Complexity of Two-Variable Logic with Counting*

Leszek Pacholski
Institute of Computer Science
University of Wrocław
Przesmyckiego 20
51-151 Wrocław, Poland
pacholsk@tcs.uni.wroc.pl

Wiesław Szwast Lidia Tendera
Institute of Mathematics
University of Opole
Oleska 48
45-052 Opole, Poland
[szwast,tendera]@math.uni.opole.pl

Abstract

Let C_k^2 denote the class of first order sentences with two variables and with additional quantifiers "there exists exactly (at most, at least) m", for $m \leq k$, and let C^2 be the union of C_k^2 taken over all integers k. We prove that the problem of satisfiability of sentences of C_1^2 is NEXPTIME-complete. This strengthens a recent result of E. Grädel, Ph. Kolaitis and M. Vardi [4] who proved that the satisfiability problem for the first order two-variable logic L^2 is NEXPTIME-complete and a very recent result by E. Grädel, M. Otto and E. Rosen [5] 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.

1. Introduction

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

The problem of satisfiability of restricted classes of first order sentences was studied in the thirties by various logicians including K. Gödel, Th. Skolem, M. Schönfinkel, P. Bernays, W. Ackermann. In 1962, in a short note, D. Scott [11] proved that the problem of satisfiability 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 [10] gave another proof of decidability by proving that L^2 has a finite model property. When in 1982 G.D. Goldfarb [3] 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 proved that the satisfiability problem for L^2 was NEXPTIME-hard. The complexity of an algorithm which could be extracted from the Mortimer's proof was doubly exponential. In the first half of 1996 E. Grädel, Ph. Kolaitis and M. Vardi [4] proved that the satisfiability problem for L^2 was in NEXPTIME. Later we found another proof [12] of the same result. Our proof was less elegant than the one in [4], but we hoped it could be extended to get the complexity bounds for C^2.

In spring 1996 E. Grädel, M. Otto and E. Rosen [5] proved that the satisfiability problem for C^2 was decidable. They proved that the set of sentences which have infinite models is 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_1^2 is NEXPTIME-complete. By the reduction of C^2 to C_1^2 given in [5] this implies that C^2 is in 2-NEXPTIME. We have a slightly more subtle reduction, which can probably give a better estimates of the complexity. We hope we shall be able to close the gap for C^2 in the final paper.

Our approach is in a very remote way based on the ideas of Mortimer. As the first step we gave [12] another proof of the result of Grädel, Kolaitis and Vardi [4]. 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 *constellation*.

*This research was supported by the Polish State Committee for Scientific Research under the project 2 P301 046 07

1043-6871/97 $10.00 © 1997 IEEE

We have also used a stronger notion of a normal form - going further than Grädel, Otto and Rosen in [5]. This was used to provide in [12] a "syntactic" proof of the result of [4]. The "syntactic" structure was in this case almost equivalent to a description of a model, but turned out to be quite useful when we moved to C^2.

In contrast to [5] our notions were almost entirely syntactic. We liked the feudal terminology of [5], and we have similar notions, however *kings* in our sense are more that just entities which are rare (appear finitely often), but have "syntactic" characteristics. In fact it is easy to give examples of models whose sets of kings (in the sense of [5]) have arbitrary large cardinality (for a language of bounded size). This implies that the method of [5] could not give complexity bounds and could hardly be adapted to the finite models case (in a finite model everyone is a *king*).

To get our result we analyze the structure of the feudal court. We have less kings and kings are characterized by the fact, that they are connected between themselves only using *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 [5]) and provides enough information to reconstruct the model and thus gives rise a 2-NEXPTIME algorithm for C_1^2 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 2) of C_1^2 of size n whose unique model coincides with V and has cardinality $O(2^{2^n})$.

To push the complexity down we had to give a finer analysis. We noticed that the number of vassals in V_i that have different relations between themselves and between elements of lower classes is small (exponential). They may differ only by their relations to their sovereigns (they are connected to their sovereigns by different relations). Moreover, the types of relations between elements of V_i and elements of V_{i+1} do not depend on i. Thus we are given a tree-like structure of an exponential depth, where elements of each level are indiscernible. Therefore a model can be described by the depth of this tree-like structure and by the relations of a sovereign to its immediate vassals. These gives rise to two sets of informations both of exponential size. Moreover, the consistency of these two sets can be checked in exponential time (with respect to n - the size of a formula).

In more technical terms a potential model is described by a set of indexed constellations. Roughly speaking, an indexed constellation in addition to an information on two-types realized by an element carries for some two-types *requests* for partner constellations - constellations that should realize, together with the host constellation, these two-types.

It is worth to notice, that by a recent result of E. Grädel, M. Otto and E. Rosen [6], extensions of two-variables logic L^2 by a weak access to cardinalities trough 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. [7]) 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. [2]).

2. Preliminaries

We assume that the reader is familiar with the standard notions of logic and automata theory.

Let $\mathcal{C}_p^2$ be the fragment of $\mathcal{C}^2$ consisting of sentences Φ such that the counting quantifiers appearing in Φ are of the form $\exists^{=i}$, $\exists^{\leq i}$ or $\exists^{\geq i}$, for some $i \leq p$. Let $\mathcal{C}_{p,=}^2$ be the fragment of $\mathcal{C}_p^2$ in which the form of the counting quantifiers is restricted to $\exists^{=i}$, for some $i \leq p$.

Let $\mathcal{L}$ be a relational vocabulary including only unary and binary predicate letters. Let $\mathcal{R} \subseteq \mathcal{L}$, $\mathcal{R} = \{R_1, \ldots, R_m\}$.

Definition 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 and i, m_i, m are positive integers. Φ is in $\exists^{=1}$-*constellation form* if $m_i = 1$ for each $i \leq m$.

This definition may seem too strong. The second part of the formula seem to say that all elements are similar from the point of view of $\mathcal{R}$. Note however, that we do not require $x \neq y$ after the counting quantifier, therefore, at least in the case of $m_i = 1$, the fact that $R_i(x,x)$ can be used to code those elements x, and those relations R_i for which counting quantifier of the second part of Φ does not apply.

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, including the formula $x \neq y$. A type t is often considered as a 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 $t(x,y)$.

Let $\mathcal{A}$ be a set of 2-types.

Definition 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 $\neg R_i(y,x) \in t\}$.

The intuition behind the definition above is, that $\mathcal{A}^{\leftrightarrow}$, $\mathcal{A}^{\leftarrow}$ and $\mathcal{A}^{\rightarrow}$ represent *counting types*. For us $R_i(x,y) \in t$ means that whenever (a,b) and (a,b') realize t in any of the models we shall construct, then $b = b'$.

Definition 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 $s_1, \ldots, s_k \in \mathcal{A}$. Define

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

$P_0 = \{R_j \in \mathcal{R} : R_j(x,x) \in center(S)\}$,

$P_i = \{R_j \in \mathcal{R} : R_j(x,y) \in s_i\}$, for $1 \leq i \leq k$.

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

1) $center(S)$ is consistent,

2) for every $1 \leq i \leq k$ there is j, $1 \leq j \leq m$, such that $R_j(x,y) \in s_i$,

3) for every $0 \leq i,j \leq k$, if $P_i \cap P_j \neq \emptyset$ then $i = j$,

4) $\bigcup_{i=0}^{k} P_i = \mathcal{R}$.

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.

Definition 3 states that a set S of types is an $\mathcal{A}$-$\mathcal{R}$-constellation if every R_i positively appears in some type of S, every type in S contains a positive occurrence of R_i, and, for each $i \leq m$, at most one type of S contains a positive occurrence of $R_i(x,y)$. Note that $(S \setminus center(S)) \subseteq \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\rightarrow}$.

Definition 3 does not mean that each constelation contains a counting type. There may be constelations such that $\mathcal{R} = P_0$. In fact P_0 codes relations in $\mathcal{R}$ which are not important in S.

Let $\mathfrak{A}$ be an $\mathcal{L}$-structure and A be the universe of $\mathfrak{A}$. Let $a,b \in A$. Denote by $tp^{\mathfrak{A}}(a,b)$ the unique type $t(x,y)$ realized by $< a,b >$.

Definition 4 Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. An element $a \in A$ *realizes* an $\mathcal{A}$-$\mathcal{R}$-constellation S if there exists a unique sequence of elements $b_0 (= a), b_1, \ldots, b_k \in A$ such that $tp^{\mathfrak{A}}(a,b_i) = s_i$ and for every $b \in A$, $b \neq b_i$, $0 \leq i \leq k$, $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$. An $\mathcal{A}$-$\mathcal{R}$-constellation S is *realized* in $\mathfrak{A}$ if there exists $a \in A$ such that a realizes S.

If S is an $\mathcal{A}$-$\mathcal{R}$-constellation realized by an element $a \in A$ then we write $X_a^{\mathfrak{A}} = S$.

Definition 5 Let $\mathcal{S}$ be a set of $\mathcal{A},\mathcal{R}$-constellations. A structure $\mathfrak{A}$ is a *model for* $\mathcal{S}$, $\mathfrak{A} \models \mathcal{S}$, if

for every $S \in \mathcal{S}$, S is realized in $\mathfrak{A}$, and

for every $a \in A$ there is $S \in \mathcal{S}$ such that a realizes S.

The set $\mathcal{S}$ is a *galaxy* if there is a structure $\mathfrak{A}$ such that $\mathfrak{A} \models \mathcal{S}$.

3. Satisfiability of Constellation Sentences

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

Theorem 1 *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 $\mathcal{A} = \{t(x,y)$: $t(x,y)$ is a 2-type over $\mathcal{L}$ and $t(x,y) \rightarrow \phi\}$.

Then there is an $\mathcal{L}$-structure $\mathfrak{A}$ such that $\mathfrak{A} \models \Phi$ if and only if there exists a set $\mathcal{S}$ of $\mathcal{A}$-$\mathcal{R}$-constellations which is a galaxy.

Proof. ($\Rightarrow$) Let $\mathfrak{A} \models \Phi$.

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. Let $\mathcal{S} = \{S$: S is an $\mathcal{A}$-$\mathcal{R}$- constellation and S is realized in $\mathfrak{A}\}$. By Definition 4, $\mathfrak{A} \models \mathcal{S}$ and hence $\mathcal{S}$ is a galaxy.

($\Leftarrow$) Let $\mathcal{S}$ be a galaxy and assume $\mathfrak{A} \models \mathcal{S}$. Let $a \in A$. By Definition 5, a realizes an $\mathcal{A}$-$\mathcal{R}$-constellation $S \in \mathcal{S}$, $S = \{s_0, \ldots, s_k\}$. This implies the existence of a sequence $b_0, b_1, \ldots, b_k$ of distinct elements of A such that $b_i \neq a$, for $i > 0$, and

1. $tp^{\mathfrak{A}}(a,b_i) = s_i$, for $i = 0, \ldots, k$,

2. $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{-} \subset \mathcal{A}$, for $b \in \mathcal{A}, b \neq b_i$.

So, by Definition 3, the elements $b_0, b_1, \ldots, b_k$ witness for a that the part $\bigwedge_{1 \leq i \leq m} \exists^{=1} y R_i(a,y)$ of Φ holds. Moreover for every $b \in A, b \neq a$, $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}$, and then $\mathfrak{A} \models \phi(a,b)$. Hence, $\mathfrak{A} \models \Phi$.

4. The Reduction

For an C^2-sentence Φ we denote by $|\Phi|$ the *length* of Φ, that is the number of all symbols occurring in Φ. For the sake of simplicity we assume that predicates are represented as one letter symbols.

Theorem 2 *Let Φ be an C^2_p-sentence over $\mathcal{L}$. There exists a $C^2_{p,=}$-sentence Ψ in constellation form in language $\mathcal{L}'$ such that Φ is satisfiable if and only if Ψ is satisfiable. Moreover, $|\Psi| = c\,|\Phi|$, for some constant c.*

Our reduction resembles the one used by E. Grädel, M. Otto and E. Rosen in [5] but it transforms a $\mathcal{C}^2_p$ -sentence into a $\mathcal{C}^2_{p,=}$-sentence and it is done with some care to guarantee a linear increase of the length of the original sentence. The proof is omitted here.

Corollary 1 *There exists a polynomial-time algorithm constructing a sentence Ψ for a given sentence Φ, satisfying conditions of Theorem 2.*

5. The Galaxy Theorem

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

If t is a type, we denote by t^* a symmetrical type to t, that is a type obtained from t by replacing each occurrence of the variable x by y and y by x.

Definition 6 Let S, T be constellations and $s(x,y) \in \mathcal{A}$. *S is connectable to T with $s(x,y)$* if $center(S) \subseteq s(x,y)$, $center^*(T) \subseteq s(x,y)$ and, if $s \in \mathcal{A}^{\leftrightarrow}$, then $s \in S$ and $s^* \in T$, if $s \in \mathcal{A}^{\rightarrow}$, then $s \in S$, and if $s \in \mathcal{A}^{\leftarrow}$, then $s^* \in T$.

Let $\mathcal{S}$ be a galaxy, $\mathfrak{A} \models \mathcal{S}$. Denote by $rank_{\mathfrak{A}}$ a function such that $rank_{\mathfrak{A}} : \mathcal{S} \mapsto N \cup \{\infty\}$, $rank_{\mathfrak{A}}(S) = card(\{a \in A : X^{\mathfrak{A}}_a = S\})$.

Definition 7 $rank(\mathcal{S}) = \infty$ if there is a structure $\mathfrak{B}$ such that $\mathfrak{B} \models \mathcal{S}$ and $min_{S \in \mathcal{S}}(rank_{\mathfrak{B}}(S)) > 2m + 1$.

Lemma 1 *Let $\mathfrak{A} \models \mathcal{S}$, $S, T \in \mathcal{S}$. If $rank_{\mathfrak{A}}(S) > 2m + 1$ and $rank_{\mathfrak{A}}(T) > 2m + 1$, then there exist $a, b \in A$ such that $X^{\mathfrak{A}}_a = S$, $X^{\mathfrak{A}}_b = T$ and $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^{\leftarrow}$.*

Proof. Assume $X = \{x_i \in \mathfrak{A} : x_i \text{ realizes } S\}$, $card(X) > 2m + 1$, and $Y = \{y_i \in \mathfrak{A} : y_i \text{ realizes } T\}$, $card(Y) > 2m + 1$. Let $S = \{s_0, \ldots, s_k\}$ and $T = \{t_0, \ldots, t_l\}, k, l \leq m$. By definition 4, for every $x_i \in B$ there is at most k distinct elements $y_{i_1}, \ldots, y_{i_k}$ such that $tp^{\mathfrak{A}}(x_i, y_{i_j}) \in S$. So, there are at most $k(2m+2)$ pairs $< x_i, y_j >$ such that $tp^{\mathfrak{A}}(x_i, y_j) \in S$ and there are at most $l(2m+2)$ pairs $< y_i, x_j >$ such that $tp^{\mathfrak{A}}(y_i, x_j) \in T$. Now, since $(k+l)(2m+2) < (2m+2)^2$ there exists $x \in X$ and $y \in Y$ such that $tp^{\mathfrak{A}}(x,y) \notin S$ and $tp^{\mathfrak{A}}(y,x) \notin T$. So, $tp^{\mathfrak{A}}(x,y) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$ and $tp^{\mathfrak{A}}(y,x) \in \mathcal{A}^{\leftarrow} \cup \mathcal{A}^{-}$. By definition 2, $tp^{\mathfrak{A}}(x,y) \in \mathcal{A}^{-}$.

Corollary 2 *Let $\mathfrak{A} \models \mathcal{S}$ and $rank(\mathcal{S}) = \infty$. Then, there is a structure $\mathfrak{B}$, such that $\mathfrak{B} \models \mathcal{S}$ and for every $S \in \mathcal{S}$ $rank_{\mathfrak{B}}(S) = \infty$.*

Proof. Let $\mathfrak{A} \models \mathcal{S}$ and $rank_{\mathfrak{A}}(S) = n$. We show that there is a structure $\mathfrak{B}$, $\mathfrak{B}$ is an expansion of $\mathfrak{A}$, such that $\mathfrak{B} \models S$ and $rank_{\mathfrak{B}}(S) > n$. By Lemma 1, for every constellations $S, T \in \mathcal{S}$ there exists a type $t(x,y) \in \mathcal{A}^{-}$ such that S is connectable to T with $t(x,y)$. Let $\mathfrak{A}'$ be a structure isomorphic to $\mathfrak{A}$ such that $A \cap A' = \emptyset$. Define $B = A \cup A'$ and let $\mathfrak{B} \restriction A = \mathfrak{A}$, $\mathfrak{B} \restriction A' = \mathfrak{A}'$ and for every $a \in A$, for every $a' \in A'$ find $t(x,y) \in \mathcal{A}^{-}$ such that $X^{\mathfrak{A}}_a$ is connectable to $X^{\mathfrak{A}'}_{a'}$ with $t(x,y)$ and put $tp^{\mathfrak{B}}(a,a') = t(x,y)$.

Proposition 1 *The following conditions are equivalent:*

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

Proof. (1) $\Rightarrow$ (2). Condition (a) follows from Lemma 1 and definition of a galaxy.

(2) $\Leftarrow$ (1). We give an algorithm that constructs a structure $\mathfrak{A}$ such that $\mathfrak{A} \models \mathcal{S}$. During our infinite construction new elements will be added to the universe, some elements of the universe will be cancelled (when the constellation that is to be realized by the element cancelled has been built) and some unordered pairs of elements will be reserved (when the type realized by the pair has been defined). Additionally, a function I will be defined, $I : A \mapsto \mathcal{S}$, in such a way that for every $a \in A$, $I(a) = X^{\mathfrak{A}}_a$. In every step of the construction the universe of the partially defined model $\mathfrak{A}$ is finite. It is also assumed that there is a fixed linear ordering on the universe, and a new element added to the universe is greater then the old elements.

1. Let $A = \{a_1, \ldots, a_k\}$. Put $I(a_i) = S_i$.

2. Let $a \in A$ be the first not cancelled element.

3. For every $s_i \in I(a)$, if there is no element $b \in A$ such that $\{a,b\}$ is reserved and $tp^{\mathfrak{A}}(a,b) = s_i$, then add a new element b_i at the end of A; put $tp^{\mathfrak{A}}(a,b_i) = s_i$; find a constellation $T \in \mathcal{S}$ such that S is connectable to T with s_i; put $I(b_i) = T$ and reserve $\{a,b\}$.

4. For every $c < a$ put $tp^{\mathfrak{A}}(a,c) = t \in \mathcal{A}^-$ such that $I(a)$ is connectable to $I(c)$ with t.

5. Cancel a.

6. Go to 2.

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

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

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

An iterative application of the following algorithm applied to every $S \in \mathcal{S}'$ yields a structure $\mathfrak{B}$ such that for every $S \in \mathcal{S}'$ $rank_{\mathfrak{B}}(S) = \infty$ and for every $S \in \mathcal{S} \setminus \mathcal{S}'$ $rank_{\mathfrak{B}}(S) = rank_{\mathfrak{A}}(S)$ (cancelling, reserving elements and a function I have the same role as in the construction in proof of Proposition 1). At the beginning, put $\mathfrak{A}'$=$\mathfrak{A}$.

1. Let $A'' = A' \cup \{x\}$.

2. For every $a \in A'$ put $I(a) = X_a^{\mathfrak{A}'}$ and cancel a.

3. Put $I(x) = S$.

4. Let x be the first not cancelled element of A''.

5. Find $a \in A \setminus V$ such that $X_a^{\mathfrak{A}} = I(x)$ and for every $b \in V$ $tp^{\mathfrak{A}}(a,b) \in \mathcal{A}^- \cup \mathcal{A}^{\rightarrow}$
(such an element a exists, since there at most $m \cdot card(V)$ elements that are connected with an element from V with a type $t \in \mathcal{A}^{\leftrightarrow} \cup \mathcal{A}^{\leftarrow}$).

6. For every $s_i \in S$

   (a) if there is $b \in V$ such that $tp^{\mathfrak{A}}(a,b) = s_i$ then put $tp^{\mathfrak{A}}(x,b) = s_i$
   else

   (b) if there is no element $d \in A''$ such that $\{x,d\}$ is reserved and $tp^{\mathfrak{A}''}(x,d) = s_i$, then add a new element b_i to A'', put $tp^{\mathfrak{A}}(x,b_i) = s_i$, reserve $\{x,b_i\}$, find $a_i \in A \setminus V$ such that $tp^{\mathfrak{A}}(a,a_i) = s_i$ and put $I(b_i) = I(a_i)$.
   (a_i can be found since $X_a^{\mathfrak{A}} = S$ and so, there is an element $b_i \in A$ such that $t^{\mathfrak{A}}(a,b_i) = s_i$. Since $b_i \in A$ there is a constellation $T \in \mathcal{S}, T = I(b_i)$, that is realized by b_i in $\mathfrak{A}$.)

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 $\mathfrak{A}$ with t and reserve $< x,c >$.
(By Lemma 1, for every $S,T \in \mathcal{S}'$ S is connectable to T in $\mathfrak{A}$ with some $t \in \mathcal{A}^-$.)

8. Cancel 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 $rank_{A''}(S) > rank_{\mathfrak{A}'}(S)$.

In step 6, when the types $tp^{\mathfrak{A}''}(x,b)$, where $b \in V$, are put 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 because only types in $\mathcal{A}^-$ are put.

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

Lemma 3 *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 $\mathfrak{B}$ such that $\mathfrak{B} \models \mathcal{S}$ and for every $S \in \mathcal{S}$ $rank_{\mathfrak{B}}(S) < r$ or $rank_{\mathfrak{B}}(S) = \infty$.*

Proof. Let $\mathfrak{A} \models \mathcal{S}$. It suffices to define $V \subseteq A$ of appropriate cardinality such that V satisfies the conditions of Lemma 2.

The set V will be constructed in stages.

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

Stage i. $(i > 1)$

1. If for every $a \in A \setminus V_{i-1}$ $rank_{\mathfrak{A}}(X_a^{\mathfrak{A}}) > card(V_{i-1}) \cdot m$,
then let $V_i = V_{i-1}$ and **stop**.
2. Let $V_i = V_{i-1} \cup \{a \in A \setminus V_{i-1} : rank_{\mathfrak{A}}(X_a^{\mathfrak{A}}) \leq card(V_{i-1} \cdot m\}$.
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 $X_a^{\mathfrak{A}} = S\}$. 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 $card(K) \leq 3q^p$. Moreover, for every $a \in V$, $rank_{\mathfrak{A}}(X_a^{\mathfrak{A}}) \leq card(V)$, and for every $a \in A \setminus V$, $rank_{\mathfrak{A}}(X_a^{\mathfrak{A}}) > card(V) \cdot m$. Put $r = 3 \cdot (1 + m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$. So, by Lemma 2, the thesis is proved.

Denote by n the set $\{0, 1, \ldots, n-1\}$, for a nonnegative integer n.

Definition 8 Let $\mathcal{S}$ be a set of constellations.
A system $< \mathcal{S}_1, \mathcal{S}_2, V, C, I, F, G >$ is a *finite representation of* $\mathcal{S}$ if and only if the following conditions hold for every $i, j, k \in C$, $i \neq j$, and for every $S \in \mathcal{S}_2$

(1) $\mathcal{S} = \mathcal{S}_1 \dot{\cup} \mathcal{S}_2$, $V \leq C$ are nonnegative integers such that, $C \leq 4m \cdot (m \cdot card(\mathcal{S}))^{card(\mathcal{S})}$,

(2) I, F, G are functions such that $I : C \mapsto \mathcal{S}$, $F : C \times C \mapsto \mathcal{A}$, $F(i,i) = F(i,j) \restriction \{x\}$, $G : \mathcal{S}_2 \times V \mapsto \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{-}$,

(3) if $i \in V$ then $I(i) \in \mathcal{S}_1$, if $j \in C \setminus V$ then $I(j) \in \mathcal{S}_2$, if $T \in \mathcal{S}_1$ then there is $l \in V$ such that $I(j) = T$

(4) $F(i,j) = F(j,i)^*$ and $F(i,k) \restriction \{x\} = F(i,j) \restriction \{x\}$,

(5) if $D(j)$ is defined as the set $D(j) = \{F(j,k) : k \in C, k \neq j, F(j,k) \in \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}\}$ then

  (a) for every $s \in D(j)$ there is exactly one $l \in C, l \neq j$, such that $F(j,l) = s$,

  (b) if $i \in V$ then $D(i) = I(i)$,

  (c) if $j \in C \setminus V$ then $D(j) \subseteq I(j)$ and for every $s \in I(j) \setminus D(j)$ there is $T \in \mathcal{S}_2$ such that $I(j)$ is connectable to T with s,

(6) if $j \in C \setminus V$ then there is $l \in V$ such that $F(l,j) \in \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}$,

(7) $\{G(S,l) \in \mathcal{A}^{\rightarrow} : l \in V\} \subseteq S$,

(8) for every $s \in S$, if $s \in \mathcal{A}^{\rightarrow}$ and there is no $T \in \mathcal{S}_2$ such that S is connectable to T with s then there is the unique $l \in V$ such that $G(S,l) = s$,

(9) for every $s \in S$, if there is no $l \in V$ such that $G(S,l) = s$ then there is $T \in \mathcal{S}_2$ such that S is connectable to T with s,

(10) for every $T \in \mathcal{S}_2$, S is connectable to T with some $t \in \mathcal{A}^{-}$.

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

Theorem 3 *Let $\mathcal{S}$ be 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. By Lemma 3, let $\mathfrak{A}$ be a structure and r be a constant such that $\mathfrak{A} \models \mathcal{S}$ and for every $S \in \mathcal{S}$ $rank_{\mathfrak{A}}(S) < r$ or $rank_{\mathfrak{A}}(S) = \infty$. Put
$\mathcal{S}_1 = \{S \in \mathcal{S} : rank_{\mathfrak{A}}(S) < r\}$,
$\mathcal{S}_2 = \{S \in \mathcal{S} : rank_{\mathfrak{A}}(S) = \infty\}$,
$V_1 = \{a \in A : rank_{\mathfrak{A}}(X_a^{\mathfrak{A}}) < r\}$,
$C_1 = V_1 \cup \{a \in A :$ there is $b \in V_1$ such that $tp^{\mathfrak{A}}(b,a) \in \mathcal{A}^{\rightarrow} \cup \mathcal{A}^{\leftrightarrow}\}$.

Without loss of generality we can assume that that the names of elements of V_1 and C_1 are $0, 1, \ldots, card(V_1) - 1$ and $0, 1, \ldots, card(C_1) - 1$, respectively. So, we can identify the set V_1 and C_1 with the set $card(V_1)$ and $card(C_1)$, respectively.

Let $V = card(V_1)$, $C = card(C_1)$. For every $i \in V$, put $I(i) = X_i^{\mathfrak{A}}$. For every $i, j \in C, i \neq j$, put $F(i,j) = tp^{\mathfrak{A}}(i,j)$. For every $S \in \mathcal{S}_2$ find $a \in A \setminus C$ such that $X_a^{\mathfrak{A}}(a) = S$, and for every $k \in V$ put $G(S,k) = tp^{\mathfrak{A}}(a,k)$.

One can easily check that conditions 1-10 of the definition hold.

($\Leftarrow$) Let $< \mathcal{S}_1, \mathcal{S}_2, V, C, I, F, G >$ be a finite representation of $\mathcal{S}$.

Case 1. $\mathcal{S}_1 = \emptyset$. By condition 3, $V = \emptyset$. By 6, $C = \emptyset$. Then, conditions 9 and 10 are equivalent to conditions (a) and (b) of Proposition 1.

Case 2. $\mathcal{S}_2 = \emptyset$. By condition 3, $V = C$. Then, by conditions 1-5, we can define $\mathfrak{B}$, a model for $\mathcal{S}$, in such a way that the universe of $\mathfrak{B}$ is V and for every $i, j \in V$, $tp^{\mathfrak{B}}(i,j) = F(i,j)$.

Case 3. $\mathcal{S}_1 \neq \emptyset$ and $\mathcal{S}_2 \neq \emptyset$. We will define a model $\mathfrak{A}$ for $\mathcal{S}$ with the universe $A \supseteq C$. During our infinite construction, cancelling and reserving have the same role as in the previous algorithms. Additionally, the given function I will be extended to all the elements of A in such a way that for every $j \in A$, $I(j) = X_j^{\mathfrak{A}}$. In every step of construction the universe of partially defined model $\mathfrak{A}$ is finite and it is assumed that there is a fixed linear ordering on the universe, and every new element added to the universe is greater then the old elements. The construction proceeds in two stages.

Stage 1.
1. Let $A = C$.
2. For every $i, j \in A$, put $tp^{\mathfrak{A}}(i,j) = F(i,j)$ (cf. (2) and (4) of Definition 8).
3. For every $i \in V$, cancel i.
4. For every $i, j \in C$, reserve $< i, j >$.

5. For every $S \in \mathcal{S}_2$ if there is no $j \in A$ such that $I(j) = S$, then add a new element b to A and put $I(b) = S$.

Stage 2. 1. Let j be the first not cancelled element of A ($I(j) \in \mathcal{S}_2$).

2. If $j \in C$ then
for every $s \in I(j) \setminus D(j)$ find $T \in \mathcal{S}_2$ such that $I(j)$ is connectable to T with s (cf. (c) in (5)), add a new element b to A, put $I(b) = T$, put $tp^{\mathfrak{A}}(j, b) = s$, reserve $< j, b >$,
cancel j,
go to 1.

3. For every $i \in V$ put $tp^{\mathfrak{A}}(j, i) = G(I(j), i)$ (cf. (7) and (8)).

4. For every $s \in I(j)$, if there is no $k \in A$ such that $< k, j >$ is reserved and $tp^{\mathfrak{A}}(k, j) = s^*$ then find $T \in \mathcal{S}_2$ that is connectable to $I(j)$ with s^* (cf. (9)), add a new element b to A, put $I(b) = T$, put $tp^{\mathfrak{A}}(j, b) = s$ and reserve $< j, b >$.

5. For every $i < j$, if $< i, j >$ is not reserved then find (cf. (10)) $t \in \mathcal{A}^-$ such that $I(j)$ is connectable to $I(i)$ with t, put $tp^{\mathfrak{A}}(j, i) = t$ and reserve $< j, i >$.

6. Cancel j.

7. Go to 1.

After performing stage 1, every $i \in V$ realizes the constellation $I(i) \in \mathcal{S}$ in the partially defined structure $\mathfrak{A}$, every constellation $S \in \mathcal{S}_1$ is realized by some $i \in V$ (cf. (3)) and only elements of V are cancelled. Moreover, for every $S \in \mathcal{S}$, there is $j \in A$ such that $I(j) = S$.

The aim of stage 2 is to realize all the constellations of $\mathcal{S}_2$ by elements of A. Step 2 is executed in case when some types between the chosen j and the other elements of A were defined according to the function F at stage 1. For every type of $I(j)$ that has not been defined, a new element b is added to A and some $T \in \mathcal{S}_2$ is put as $I(b)$. So, only constellations of $\mathcal{S}_2$ are to be realized in next steps. In step 5, when the types between an element j and earlier, already cancelled elements are defined, the constellation realized by the earlier elements are not changed because only types in $\mathcal{A}^-$ are put.

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

6. An example

It is well-known that the class $\mathcal{C}_1^2$ admits axioms of infinity, i.e. sentences that have only infinite models. Definition 8 was introduced in order to formulate an algorithm which solves the satisfiability problem for sentences in the constellation form without constructing the complete model. The idea is to use Theorem 3 and Theorem 1.

The size of the finite representation $< \mathcal{S}_1, \mathcal{S}_2, V, C, I, F, G >$ of a set of constellations $\mathcal{S}$ depends mainly on the cardinality of the set C that is bounded in Definition 8 by $4m \cdot (m \cdot card(\mathcal{S}))^{card(\mathcal{S})} = O(2^{2^{cn^2}})$. Below we give an example of a sentence in $\mathcal{C}_1^2$ that has finite models in which the cardinality of C is doubly exponential.

Proposition 2 *For every positive integer n there exists a sentence $\Phi \in \mathcal{C}_1^2$ of length $O(n \log n)$ such that Φ is satisfiable and, if $\mathfrak{A} \models \Phi$ then $card(\mathfrak{A}) = 2^{2^n} - 1$.*

Proof In our proof, following the idea of H. Lewis's [9] proof that NEXPTIME is reducible to the monadic Gödel class, we use an economical representation of the successor relation between encodings of natural numbers that is reminiscent to that used by N. Jones and A. Selman in [8].

Let n be a positive integer.

Let $\mathcal{L} = \{B_0, B_1, \ldots, B_{n-1}, C_0, C_1, \ldots, C_n, Left, Right, Root, Leaf\}$, where every B_i, C_i, $Root$, $Leaf$ are monadic predicate letters and $Left$, $Right$ are binary predicate letters. The sentence Φ will describe the unique model (up to isomorphism) that is a full binary tree of the height equal to 2^n.

The sentence Φ is a conjunction of the following sentences.

$$\exists^{=1} x\ Root(x)$$
$$\forall x\ [\neg Leaf(x) \rightarrow \exists^{=1} y\ Left(x, y)]$$
$$\forall x\ [\neg Leaf(x) \rightarrow \exists^{=1} y\ Right(x, y)]$$
$$\forall x\ [\neg Root(x) \rightarrow \exists^{=1} y\ (Left(y, x) \vee Right(y, x))]$$
$$\forall x \forall y\ \neg[Left(x, y) \wedge Right(x, y)]$$
$$\forall x \forall y\ [(Left(x, y) \vee Right(x, y)) \rightarrow \neg(Leaf(x) \vee Root(y))]$$
$$\forall x\ [Root(x) \leftrightarrow \bigwedge_{0 \leq i < n} \neg B_i(x)]$$
$$\forall x\ [Leaf(x) \leftrightarrow \bigwedge_{0 \leq i < n} B_i(x)]$$
$$\forall x\ C_n(x)$$
$$\forall x\ [\bigwedge_{0 \leq i < n} (C_i(x) \leftrightarrow (C_{i+1}(x) \wedge B_i(x)))]$$
$$\forall x \forall y\ [Left(x, y) \vee Right(x, y) \rightarrow (\bigwedge_{0 \leq i < n} (B_i(y) \leftrightarrow \neg(B_i(x) \leftrightarrow C_{i+1}(x))))]$$

Let, for every $d < 2^n$, $Level_d$ denotes the unique 1-type over the set $\{B_0, \ldots, B_{n-1}\}$ such that $B_i(x) \in Level_d$ 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 $\mathfrak{T}$ 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,
$Right(a,b)$	iff	b is the immediate right successor of a,
$Level_d(a)$	iff	the distance from the root to a is equal to d.

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

7. Complexity

Recall that for any function $t(n)$ from positive integers to positive integers, NTIME($t(n)$) is the class of all decision problems that can be solved by a nondeterministic 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.

Corollary 3 SAT($\mathcal{C}_1^2$) $\in$ 2-NEXPTIME.

Proof. Let Φ be a $\mathcal{C}_1^2$-sentence. Our algorithm works as follows.

First, build the sentence Ψ as in Theorem 2. This can be done deterministically in time polynomial with respect to the length of Φ (cf. Corollary 1).

Denote by $length(\Phi)$ the length of the sentence Φ taking into account the length of the representation of predicate letters. Note that if $\mid \Phi \mid = q$ according to the notation in Section 4 then $length(\Phi) = O(q \log q)$. Now, if $length(\Phi) = q$ then $length(\Psi) = O(q)$. Let $length(\Psi) = n$.

Next, by Theorem 1, build the sets $\mathcal{A}, \mathcal{R}$ and guess a set of constellations $\mathcal{S}$. Note that $card(\mathcal{A}) \leq 2^{4k}$, where $k = card(\mathcal{L})$ and $card(\mathcal{S}) \leq (2^{4k})^m$, where $m = card(\mathcal{R})$ (the number of existential quantifiers appearing in Ψ and in Φ as well). $\mathcal{S}$ can be guessed in time $(2^{4k})^m \cdot m \cdot 4k = O(2^{cn^2})$, for some constant c.

At the end, apply Theorem 3. Guess a system $< \mathcal{S}_1, \mathcal{S}_2, V, C, I, F, G >$. The components can be guessed nondeterministically in time:

$\mathcal{S}_1$, $\mathcal{S}_2$	–	$O(card(\mathcal{S})) = O(2^{cn^2})$, for some c,
V, C	–	$O(4m \cdot (m \cdot card(\mathcal{S}))^{card(\mathcal{S})}) = O(2^{2^{cn^2}})$, for some c,
I, F	–	$O(C^2) = O(2^{2^{cn^2}})$, for some c,
G	–	$O(card(\mathcal{S}_2) \cdot card(V)) = O(2^{2^{cn^2}})$.

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

Then, check whether the system is a finite representation of $\mathcal{S}$. It is easy to see that it also can be done in time $O(2^{2^{cn^2}})$.

The main result of this paper is the following theorem.

Theorem 4 SAT($\mathcal{C}_1^2$) $\in$ NEXPTIME.

In order to prove the theorem we introduce several new definitions.

Definition 9 Let $S \in \mathcal{S}$. A triple $< S, f, u >$ is an *indexed constellation of* S if $f : S \mapsto \mathcal{S}$, u is a positive integer and for every $s \in S$, S is connectable to $f(S)$ with s.

For a set of constellations $\mathcal{T}$, denote by $\mathcal{T}_{ind}$ the set of indexed constellations of $\mathcal{T}$.

Definition 10 $\mathcal{X} \subseteq \mathcal{T}_{ind}$ is *acceptable* if for every $T \in \mathcal{T}$ there is $< T, f, u > \in \mathcal{X}$ and if $< T, f, u > \in \mathcal{X}$ and $< T, f, v > \in \mathcal{X}$ then $u = v$.

For every $S \in \mathcal{S}$ denote by $H(S)$ the sum $\sum_{<S,f,u> \in \mathcal{X}} u$.

Definition 11 Let $S \in \mathcal{S}$. A set X of types is a *subconstellation of* S if $X \subseteq S$ and $center(S) \in X$.

Denote by $\overline{\mathcal{S}}$ the set of all subconstellations. The Definitions 4 and 5 of realizability of a constellation and of a model for a set of constellations apply also to subconstellations.

Let $\mathcal{X}$ be acceptable. Let $S, T \in \mathcal{S}$. Denote by $S\restriction_f\{T\}$ the set $\{s \in S : f(s) = T\} \cup \{center(S)\}$ and put

$$S\restriction_{\mathcal{X}}\{T\} = \{X \in \overline{\mathcal{S}} : X = S\restriction_f\{T\}, < S, f, u > \in \mathcal{X}\}.$$

Without loss of generality we can assume that there is a fixed ordering on the set $\mathcal{X}$.

Definition 12 An $\mathcal{L}$-structure $\mathfrak{A}$ is a *model for* S *with respect to* $\mathcal{X}$ ($\mathfrak{A} \models_{\mathcal{X}} S$) if and only if $\mathfrak{A} \models S\restriction_{\mathcal{X}}\{S\}$ and $A = \{a_1, \ldots, a_{u_1}, a_{u_1+1}, \ldots, a_{u_1+\ldots+u_k}\}$, where elements of every sequence $(a_{u_1+\ldots+u_{j-1}+1}, \ldots, a_{u_1+\ldots+u_j})$ realize the subconstellation $X = S\restriction_{f_j}\{S\}$ and $< S, f_j, u_j > \in \mathcal{X}$ is the j-th indexed constellation in the fixed ordering restricted to indexed constellations of S.

In other words, dealing with a model for S with respect to $\mathcal{X}$ we not only have a model for the subconstellations of S but we also guarantee which elements and in what quantity realize a subconstellation that is obtained from a fixed indexed constellation of S. Intuitively, this gives a possibility to expand such a model in a certain way.

Definition 13 An $\mathcal{L}$-structure $\mathfrak{A}$ is a *model for* $\{S,T\}$ *with respect to* $\mathcal{X}$ ($\mathfrak{A} \models_{\mathcal{X}} \{S,T\}$) if and only if $S \neq T$ and there exist $\mathfrak{A}_S$, $\mathfrak{A}_T \preceq \mathfrak{A}$, $A_S \dot{\cup} A_T = A$, $\mathfrak{A}_S \models S\restriction_{\mathcal{X}}\{S\}$, $\mathfrak{A}_T \models S\restriction_{\mathcal{X}}\{T\}$, and $A = \{a_1,\ldots,a_{u_1},a_{u_1+1},\ldots,a_{u_1+\ldots+u_k}\}$, where elements of every sequence $(a_{u_1+\ldots+u_{j-1}+1},\ldots,a_{u_1+\ldots+u_{j-1}+u_j}) \in A_S$ realize the subconstellation $X = S\restriction_{f_j}\{T\}$ and $< S,f_j,u_j > \in \mathcal{X}$ is the j-th indexed constellation in the fixed ordering restricted to the indexed constellations of S and elements of every sequence $(a_{v_1+\ldots+v_{i-1}+1},\ldots,a_{v_1+\ldots+v_{i-1}+v_i}) \in A_T$ realize the subconstellation $X = T\restriction_{f_i}\{S\}$ and $< T,f_i,v_i > \in \mathcal{X}$ is the i-th indexed constellation in the fixed ordering restricted to the indexed constellations of T.

Definition 14
A system $< \mathcal{S}_1,\mathcal{S}_2,\mathcal{S}_3,\mathcal{X}_1,\mathcal{X}_2,G_1,\ldots,G_{card(\mathcal{S}_3)} >$ is a *concise finite representation of* S if and only if

(1) $\mathcal{S}_1 \dot{\cup} \mathcal{S}_3 = \mathcal{S}$, $\mathcal{S}_2 \subseteq \mathcal{S}_3$,
(2) $\mathcal{X}_1 \subseteq \mathcal{S}_{1,ind}, \mathcal{X}_2 \subseteq \mathcal{S}_{2,ind}$ are acceptable,
(3) for every $S_i \in \mathcal{S}_3$, $G_i : S_i \mapsto \mathcal{S}_1 \cup \{\#\}$,
(4) for every $< S,f,u >$, if $< S,f,u > \in \mathcal{X}_1$ then $f(S) \subseteq \mathcal{S}_1 \cup \mathcal{S}_2$,
(5) for every $S_i,S_j \in \mathcal{S}_1 \cup \mathcal{S}_2$, where $i < j$, there exists $\mathfrak{A}_{ij}$ such that $\mathfrak{A}_{ij}$ is an expansion of $\mathfrak{A}_i \cup \mathfrak{A}_j$ and $\mathfrak{A}_{ij} \models_{\mathcal{X}} \{S_i,S_j\}$,
(6) for every $S \in \mathcal{S}_1 \cup \mathcal{S}_2$, for every $s \in S$, if $< S,f,u > \in \mathcal{X}_1 \cup \mathcal{X}_2$ and $f(s) \in \mathcal{S}_3$ then S is connectable to $f(s)$ with s,
(7) for every $S_i \in \mathcal{S}_3$, for every $s \in S_i$, if $G_i(s) \neq \#$ then $s \in \mathcal{A}^{\rightarrow}$ and S_i is connectable to $G_i(s)$ with s,
(8) for every $S_i \in \mathcal{S}_3$, for every $S \in \mathcal{S}_1$, $card(\{s \in S_i\colon G_i(s) = S\}) \leq H(S)$ and if $card(\{s \in S_i\colon G_i(s) = S\}) < H(S)$, then there is $t \in \mathcal{A}^{-}$ such that S_i is connectable to S with t.
(9) for every $S_i \in \mathcal{S}_3$ for every $s \in S_i$, if $G_i(s) = \#$ then there is $S \in \mathcal{S}_3$ such that S_i is connectable to S with s,
(10) for every $S,T \in \mathcal{S}_3$ S is connectable to T with some $t \in \mathcal{A}^{-}$.

Lemma 4 *$\mathcal{S}$ is a galaxy if and only if there exists a concise finite representation of $\mathcal{S}$.*

Proof. One can check that $\mathcal{S}$ is concisely finitely representable if and only if $\mathcal{S}$ is finitely representable. Now, use Theorem 3.

Proof of Theorem 4.

The proof proceedes in the same way as the proof of Corollary 3.

For a sentence Ψ in the $\exists^{=1}$-constellation form of the length n build the sets $\mathcal{A},\mathcal{R}$ and guess a set of constellations $\mathcal{S}$. Then, use Lemma 4 and guess a system $< \mathcal{S}_1,\mathcal{S}_2,\mathcal{S}_3,\mathcal{X}_1,\mathcal{X}_2,G_1,\ldots,G_{card(\mathcal{S}_3)} >$. In contrast to the proof of Corollary 3, this can be done in time $O(2^{cn^3}\cdot\log(2^{2^{cn^2}}) = O(2^{cn^3})$, for some constant c. For, note that $card(\mathcal{S}_{ind}) \leq 2^{cn^3}$ and maximal number of elements that realize a constellation from $\mathcal{S}_1$ or $\mathcal{S}_2$ is bounded by $card(C)$ from Theorem 3.

As the last step, check whether the conditions (1)-(10) hold. All the conditions besides (5) can be easily checked in the required time. We show that the same holds for condition (5). This will follow from two combinatorical lemmas given below.

Lemma 5 *Let Y be a set of cardinality y. Let $f_0,\ldots,f_{p-1} : y \overset{onto}{\longmapsto} y$, $f_0(x) = x$, $f_i(x) \neq f_j(x)$, for $0 \leq i < j < p$ and $f_i(x) = z$ then $f_j(z) \neq x$, for $0 \leq i,j < p$. There exists a function $g : y \overset{onto}{\longmapsto} y$, such that for every $x \in y$ for every $i, 0 \leq i < p$ $g(x) \neq f_i(x)$ and if $g(x) = z$ then $f_i(z) \neq x$, provided $y > 2p+3$.*

Proof. We use the Sylvester's Formula that is a special case of the Sieve Formula (cf. [1], Ch. 3., pp.90-91).

Sylvester's Formula *Let $Q = \{1,\ldots,q\}$, $P_1,\ldots,P_q \subset X$. The number of elements of X that do not belong to any of the sets P_i is*

$$T_q^0 = \sum_{k=0}^{q}(-1)^k \sum_{\substack{K\subseteq Q,\\ card(K)=k}} m(K),$$

where $m(K) = card(\bigcap_{i\in K} P_i)$ if $K \neq \emptyset$, and $m(\emptyset) = card(X)$.

Define X as the set of all permutations on y, $P_{ij} = \{f \in X : f_j(i) = f(i)$ or $f(i) = z$ and $f_j(z) = i\}$, for $i \in y$ and $j \in p$ and define $Q = y \times p$. If $K \subseteq Q$, $card(K) > y$, then there are two pairs $(i_1,j_1),(i_2,j_2)$ in the set K such that $i_1 = i_2$ and hence, $\bigcap_{(i,j)\in K} P_{ij} = \emptyset$. So, if $card(K) > y$ then $m(K) = 0$. If $card(K) = k$, $k \leq y$, then $K = \{(i_1,j_1),\ldots,(i_k,j_k)\}$, where $i_1,\ldots,i_k \in y$ and $j_1,\ldots,j_k \in p$. Therefore, $m(K) = (2p)^k(y-k)!$

and $\sum_{card(K)=k} m(K) = \binom{y}{k}(2p)^k(y-k)!$. So,

$$T_p^0 = y! \sum_{k=0}^{y} \frac{(-1)^k}{k!}(2p)^k.$$

Since $\sum_{k=0}^{\infty} \frac{(-1)^k}{k!}p^k = e^{-2p}$, we have $T_p^0 > 1$, provided $y > 2p+3$. □

In the same way one can prove the following lemma.

Lemma 6 *Let Y_1, Y_2 be two disjoint sets of cardinality y. Let $f_0, \ldots, f_{p-1} : Y_1 \mapsto Y_2$, $f_i(x) \neq f_j(x)$, for $0 \leq i < j < p$. There exists a function $g : Y_i \mapsto Y_2$, such that for every $x \in Y_1$ for every $i, 0 \leq i < p$ $g(x) \neq f_i(x)$, provided $n > p+2$.*

To check whether condition (5) holds, first, by definition, it is necessary to check if for every $S \in \mathcal{S}_1 \cup \mathcal{S}_2$ there exists $\mathfrak{A}_S$ such that $\mathfrak{A}_S \models_{\mathcal{X}} S$. This can be done separately for every S. Fix some $S \in \mathcal{S}_1 \cup \mathcal{S}_2$. Denote by $u(s) = \sum_{<S,f,u>:f(s)=S} u$ (the sum is easy computable from $\mathcal{X}$).

Our idea is to check if it is possible to put the types of subconstellations of $S\restriction_{\mathcal{X}}\{S\}$ in the amount given by $u(s)$. A necessary condition is that for every $s \in S \cap \mathcal{A}^{\leftrightarrow}$, $u(s) = u(s^*)$ and if $s = s^*$, then $u(s)$ is even.

In the case $u(s) > 2m+3$, by Lemma 5, the condition together with the requirement that S is connectable to S with some $t \in \mathcal{A}^{-}$ is sufficient. For every $s \in S$ such that $u(s) \leq 2m+3$ we check 'manually' the existence of an appropriate substructure of cardinality at most $m(2m+3)$.

For two constellations S, T we use the analogous method. □

As a consequence of Theorem 4, by the reduction of $\mathcal{C}^2$ to $\mathcal{C}_1^2$ given in [5], we get the following corollary.

Corollary 4 SAT($\mathcal{C}^2$) $\in$ 2-NEXPTIME.

References

[1] C. Berge. *Principles of Combinatorics.* Academic Press, Inc., 1971.

[2] A. Borgida. On the relative expressive power of description logics and predicate calculus. to appear.

[3] W. D. Goldfarb. The unsolvability of the Gödel class with identity. *J. Symb. Logic*, 49:1237–1252, 1984.

[4] E. Grädel, P. Kolaitis, and M. Vardi. On the decision problem for two-variable first-order logic. *Bull. of Symb. Logic*, 3, 1997. to appear.

[5] E. Grädel, M. Otto, and E. Rosen. Two-variable logic with counting is decidable. In *This Proceedings*, 1997.

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

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

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

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

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

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

[12] W. Szwast and L. Tendera. First-order two-variable logic is in NEXPTIME. submitted.