

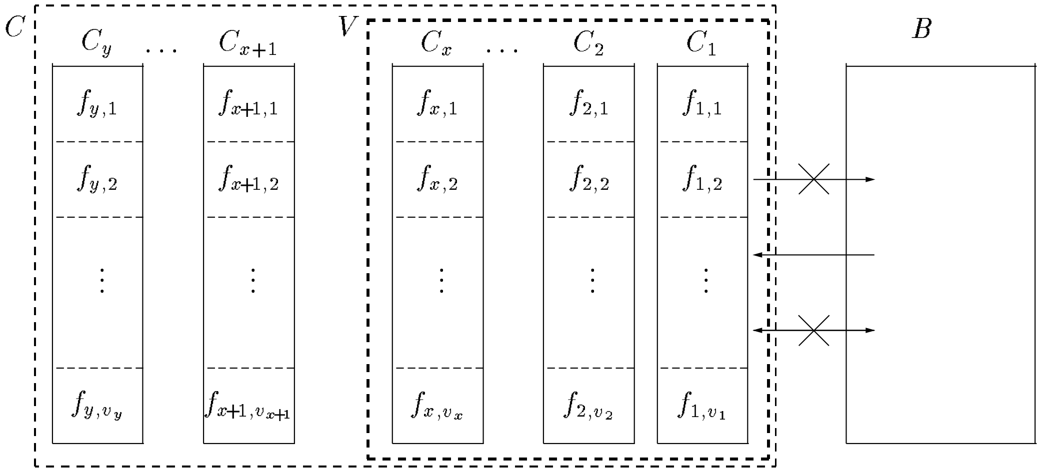

Figure 1: Partition of the universe according to the rnk-labelling

Definition 5.11 *A* concise representation of $\mathcal{S}$ *is a system*

$$\langle \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}, rnk, \mathcal{Y} \rangle,$$

where $\mathcal{S}_1, \mathcal{S}_2$ *are sets of constellations,* $\langle \mathcal{X}, rnk \rangle$ *is a* rnk*-indexing of* $\mathcal{S}_1 \cup \mathcal{S}_2$*,* $\mathcal{Y}$ *is an indexing of* $\mathcal{S} \setminus \mathcal{S}_1$*, and the following conditions hold.*

(c1) $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{S}$*,* $\mathcal{S}_1 \cap \mathcal{S}_2 = \emptyset$*,*

(c2) $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$*, where* $\mathcal{X}_1$ *is an indexing of* $\mathcal{S}_1$ *restricted to* $\mathcal{S}_1 \cup \mathcal{S}_2$ *and,* $\mathcal{X}_2$ *is an indexing of* $\mathcal{S}_2$ *restricted to* $\mathcal{S}$*,*

(c3) for every $\langle S, f_1 \rangle, \langle S, f_2 \rangle \in \mathcal{Y}$*,* $f_1 = f_2$*,*

(c4) $\sum_{S^f \in \mathcal{X}} rnk(S^f) \leq m(2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$*,*

(c5) there is a structure $\mathfrak{C}$ *such that* $\mathfrak{C} \models_{\mathcal{X}}^{rnk} \mathcal{S}_1 \cup \mathcal{S}_2$*,*

(c6) for every $S^f \in \mathcal{Y}$*, and every* $s \in S$*, if* $f(s) \in \mathcal{S}_1$ *then* $s \in \mathcal{A}^{\rightarrow}$*,*

(c7) for every $S^f \in \mathcal{Y}$ *and every* $T \in \mathcal{S}_1$*,* $card(\{s \in S : f(s) = T\}) \leq \sum_{T^f \in \mathcal{X}_1} rnk(T^f)$ *and if* $card(\{s \in S\colon f(s) = T\}) \langle \sum_{T^f \in \mathcal{X}_1} rnk(T^f)$ *then there exist* $t \in \mathcal{A}^{-}$ *such that* S *is connectable to* T *by* t*,*

(c8) for every $S, T \in \mathcal{S} \setminus \mathcal{S}_1$*,* S *is connectable to* T *by some* $t \in \mathcal{A}^{-}$*.*

Some comments are in order here. Conditions (c1)-(c8) of the above definition precisely describe the situation illustrated in Figure 1.

(c1) Three subsets of $\mathcal{S}$ are distinguished: $\mathcal{S}_1$ - constellations realized by elements of V, $\mathcal{S}_2$ - constellations realized by elements of $C \setminus V$, and $\mathcal{S} \setminus \mathcal{S}_1$ - constellations realized by elements of B.

(c2) $\mathcal{X}_1$ is an indexing of $\mathcal{S}_1$ and it defines partitions of set $C_i \subseteq V$ into appropriate classes. The indexing guarantee that the elements of V realize constellations of $\mathcal{S}_1$ in the substructure restricted to C. Similarly, $\mathcal{X}_2$ defines partitions of $C_i \subseteq C \setminus V$.

(c3) The indexing $\mathcal{Y}$ defines 2-types which are realized by pairs of elements $\langle a, b \rangle$, where $a \in B$, and $b \in V$. Note, that if B is nonempty then the constellations realized in B or in $C \setminus V$ are expected to appear infinitely many times.

(c4) The function rnk defines the cardinality of every class of C_i and so, the cardinality of V and C.

(c5) This condition takes care of definability of $\mathfrak{C}$. In particular, it specifies which elements in C_i are connected with elements in C_j by counting types, and which counting types are used to realize the connections.

(c6) An element $a \in B$ can be connected to an element $b \in V$ only by a type from $\mathcal{A}^{\rightarrow} \cup \mathcal{A}^{-}$. These types do not change the constellation realized by elements in V.

(c7) If an element $a \in B$ realizes S such that $S^f \in \mathcal{Y}$, then the number of elements in V is sufficient to realize types of S. Moreover, it is possible to define non-counting types between a and elements of V, if necessary.

(c8) Every two constellations which are realized infinitely many times are connectable by a non-counting type in $\mathcal{A}^{-}$.

Lemma 5.12 *A set of constellations $\mathcal{S}$ is a galaxy if and only if there exists a concise representation of $\mathcal{S}$.*

Proof. ($\Rightarrow$) Let $\mathcal{S}$ be a galaxy. Take a structure $\mathfrak{A}$, a set $C \subseteq A$, $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{S}$, $\mathcal{X}$, and a function rnk given by Proposition 5.10. For every constellation $S \in \mathcal{S} \setminus \mathcal{S}_1$ find an element $b \in A \setminus C$ such that b realizes S (if it exists) and add the indexed constellation realized by b to $\mathcal{Y}$. Note that if $\mathcal{S} = \mathcal{S}_1$ then $\mathcal{Y} = \emptyset$.

It is obvious that $\langle \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}, rnk, \mathcal{Y} \rangle$ satisfies conditions (c1)-(c8).

($\Leftarrow$) Let $\langle \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}, rnk, \mathcal{Y} \rangle$ be a concise representation of $\mathcal{S}$. By Theorem 4.18 it suffices to show that there exists a finite representation of $\mathcal{S}$. Let $\mathfrak{C}$ be the structure given by (c5), and let lab be the rnk-labeling of C. Let $V = \{a \in C : lab(a) \in \mathcal{S}_1\}$. We will define functions I, F, G so that the system $\langle \mathcal{S}_1, V, C, I, F, G \rangle$ is a finite representation of $\mathcal{S}$. To define I, for every $a \in C$, put $I(a) = S$, where $lab(a) = \langle S, f \rangle$. In order to define F, for every $a, b \in C$, put $F(a, b) = tp^{\mathfrak{C}}(a, b)$. Now, let $S \in (\mathcal{S} \setminus \mathcal{S}_1)$, $S = \{s_0, s_1, \ldots, s_k\}$. By (c3), there exists $\langle S, f \rangle \in \mathcal{Y}$. By condition (c8), find k distinct elements $a_1, \ldots, a_k \in V$ such that for every i, $1 \leq i \leq k$, $f(s_i) = lab(a_i)$. For every a_i, $1 \leq i \leq k$, define $G(S, a_i) = s_i$. If there is an element $b \in V$ such that $G(S, b)$ has not been defined yet, then, by (c8), find a type $s \in \mathcal{A}^{-}$ such that S is connectable to $lab(b)$ by s, and put $G(S, b) = s$. It is easy to check that conditions (f1)-(f7) of Definition 4.17 hold. □

5.3 Complexity

Proof of Theorem 5.1.

The proof proceeds in the same way as the proof of Corollary 4.20.

Let Φ be a $\mathcal{C}_1^2$-sentence of length n. By Corollary 4.8 we obtain a sentence Ψ in $\exists^{=1}$-constellation form which is satisfiable if and only if Φ is satisfiable. After defining the set $\mathcal{A}$, we guess a set $\mathcal{S}$ of $\mathcal{A}$-$\mathcal{R}$-constellations, as in Theorem 4.6.

Then, we guess sets $\mathcal{S}_1$ and $\mathcal{S}_2$ of constellations, a rnk-indexing $\langle \mathcal{X}, rnk \rangle$ of $\mathcal{S}_1 \cup \mathcal{S}_2$, and an indexing $\mathcal{Y}$ of $\mathcal{S} \setminus \mathcal{S}_1$, as in Definition 5.11.

In contrast to the proof of Corollary 4.20, this step can be performed in time $O(2^{n^3})$ since $card(\mathcal{S}_{ind}) \leq 2^{n^3}$, and the length of a maximal value of the function rnk is bounded by $\log(m(2m \cdot card(\mathcal{S}))^{card(\mathcal{S})}) = O(2^{dn^2})$, for some constant d.

Finally, we check in time $O(2^{dn^3})$ whether $\langle \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}, rnk, \mathcal{Y}\rangle$ is a concise representation of $\mathcal{S}$. □

Remark. It can be easily seen that all the conditions of Definition 5.11 except (c5) can be verified in time $O(2^{dn^3})$, for some constant d. It is less obvious that the same holds for (c5). We devote the next subsection to the problem how to verify (c5) in exponential time.

As a consequence of Theorem 5.1, by Corollary 4.9, we get the following corollary.

Corollary 5.13 SAT($\mathcal{C}^2$) $\in$ 2-NEXPTIME.

There are at least two reasons why it is difficult to improve the above result. One has been already discussed at the end of section 4.2. Another one is that it is difficult to generalize the notion of a constellation to count an arbitrary number of witnesses without increasing the number of possible constellations to double exponential. In spite of this we conjecture that the satisfiability problem for the full C^2 has only exponential complexity.

5.4 Verification of (c5)

The following definition will be used in the Decomposition Theorem (Lemma 5.15).

Definition 5.14 *Let $\mathcal{T} \subseteq \mathcal{S}$, and let $\langle \mathcal{X}, rnk\rangle$ be a rnk-indexing of $\mathcal{T}$. For $S_i, S_j \in T$ we define $\mathcal{X}_{ij} = \{S^f \in \mathcal{X} : S = S_i$ or $S = S_j\}$, and $rnk_{ij} = rnk\lceil\mathcal{X}_{ij}$.*

The following lemma gives a condition which is equivalent to condition (c5) of Definition 5.11 but is more tractable.

Lemma 5.15 (Decomposition Theorem) *Let $\mathcal{T} \subseteq \mathcal{S}$, and let $\langle \mathcal{X}, rnk\rangle$ be a rnk-indexing of $\mathcal{T}$. Then the following conditions are equivalent:*

1. *There is a structure $\mathfrak{C}$ such that $\mathfrak{C} \models^{rnk}_{\mathcal{X}} \mathcal{T}$,*
2. *For every $S_i, S_j \in \mathcal{T}$ there exists a structure $\mathfrak{C}_{ij}$ such that $\mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}$.*

Remark. Condition 1 coincides with condition (c5).
Proof. (1) ⇒ (2) is obvious.

(2) ⇒ (1). Assume that condition (2) holds. Let
$\mathcal{X} = \{\langle S_1, f_{1,1}\rangle, \ldots, \langle S_1, f_{1,v_1}\rangle, \langle S_2, f_{2,1}\rangle, \ldots, \langle S_2, f_{2,v_2}\rangle, \ldots, \langle S_y, f_{y,1}\rangle, \ldots, \langle S_y, f_{y,v_y}\rangle\}$.
For every i, j, $1 \le i \le j \le y$, let $\mathfrak{C}_{ij}$ be a structure such that $\mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}$, and let lab_{ij} be the rnk_{ij}-labeling of (the universe of) $\mathfrak{C}_{ij}$[3]. Note that

$$card(\{a \in C_{ij} : lab_{ij}(a) = S_i^f \text{ and } S_i^f \in \mathcal{X}_{ij}\}) = \sum_{S_i^f \in \mathcal{X}_{ij}} rnk_{ij}(S_i^f) = card(C_{ii}).$$

We are going to define a structure $\mathfrak{C}$. Let C, the universe of $\mathfrak{C}$, be a set such that there exists a rnk-labeling of C, and let lab be such a labeling. It is easy to notice that C could also be defined as a union of disjoint copies of C_{ii}. In fact, define $C_i = \{a \in C : lab(c) = S_i^f$, for some function $f\}$, for every i, $1 \le i \le y$. Then $C = \bigcup_{i \le y} C_i$, and $card(C_i) = card(C_{ii})$.

[3]The notation $\mathcal{X}_{ii}, C_{ii}$, and $\mathfrak{C}_{ii}$ can be misleading – the notation $\mathcal{X}_i, C_i$, and $\mathfrak{C}_i$ would be more intuitive, but we keep the less intuitive notation since it is more uniform.

Now, we shall define types realized by pairs of elements in $\mathfrak{C}$. For every i, j such that $1 \le i \le j \le y$, choose a function g_{ij} such that $g_{ij} : C_{ij} \xrightarrow[onto]{1-1} C_i \cup C_j$, and for every $a \in C_{ij}$, $lab_{ij}(a) = lab(g_{ij}(a))$. For every a, b such that $a \in C_i$, $b \in C_j$ and $i \le j$, put $tp^{\mathfrak{C}}(a,b) = tp^{\mathfrak{C}_{ij}}(g_{ij}^{-1}(a), g_{ij}^{-1}(b))$.

To show that the structure $\mathfrak{C}$ satisfies condition 1, let $S_i, S_j \in \mathcal{T}$, and $a \in C_i$ (cf. Definition 5.9). Set $B = \{tp^{\mathfrak{C}}(a,b) : b \in C_j\} \cap (\mathcal{A}^{\rightharpoonup} \cup \mathcal{A}^{\leftrightarrow})$. By construction, $B = \{tp^{\mathfrak{C}_{ij}}(g_{ij}^{-1}(a), g_{ij}^{-1}(b)) : b \in C_j\} \cap (\mathcal{A}^{\rightharpoonup} \cup \mathcal{A}^{\leftrightarrow})$ and $B \cup \{tp^{\mathfrak{C}_{ij}}(a,a)\} = lab_{ij}(g_{ij}^{-1}(a)){\restriction}\{S_j\} = lab(a){\restriction}\{S_j\}$. □

Now, we present three technical lemmas each of them showing how to check condition 2 of Lemma 5.15. Lemma 5.18, deals with the case $i = j$, Lemma 5.19 with the case when $i \neq j$ and both S_i and S_j are realized by many elements, and Lemma 5.20 with the when case $i \neq j$ but only one of S_i and S_j is realized by many elements.

We are very sorry that in spite of the suggestions of the referees, many requests of our friends and our best intentions we have not been able to make the proofs more readable.

We have tried to write a reader-friendly paper, but we have been only partially successful in this attempt. We did not find a way to avoid yet another technical definition below.

We will use the following notation.

Definition 5.16 *Assume that $\mathcal{T} \subseteq \mathcal{S}$, and $\langle \mathcal{X}, rnk\rangle$ is a rnk-indexing of $\mathcal{T}$. Let q be a positive integer. For $S_i, S_j \in \mathcal{T}$, and every $s \in S_i$ define*

$$\begin{aligned}
c_i &= \sum_{S_i^f \in \mathcal{X}} rnk(S_i^f), \\
u_{ij}(s) &= \sum_{S_i^f \in \mathcal{X}, f(s)=S_j} rnk(S_i^f), \quad \text{for } s \in S_i, \\
S_{ij}^q &= \{s \in S_i \cap \mathcal{A}^{\leftrightarrow} : u_{ij}(s) \le q\}, \\
\mathcal{X}_{ij}^q &= \{S_i^f \in \mathcal{X}_{ij} : \text{ for some } s \in S_{ij}^q, f(s) = S_j\} \cup \\
&\quad\ \{S_j^f \in \mathcal{X}_{ij} : \text{ for some } s \in S_{ij}^q, f(s^*) = S_i\}, \\
rnk_{ij}^q &= rnk_{ij}{\restriction}\mathcal{X}_{ij}^q.
\end{aligned}$$

Observe that the notions defined by Definition 5.16 have the following meaning in the context of $\mathfrak{C}_{ij}$.

c_i	is the cardinality of $\mathfrak{C}_{ii}$,
$u_{ij}(s)$	is the number of all elements a which realize $S_i^f{\restriction}\{S_j\}$, and for which there is a b, $b \neq a$, such that $\langle a, b\rangle$ realizes s, and b realizes $S_j^f{\restriction}\{S_i\}$,
S_{ij}^q	is the set of 2-types of S_i which are realized in $\mathfrak{C}_{ij}$ by at most q pairs $\langle a, b\rangle$ such that a realizes $S_i^f{\restriction}\{S_j\}$, and b realizes $S_j^f{\restriction}\{S_i\}$,
$\mathcal{X}_{ij}^q$	is the restriction of $\mathcal{X}_{ij}$ to the constellations including types of S_{ij}^q,
rnk_{ij}^q	is the restriction of rnk_{ij} to $\mathcal{X}_{ij}^q$.

Note that $u_{ij}(s)$, c_i, S_{ij}^q, $\mathcal{X}_{ij}^q$, and rnk_{ij}^q are easily computable from $\mathcal{X}$ and rnk in time $O(2^{n^3} \cdot 2^{dn^2}) = O(2^{en^3})$, for some constant e.

Definition 5.17 *Let $\mathcal{X} \subseteq \mathcal{S}_{ind}$, let $\langle \mathcal{X}, rnk\rangle$ be a rnk-indexing of $\mathcal{T}$, and let $\mathcal{B} \subseteq \mathcal{A}$. Given a $\mathcal{L}$-structure $\mathfrak{A}$ we write $\mathfrak{A} \models_{\mathcal{B},\mathcal{X}}^{rnk} \mathcal{T}$ if and only if there exists a rnk-labeling lab of the universe A of $\mathfrak{A}$ such that for every $S_i, S_j \in \mathcal{T}$, and every $a \in A_i^{lab}$,*

$$tp^{\mathfrak{A}}(a,a) = center(lab(a){\restriction}\{S_i\}),$$

$$\{tp^{\mathfrak{A}}(a,b) : b \in A_j^{lab}\} \cap (\mathcal{A}^{\rightharpoonup} \cup \mathcal{A}^{\leftrightarrow}) = lab(a){\restriction}\{S_j\} \cap \mathcal{B},$$

and for every 2-type $t \in lab(a){\restriction}\{S_j\} \cap \mathcal{B}$ there exists a unique $b \in A_j^{lab}$ such that $tp^{\mathfrak{A}}(a,b) = t(x,y)$.

The above definition says that $\mathfrak{A} \models^{rnk}_{\mathcal{B},\mathcal{X}} \mathcal{T}$ if and only if there exists a rnk-labeling lab of A such that for every A_i^{lab}, A_j^{lab}, and every $a \in A_i^{lab}$, a realizes the sub-constellation $lab(a){\restriction}\{S_j\} \cap \mathcal{B}$ in the substructure of $\mathfrak{A}$ with the universe $\{a\} \cup A_j^{lab}$. Note that in case $\mathcal{B} = \mathcal{A}$ the above definition is equivalent to Definition 5.9.

Lemma 5.18 *Let $S_i \in \mathcal{T}$, and assume that $c_i > 2^m$.*
There is a structure $\mathfrak{C}_{ii}$ such that $\mathfrak{C}_{ii} \models^{rnk_{ii}}_{\mathcal{X}_{ii}} \{S_i, S_i\}$ if and only if

- *(i) for every $s \in S_i \cap \mathcal{A}^{\leftrightarrow}$, $u_{ii}(s) = u_{ii}(s^*)$ and $u_{ii}(s)$ is even if $s = s^*$,*
- *(ii) S_i is connectable to S_i by some $t \in \mathcal{A}^-$,*
- *(iii) there exists a structure $\mathfrak{C}'$ such that $\mathfrak{C}' \models^{rnk'_{ii}}_{S^q_{ii},\mathcal{X}'_{ii}} \{S_i\}$, where $q = 14m$.*

Proof. ($\Rightarrow$) This follows directly from the definition of $u_{ii}(s)$, Lemma 4.12, and Definitions 5.9, 5.17 and 5.16.

($\Leftarrow$) Assume that (i)-(iii) hold. Assume that $\{s_1, \ldots, s_v\} = \{s \in S_i \cap \mathcal{A}^{\leftrightarrow} : u_{ii}(s) > 0\} \cup \{s \in S_i \cap \mathcal{A}^{\rightharpoonup} : u_{ii}(s) > 0\}$, where $v < card(S_i)$ and $\{s_1, \ldots, s_p\} = S_{ii}^{14m}$. Let lab' be the rnk'_{ii}-labeling of C' given by (iii) and Definition 5.17.

Let C_{ii} be a set of cardinality $\sum_{S_i^f \in \mathcal{X}_{ii}} rnk(S_i^f)$, and let lab be a rnk_{ii}-labeling of C_{ii}. We shall build a structure $\mathfrak{C}_{ii}$ with the universe C_{ii} such that, for every $a \in C_{ii}$, a realizes $lab(a){\restriction}\{S_i\}$ in C_{ii}. The structure $\mathfrak{C}_{ii}$ will be built in several steps.

First we define an embedding h of $\mathfrak{C}'$ into $\mathfrak{C}_{ii}$ as follows.

Let $h : C' \xrightarrow[into]{1-1} C_{ii}$, be such that for every $a \in C'$, $lab'(a) = lab(h(a))$. For every $a, b \in h(C')$, such that $tp^{\mathfrak{C}'}(h^{-1}(a), h^{-1}(b)) \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\rightharpoonup}$, define $tp^{\mathfrak{C}_{ii}}(a,b) = tp^{\mathfrak{C}'}(h^{-1}(a), h^{-1}(b))$.

Now, it remains to define, for each type $s_l \in \{s_{p+1}, \ldots s_v\}$, the set of pairs of elements of C_{ii} which realize s_l. To do this we shall use the graph-theoretical Lemmas 6.2 and 6.3 given in Appendix. We proceed by induction. Assume that, for some $l \geq p$, the sets of pairs satisfying types $s_1, \ldots, s_{l-1}$ have been defined. We shall now define set of pairs satisfying s_l.

Case 1. $s_l \in \mathcal{A}^{\leftrightarrow}$.
Let $X, Y \subseteq C_{ii}$ be defined as follows

$X = \{a \in C_{ii} : s_l \in lab(a){\restriction}\{S_i\}\}$,
$Y = \{a \in C_{ii} : s_l^* \in lab(a){\restriction}\{S_i\}\}$.

Observe that s_l can be realized only by pairs $\langle a, b\rangle$ such that $a \in X$, and $b \in Y$. Also, if $s_l = s_j^*$, for some $j < l$, then the type s_l has been considered. By condition (i), $card(X) = card(Y)$, and if $s_l = s_l^*$ then $card(X)$ is even. Moreover, since $card(X) = u_{ii}(s_l)$, we have $card(X) > 14m$.

Let $G^* = (X \cup Y, E^*)$, be the graph such that $E^* = \{\{a,b\} :$ either $\langle a,b\rangle$ or $\langle b,a\rangle$ realizes a type $s_j, j < l\}$. Then, $d(G^*) < l \leq m$. Let $G = (X \cup Y, E)$ be the graph complement of G^*, and let $n = card(X \cup Y)$. We have $d(G) > n - l + 1 \geq n - m$. Note that if $E(a,b)$ then the type of $\langle a, b\rangle$ has not been specified so far.

Case 1a. $s_l = s_l^*$.
By the definition of X and Y, we have $X = Y$. By Lemma 6.2, there exists a Hamiltonian cycle $\mu = [a_1, \ldots, a_n]$ in G, and by (i) n is even. For each odd j such that $1 \leq j \leq n$, put $tp^{\mathfrak{C}_{ii}}(a_j, a_{j+1}) = s_l$.

Case 1b. $s_l \in \mathcal{A}^{\leftrightarrow}$, and $s_l \neq s_l^*$.
Let $X' = X \setminus Y$, $Y' = Y \setminus X$, $Z = X \cap Y$, $n' = card(X') = card(Y')$, and $n_Z = card(Z)$. We consider 2 subcases.

Subcase 1ba. $card(Z) \leq 2m$.

Let $G_X = (Z, X', E_X)$, where $E_X = \{\{a,b\} \in E : a \in Z, b \in X'\}$. Then G_X is a bipartite graph such that for every $A \subseteq Z$, $card(\Gamma_{G_X}(A)) > n' - l + 1 > 3m > card(A)$. So, by Lemma 6.1, there is a matching E'_X of Z onto $X_Z \subset X'$. For every $a \in X_Z$, $b \in Z$ such that $\{a,b\} \in E'_X$, put $tp^{\mathfrak{C}_{ii}}(a,b) = s_l$.

Similarly, there exists a matching E'_Y from Z onto $Y_Z \subset Y'$ in the graph G_Y defined in the same way as G_X. For every $a \in Z$, $b \in Y_Z$ such that $\{a,b\} \in E'_Y$, put $tp^{\mathfrak{C}_{ii}}(a,b) = s_l$.

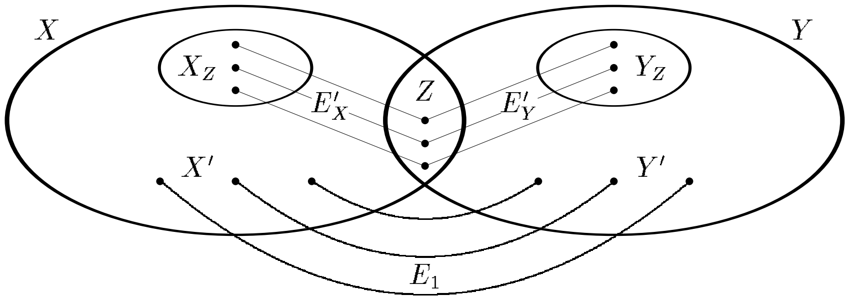

Figure 2: **Case 1b**, $card(Z) \leq 2m$.

Finally, let $G' = (X' \setminus X_Z, Y' \setminus Y_Z, E')$ be the bipartite graph such that $E' = \{\{a,b\} \in E : a \in X' \setminus X_Z, b \in Y' \setminus Y_Z\}$. Put $n'' = card(X' \setminus X_Z) = card(Y' \setminus Y_Z)$. Then, $n'' > 2m$ and $d(G') > n'' - l + 1 > n'' - m$. By Lemma 6.3, there exists a matching E_1 from $X' \setminus X_Z$ onto $Y' \setminus Y_Z$. For every $a \in X' \setminus X_Z$, $b \in Y' \setminus Y_Z$ such that $\{a,b\} \in E_1$, put $tp^{\mathfrak{C}_{ii}}(a,b) = s_l$.

Subcase 1bb. $card(X') \leq 2m$.
We have $X \cup Y = X' \dot{\cup} Z \dot{\cup} Y'$ and $d(G) \geq n - l + 1 > n - m$. By Lemma 6.4, there exists a set $Z' \subset Z$ such that X' and Y' can be matched onto Z'. Let $E_{X'}$ be the matching of X' onto Z', and let $E_{Y'}$ be the matching of Y' onto Z'.

For every $a \in X'$, $b \in Z'$ such that $\{a,b\} \in E_{X'}$, put $tp^{\mathfrak{C}_{ii}}(a,b) = s_l$. For every $b \in Z'$, $c \in Y'$ such that $\{b,c\} \in E_{Y'}$, put $tp^{\mathfrak{C}_{ii}}(b,c) = s_l$.

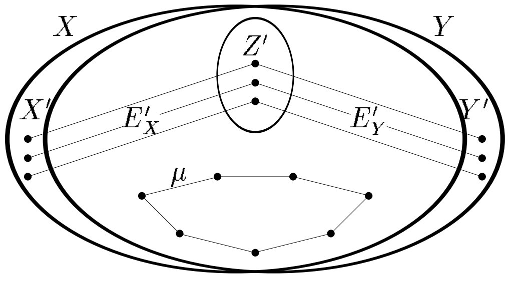

Figure 2: **Case 1b**, $card(X') \leq 2m$.

Finally, let $G' = (Z \setminus Z', E')$, where $E' = \{\{a,b\} \subset Z \setminus Z' : \{a,b\} \in E\}$. Put $n'' = card(Z \setminus Z')$. Then, $n'' > 2m$, and $d(G') \geq n'' - l + 1 > n - m$. By Lemma 6.2, there exists a Hamiltonian cycle $\mu = [a_1, \ldots, a_{n''}]$ in G'. For every j such that $1 \leq j < n''$, put $tp^{\mathfrak{C}_{ii}}(a_j, a_{j+1}) = s_l$, and put $tp^{\mathfrak{C}_{ii}}(a_{n''}, a_1) = s_l$.

Case 2. $s_l \in \mathcal{A}^{\rightarrow}$.
Let $X = \{a \in C_{ii} : s_l \in S_i^f \restriction \{S_i\}$, where f is a function such that $lab(a) = S_i^f\}$.

Let $G^* = (C_{ii}, E^*)$, where $E^* = \{\{a,b\} :$ either $\langle a,b \rangle$ or $\langle b,a \rangle$ realizes s_j, for some $j < l\}$. Then, $d(G^*) < l \leq m$. Let $G = (C_{ii}, E)$ be the graph complement of G^*, and let $n = card(C_{ii})$. We have $d(G) > n - l + 1 > n - m$, so by Lemma 6.2, there exists a Hamiltonian cycle $\mu = [a_1, \ldots, a_n]$ in G. For every j such that $1 \leq j < n$ and $a_j \in X$, put $tp^{\mathfrak{C}_{ii}}(a_j, a_{j+1}) = s_l$, and put $tp^{\mathfrak{C}_{ii}}(a_n, a_1) = s_l$.

Notice that by condition (ii), there exists a type $t \in \mathcal{A}^{-}$ such that S_i is connectable to S_i by t. So to finish the proof, it suffices to define $tp^{\mathfrak{C}_{ii}}(a,b) = t$, for any $a, b \in C_{ii}$, such that $tp^{\mathfrak{C}_{ii}}(a,b)$ has not been defined yet. □

Lemma 5.19 *Let $S_i, S_j \in \mathcal{T}$, $i \neq j$, and assume that $c_i, c_j > 3m$.*
There is a structure $\mathfrak{C}_{ij}$ such that $\mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}$ if and only if

- *(i) there are structures $\mathfrak{C}_{ii}$, $\mathfrak{C}_{jj}$ such that $\mathfrak{C}_{ii} \models^{rnk_{ii}}_{\mathcal{X}_{ii}} \{S_i\}$, and $\mathfrak{C}_{jj} \models^{rnk_{jj}}_{\mathcal{X}_{jj}} \{S_j\}$,*
- *(ii) $u_{ij}(s) = u_{ji}(s^*)$, for each $s \in S_i \cap \mathcal{A}^{\leftrightarrow}$, and $u_{ji}(s) = u_{ij}(s^*)$, for each $s \in S_j \cap \mathcal{A}^{\leftrightarrow}$,*
- *(iii) there exists a structure $\mathfrak{C}'$ such that $\mathfrak{C}' \models^{rnk^q_{ij}}_{S^q_{ij}, \mathcal{X}^q_{ij}} \{S_i, S_j\}$, where $q = 2m$,*
- *(iv) S_i is connectable to S_j by some $t \in \mathcal{A}^{-}$.*

Proof. ($\Rightarrow$) This part of the proof is obvious.

($\Leftarrow$) Assume that (i)-(iv) hold. Let $\{s_1, \ldots, s_v\} = \{s \in S_i \cap \mathcal{A}^{\leftrightarrow} : u_{ij} > 0\} \cup \{s \in (S_i \cup S_j) \cap \mathcal{A}^{\rightarrow} : u_{ij}(s) > 0\}$, where $v < card(S_i \cup S_j)$. Assume that $S_{ij}^{2m} = \{s_1, \ldots, s_p\}$, and $\{s_{r+1}, \ldots, s_v\} = \{s \in (S_i \cup S_j) \cap \mathcal{A}^{\rightarrow} : u_{ij}(s) > 2m\}$.

Let $\mathfrak{C}_{ii}$ and $\mathfrak{C}_{jj}$ be such that (i) holds, and assume that $\mathfrak{C}_{ii}$ and $\mathfrak{C}_{jj}$ are disjoint. Let $C_{ij} = C_{ii} \cup C_{jj}$. For every $a, b \in C_{ii}$, put $tp^{\mathfrak{C}_{ij}}(a,b) = tp^{\mathfrak{C}_{ii}}(a,b)$, and for every $a, b \in C_{jj}$, put $tp^{\mathfrak{C}_{ij}}(a,b) = tp^{\mathfrak{C}_{jj}}(a,b)$. Let lab_{ii} be the rnk_{ii}-labeling of C_{ii}, and lab_{jj} be the rnk_{jj}-labeling of C_{jj} as in Definition 5.9. To define the rnk_{ij}-labeling lab_{ij} of C_{ij}, we put $lab_{ij} = lab_{ii} \cup lab_{jj}$.

Now, for $a \in C_{ii}$ and $b \in C_{jj}$, we shall assign a type to $\langle a,b \rangle$, in such a way that for every $a \in C_{ii}$, a realizes in $\mathfrak{C}_{ij} \restriction C_{jj} \cup \{a\}$ the sub-constellation $lab_{ij}(a) \restriction \{S_j\}$, and for every $b \in C_{jj}$, b realizes in $\mathfrak{C}_{ij} \restriction C_{ii} \cup \{b\}$ the sub-constellation $lab(b)_{ij} \restriction \{S_i\}$.

As in the proof of Lemma 5.18, the construction proceeds in steps. First, we embed the structure $\mathfrak{C}'$ given by (iii) into $\mathfrak{C}_{ij}$, and then we consider types $s_l \in \{s_{p+1}, \ldots, s_v\}$.

Define

$X = \{a \in C_{ii} : s_l \in lab(a)\restriction\{S_j\}\}$,

$Y = \{a \in C_{jj} : s_l^* \in lab(a)\restriction\{S_i\}\}$.

Now, we deal with types in $\mathcal{A}^{\leftrightarrow}$. Let $s_l \in \mathcal{A}^{\leftrightarrow}$. By (ii) $card(X) = card(Y)$. Moreover, by the definition of u_{ij}, for every $s \in \mathcal{A}^{\leftrightarrow}$, $s \in S_i$ if and only if $s^* \in S_j$. Since $card(X) = u_{ij}(s_l) > 2m$, we can proceed as in Case 1b of the proof of Lemma 5.18 with $Z = \emptyset$.

Finally assume that we have already dealt with the types $s_1, \ldots, s_r$, and we want to realize types in $s_{r+1}, \ldots, s_v$.

Let $E = \{\{a, b\} : a \in C_{ii}, b \in C_{jj}$ and $\langle a, b\rangle$ realizes s_j, $j \leq r\}$, and $G = (C_{ii}, C_{jj}, E)$ be a bipartite graph. For every $a \in C_{ii}$, let $d'(a) = card(lab(a)\restriction\{S_j\})$.

Now, by Lemma 6.5 G can be expanded to a bipartite graph $G' = (C_{ii}, C_{jj}, E')$ such that $E \subseteq E'$,

(a) for every $a \in C_{ii}$, $d_{G'}(a) = d'(a)$ and

(b) for every $b \in C_{jj}$, $d_{G'}(b) \leq c_i - m$.

By (a), for every $a \in C_{ii}$, we can find $card(lab(a)\restriction\{S_j\} \cap \mathcal{A}^{\rightarrow})$ elements $b \in C_{jj}$ such that $\langle a, b\rangle \in E' \setminus E$, and assign types in $lab(a)\restriction\{S_j\} \cap \mathcal{A}^{\rightarrow}$ to pairs $\langle a, b\rangle$. On the other hand, by (b), for every $b \in C_{jj}$, we can find $card(lab(b)\restriction\{S_i\} \cap \mathcal{A}^{\rightarrow})$ elements $a \in C_{ii}$ such that $\langle a, b\rangle \notin E'$ to realize the types of $lab(b)\restriction\{S_i\} \cap \mathcal{A}^{\rightarrow}$. $\square$

Let

$$u = \sum_{s \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\leftarrow}} u_{ij}(s) + \sum_{s \in \mathcal{A}^{\rightarrow}} u_{ji}(s).$$

The integer u is the number of pairs of elements of $\mathfrak{C}_{ij}$ which realize counting types

Lemma 5.20 *Let $S_i, S_j \in \mathcal{T}$, $i \neq j$, and assume that $c_i > 3m$ and $c_j \leq 3m$. There is a structure $\mathfrak{C}_{ij}$ such that $\mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}$ if and only if*

(i) there are structures $\mathfrak{C}_{ii}$, $\mathfrak{C}_{jj}$ such that $\mathfrak{C}_{ii} \models^{rnk_{ii}}_{\mathcal{X}_{ii}} \{S_i\}$, and $\mathfrak{C}_{jj} \models^{rnk_{jj}}_{\mathcal{X}_{jj}} \{S_j\}$,

(ii) for every $s \in S_i \cap \mathcal{A}^{\leftrightarrow}$, $u_{ij}(s) = u_{ji}(s^*)$, and for every $s \in S_j \cap \mathcal{A}^{\leftrightarrow}$, $u_{ji}(s) = u_{ij}(s^*)$

(iii) there exists a structure $\mathfrak{D}$ with the domain $D = D_1 \dot\cup D_2$, and there exists a rnk'-indexing $\langle \mathcal{X}', rnk'\rangle$ of $\{S_i, S_j\}$ such that $card(D_1) \leq 3m^2$, $card(D_1) \leq c_i$, $card(D_2) = c_j$, $\mathcal{X}' \subseteq \mathcal{X}_{ij}$, for every $S_j^f \in \mathcal{X}_{ij}$, $S_j^f \in \mathcal{X}'$, for every $S_j^f \in \mathcal{X}'$, $rnk'(S_j^f) = rnk_{ij}(S_j^f)$, for every $S_i^f \in \mathcal{X}'$, $rnk'(S_i^f) \leq rnk_{ij}(S_i^f)$ and

$$\mathfrak{D} \models^{rnk'}_{\mathcal{X}'} \{S_i, S_j\},$$

(iv) for every $S_i^f \in \mathcal{X}_{ij}$, $card((S_i^f\restriction\{S_j\}) \setminus \{center(S_i)\}) \leq c_j$,

(v) if $u < c_i \cdot c_j$ then S_i is connectable to S_j by some $t \in \mathcal{A}^{\rightarrow}$.

Proof. ($\Rightarrow$) This direction is obvious.

($\Leftarrow$) Assume that (i)-(v) hold. Assume the structures $\mathfrak{C}_{ii}$ and $\mathfrak{C}_{jj}$ given by (i) have disjoint universes. Put $C_{ij} = C_{ii} \cup C_{jj}$, for every $a, b \in C_{ii}$, put $tp^{\mathfrak{C}_{ij}}(a, b) = tp^{\mathfrak{C}_{ii}}(a, b)$, and for every $a, b \in C_{jj}$, put $tp^{\mathfrak{C}_{ij}}(a, b) = tp^{\mathfrak{C}_{jj}}(a, b)$. Let lab_{ii} be the rnk_{ii}-labeling of C_{ii}, and lab_{jj} be the rnk_{jj}-labeling of C_{jj} as in the definition 5.9. Define the rnk_{ij}-labeling lab_{ij} of the set C_{ij} by putting $lab_{ij} = lab_{ii} \cup lab_{jj}$.

Now, by (iii), define an embedding h of $\mathfrak{D}$ into $\mathfrak{C}_{ij}$ as follows.

Let $h : D \xrightarrow[into]{1-1} C_{ij}$, be a mapping such that for every $a \in D$, $lab'(a) = lab(h(a))$. For every $a, b \in h(D)$ such that $a \in C_{ii}$ and $b \in C_{jj}$ put $tp^{\mathfrak{C}_{ij}}(a,b) = tp^{\mathfrak{D}}(h^{-1}(a), h^{-1}(b))$.

Observe that by Definition 5.17, for every $a \in C_{jj} \cup h(D_1)$, $C_a^{\mathfrak{C}_{ij}\restriction h(D)} = lab(a)\restriction\{S_i, S_j\}$. Moreover, by (ii) and (iii), for every indexed constellation $S_i^f \in \mathcal{X}_{ij}$, if there is a type $s \in S_i \cap \mathcal{A}^{\leftrightarrow}$ such that $f(s) = S_j$, then $rnk'(S_i^f) = rnk(S_i^f)$. It follows that if $a \in C_{ii} \setminus h(D)$ then $s \notin \mathcal{A}^{\leftrightarrow}$, for each $s \in lab(a)\restriction\{S_j\}$. By (iv), for every $a \in C_{ii} \setminus h(D)$, for every $s \in lab(a)\restriction\{S_j\})$, find $b \in C_{jj}$ such that $tp^{\mathfrak{C}_{ij}}(a,b)$ has not been defined, and put $tp^{\mathfrak{C}_{ij}}(a,b) = s$. To finish the proof of Lemma 5.20, for every $a \in C_{ii}$, for every $b \in C_{jj}$, if $tp^{\mathfrak{C}_{ij}}(a,b)$ has not been defined then put $tp^{\mathfrak{C}_{ij}}(a,b) = t$, where $t \in \mathcal{A}^{-}$ and S_i is connectable to S_j by t (cf. (v)). □

Corollary 5.21 *(c5) can be checked in exponential time.*

Proof. By Decomposition Theorem (Lemma 5.15), it suffices to check whether, for every $S_i, S_j \in \mathcal{S}_1 \cup \mathcal{S}_2$,

$$(*) \text{ there exists } \mathfrak{C}_{ij} \text{ such that } \mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}.$$

In the case $\boldsymbol{i = j}$, if $c_i \leq 2^m$, (*) can be checked by guessing the structure $\mathfrak{C}_{ii}$ of cardinality c_i, and then verifying if $\mathfrak{C}_{ii} \models^{rnk_{ii}}_{\mathcal{X}_{ii}} \{S_i, S_i\}$. This will take no more than $O(2^{m^2}) = O(2^{n^2})$ steps. If $card(C_{ii}) > 2^m$, then by Lemma 5.18, it suffices to verify conditions (i)-(iii). This can be done in time $O(2^{dn^3})$, for some constant d.

In the case $\boldsymbol{i \neq j}$, if $c_i, c_j \leq 3m$, it suffices to guess a structure $\mathfrak{C}_{ij}$ of cardinality $c_i + c_j$ and verify if $\mathfrak{C}_{ij} \models^{rnk_{ij}}_{\mathcal{X}_{ij}} \{S_i, S_j\}$. This can be done in time polynomial with respect to m. To check whether (*) holds for $c_i > 3m$, it suffices to verify conditions (i)-(iv) of Lemma 5.19 or conditions (i)-(v) of Lemma 5.20. This also can be done in time $O(2^{dn^3})$, for some constant d.

In each of the cases above, checking whether (*) holds can be done in time $O(2^{dn^3})$, so it takes at most $O((2^{dn^3})^2) = O(2^{cn^3})$ steps to verify that (*) holds for every i, j. This finished the proof and completes the proof of Theorem 5.1. □

6 Appendix

We assume that the reader is familiar with the basic notions of graph theory. We use standard notation of graph theory (see e.g. [4]).

In this paper a *graph* $G = (X, E)$ is a *finite* set X of nodes and a set E of edges, which are unordered pairs of nodes. For $x \in X$ we denote by $\Gamma_G(x)$ the set of neighbors of x, i.e. the set $\{y : \{x, y\} \in E\}$, and, for $A \subseteq X$, we put $\Gamma_G(A) = \bigcup_{a \in A} \Gamma_G(a)$. The degree of a node x, denoted by $d_G(x)$, is the number of neighbors of x. By $d(G)$ we denote the minimal value of $d_G(x)$. Given a graph $G = (X, E)$, a matching is defined as a set $E_0 \subseteq E$ such that, for each pair $\{u, v\}, \{u', v'\} \in E_0$ of edges, we have $\{u, v\} \cap \{u', v'\} = \emptyset$. A graph is *bipartite* if its nodes can be partitioned into two sets X_1, X_2 such that no two nodes in the same set are adjacent, such a bipartite graph is often denoted as $G = (X_1, X_2, E)$. Given a bipartite graph $G = (X, Y, E)$ and we say that X is matched into Y if there is a matching $E_0 \subseteq E$ such that for every $x \in X$ there exists $y \in Y$ such that $\{x, y\} \in E_0$.

Let m be a fixed nonnegative integer. The proof of the main result of this paper (Theorem 5.1) heavily depends on the following lemmas.

Lemma 6.1 (König-Hall Theorem [21], cf. [4], p. 134) *In a bipartite graph $G = (X, Y, E)$, X can be matched into Y if and only if $card(\Gamma_G(A)) \geq card(A)$, for every $A \subseteq X$.*

Lemma 6.2 *Let G be a graph with n nodes and with $d(G) \geq n - m$. If $n > 2m$ then G has a Hamiltonian cycle.*

Proof. This is an easy consequence of the theorem by J.A. Bondy [6] (cf. [4], p. 212) which says that *a graph G with $n \geq 3$ nodes, and with degrees $d_1 \leq, \ldots, \leq d_n$ has a Hamiltonian cycle if for every i, j such that $i \neq j$, $d_i \leq i$ and $d_j \leq j$, we have $d_i + d_j \geq n$.*

In fact, we have $d(G) \geq n - m$, so $d_i + d_j \geq n$ always holds for $n > 2m$. □

Lemma 6.3 *If $G = (X, Y, E)$ is a bipartite graph such that $card(X) = card(Y) = n$, $d(G) \geq n - m$ and $n > 2m$ then X can be matched into Y.*

Proof. We use Lemma 6.1. Towards a contradiction, assume that there exists $A \subseteq X$ such that $card(\Gamma_G(A)) < card(A)$. Then $card(\Gamma_G(A)) < n$ and, since $d(G) \geq n - m$, $card(\Gamma_G(A)) \geq n - m$ and $card(A) > n - m$. Let $y \in Y \setminus \Gamma_G(A)$. For every $x \in X$, if $x \in \Gamma_G(y)$ then $x \notin A$. Moreover, $card(\Gamma_G(y)) \geq n - m$ and so, $card(A) < m$. This gives a contradiction if $n > 2m$. □

Lemma 6.4 *Let $G = (V, E)$ be a graph with n nodes such that $d(G) \geq n - m$, and assume that $V = X'\dot\cup Z\dot\cup Y'$, where $card(X') = card(Y') \leq 2m$. If $n > 14m$ then there exists $Z' \subseteq Z$ such that both X' and Y' can be matched onto Z'.*

Proof. Let $X' = \{a_1, \ldots, a_k\}$, $Y' = \{b_1, \ldots, b_k\}$, where $k \leq 2m$. Since $d(G) \geq n - m$, we have $card(\Gamma_G(a_1)) \geq n - m$. We claim, that there is an element $c_1 \in \Gamma_G(a_1) \cap Z$ such that $c_1 \in \Gamma_G(b_1) \cap Z$. Indeed, $card(\Gamma_G(a_1) \cap Y) \geq n - m - 4m = n - 5m$, and $card(\Gamma_G(b_1) \cap Z) \geq n - 5m$. So, $\Gamma_G(a_1) \cap \Gamma_G(b_1) \cap Z \neq \emptyset$, provided $n > 10m$. Similarly, $\Gamma_G(a_i) \cap \Gamma_G(b_i) \cap (Z \setminus \{c_1, \ldots, c_{i-1}\}) \neq \emptyset$, provided $n > 10m + 2(i - 1)$. □

Lemma 6.5 *Let $G = (X, Y, E)$ be a bipartite graph such that for every $b \in Y$, $d_G(b) \leq card(X) - m$. Let $d' : X \mapsto \{0, \ldots, m\}$ and for every $a \in X$, $d_G(a) \leq d'(a)$. If $card(X), card(Y) > 3m$ then there exists a bipartite graph $G' = (X, Y, E')$ such that $E \subseteq E'$, for every $a \in X$, $d_{G'}(a) = d'(a)$, and for every $b \in Y$, $d_{G'}(b) \leq card(X) - m$.*

Proof. Let $G = (X, Y, E)$ be a bipartite graph such that for every $b \in Y$, $d_G(b) \leq card(X) - m$, and let $d' : X \mapsto \{0, \ldots, m\}$ be a function such that for every $a \in X$, $d_G(a) \leq d'(a)$.

To build the graph G' we will add new edges to the graph G repeating the following operation until we get a graph as needed.

(*) Let a be an element of X such that $d_G(a) < d'(a)$. Find an element $b \in Y$ such that $\{a, b\} \notin E$ and for every $c \in Y$ with $\{a, c\} \notin E$, $d_G(b) \leq d_G(c)$. Put $E = E \cup \{a, b\}$.

We will now show that an element b as above exists, and that the operation (*) preserves assumptions of the lemma.

Since $d_G(a) < m < card(Y)$, there exist at least $card(Y) - m$ elements c in Y such that $\{a, c\} \notin E$. We claim that among these elements there is an element b such that

$d_G(b) < card(X) - m$. In fact, towards a contradiction, assume that $d_G(b) = card(X) - m$, for each $c \in Y$ such that $\{a, c\} \notin E$. Then,

$$\sum_{c \in Y} d_G(c) = \sum_{c \in Y \setminus \Gamma_G(a)} d_G(c) + \sum_{c \in \Gamma_G(a)} d_G(c) \geq (card(Y) - m)(card(X) - m).$$

On the other hand, $d_G \leq m$, for every $e \in X$, which gives

$$\sum_{c \in Y} d_G(c) = \sum_{e \in X} d_G(e) < m \cdot card(X).$$

By the above inequalities,

$$m \cdot card(X) > (card(Y) - m)(card(X) - m)$$

and hence,

$$card(X)card(Y) - m(card(X) + card(Y)) - m(card(X) - m) < 0. \tag{1}$$

Assume $card(X) \geq card(Y)$. Then,

$$\begin{gathered} card(X)card(Y) - m(card(X) + card(Y)) - m(card(X) - m) \geq \\ card(X)card(Y) - 3m \cdot card(X) + m^2 > \\ card(X)(card(Y) - 3m) > 0, \text{ provided } card(Y) > 3m. \end{gathered}$$

The last inequality contradicts (1). □

References

[1] W. Ackermann. Über die erfüllbarkeit gewisser zählausdrücke. *Mathematische Annalen*, 100:638–649, 1928.

[2] W. Ackermann. Beiträge zum entscheidungsproblem der mathematischen logik. *Mathematische Annalen*, 112:419–432, 1936.

[3] W. Ackermann. *Solvable Cases of the Decision Problem.* North-Holland, Amsterdam, 1954.

[4] C. Berge. *Graphs and Hypergraphs.* North Holland, 1971.

[5] P. Bernays and M. Schönfinkel. Zum entscheidungsproblem der mathematischen logik. *Mathematische Annalen*, 99:342–372, 1928.

[6] J. A. Bondy. Properties of graphs with constraints and on degrees. *Studia Sc. Math. Hung.*, 4:473–475, 1969.

[7] E. Börger, E. Grädel, and Y. Gurevich. *The classical decission problem.* Perspectives in Mathematical Logic. Springer-Verlag, 1997.

[8] A. Borgida. On the relative expressive power of description logics and predicate calculus. *Artificial Intelligence*, 82:353–367, 1996.

[9] B. Dreben and W. Goldfarb. *The Decision Problem: Solvable Classes of Quantificational formulas,.* Addison-Wesley, Reading, 1979.

[10] A. Ehrenfeucht. An application of games to the completeness problem for formalised theories. *Fund. Math.*, 49:129–141, 1961.

[11] K. Gödel. Ein spezialfall des entscheidungsproblem des theoretischen logik. *Ergebnisse eines mathematischen Kolloquiums*, 2:27–28, 1932.

[12] K. Gödel. Zum entscheidungsproblem des logischen funktionenkalküls. *Monatshefte für Mathematik und Physik*, 40:433–443, 1933.

[13] W. Goldfarb. *On Decision Problems for Quantification Theory.* PhD thesis, Harvard University, 1974. abstract in Notices Amer. Math. Soc. 21 (4), p.280.

[14] W. Goldfarb. The unsolvability of the Gödel class with identity,. *Journal of Symbolic Logic*, 49:1237–1252, 1984.

[15] E. Grädel, P. Kolaitis, and M. Vardi. On the decision problem for two-variable first-order logic. *Bull. of Symb. Logic*, 3(1):53–69, 1997.

[16] E. Grädel, M. Otto, and E. Rosen. Two-variable logic with counting is decidable. In *Twelth Annual IEEE Symposium on Logic in Computer Science*, pages 306–317, 1997.

[17] E. Grädel, M. Otto, and E. Rosen. Undecidability results on two-variables logics. In *Proc. of 14th Annual Symposium on Theoretical Aspects of Computer Science*, volume 1200, pages 249–260. Springer-Verlag Lecture Notes in Computer Science, 1997.

[18] Y. Gurevich. The decision problem for standard classes. *Journal of Symbolic Logic*, 41:460–464, 1976.

[19] Y. Gurevich. On the classical decision problem. In G. Rosenberd and A. Salomaa, editors, *Current Trends in Theoretical Computer Science*, pages 254–265. World Scientific, 1993.

[20] Y. Gurevich and S. Shelah. Random models and the gödel case of the decision problem. *Journal of Symbolic Logic*, 48:1120–1124, 1983.

[21] P. Hall. On representations of subsets. *J. London Math. Soc.*, 10:26–30, 1934.

[22] W. Van Der. Hoek and M. De Rijke. Counting objects. *Journal of Logic and Computation*, 5(3):325–345, 1995.

[23] N. D. Jones and A. L. Selman. Turing machines and the spectra of first-order formulas. *J. Symb. Logic*, 39:139–150, 1974.

[24] L. Kalmár. Über die erfüllbarkeit derjenigen zählausdrücke, welche in der normalform zwei benachbarte allzeichen enthalten. *Mathematische Annalen*, 108:466–484, 1933.

[25] H. Lewis. *Unsolvable Classes of Quantificational Formulas.* Addison-Wesley, Reading, 1979.

[26] H. Lewis and W. Goldfarb. The decision problem for formulas with a small number of atomic subformulas. *Journal of Symbolic Logic*, 38:471–480, 1973.

[27] H. R. Lewis. Complexity results for classes of quantificational formulas. *J. Comp. and System Sci.*, 21:317–353, 1980.

[28] M. Mortimer. On languages with two variables. *Zeitschr. f. Logik und Grundlagen d. Math.*, 21:135–140, 1975.

[29] L. Pacholski, W. Szwast, and L. Tendera. Complexity of two-variable logic with counting. In *Twelth Annual IEEE Symposium on Logic in Computer Science*, pages 318–327, 1997.

[30] M. Rabin. Decidability of second-order theories and automata on infinite trees. *Trans. Amer. Math. Soc.*, 141:1–35, 1969.

[31] D. Scott. A decision method for validity of sentences in two variables. *J. Symb. Logic*, 27:477, 1962.

[32] S. Shelah. Decidability of a portion of the predicate calculus. *Israel Journal of Mathematics*, 28:32–44, 1977.

[33] T. Skolem. Untersuchungen über die axiome des klassenkalküls und über produktations- und summationsprobleme, welche gewisse klassen von aussagen betreffen. *Skrifter utgit au Vidensk. i Kristiania I, Math.-nat.Klasse*, 3:37, 1919.

[34] T. Skolem. Logisch-kombinatorische untersuchungen über die erfüllbarkeit oder beweisbarkeit mathematischer sätze nebst einem theorem über dichte mengen. *Norsk Vid-Akad. Oslo Mat.-Natur Kl. Skr.*, 4, 1920.

[35] T. Skolem. Über die mathematische logik. *Norsk MAt. Tidsskrift*, 106:125–142, 1928.

[36] W. Szwast and L. Tendera. First-order two-variable logic is in NEXPTIME. unpublished manuscript.

[37] H. Wang. Dominoes and the $\forall\exists\forall$-case of the decision problem. In *Preceedings Symposium on Mathematical Theory of Automata*, pages 23–55, New York, 1962. Brooklyn Polytechnic Institute.