The Minimal Logically-Defined NP-Complete Problem

Régis Barbanchon, Etienne Grandjean

The Minimal Logically-Defined NP-Complete Problem

Régis Barbanchon and Etienne Grandjean

GREYC, Université de Caen, 14032 Caen Cedex, France
{regis.barbanchon,etienne.grandjean}@info.unicaen.fr

Abstract. We present an NP-complete problem defined by an existential monadic second-order formula over *functional structures* that :

1. is *minimal* under several syntactic criteria (i.e., any problem defined by an EMSO formula that further restricts one criterion becomes PTIME or trivial even if all other criteria are relaxed);
2. is *unique* for such restrictions, up to renamings and symmetries;

Our reductions and proofs are surprisingly very elementary and simple in comparison with some recent similar results classifying existential second-order formulas over *relational structures* according to their ability either to express NP-complete problems or to express only PTIME ones.

Key words: Computational Complexity, Descriptive Complexity, Finite Model Theory, Second-Order Logic, NP-Completeness, Parsimonious Reductions.

1 Introduction and main results

1.1 Which formulas express NP-complete problems?

In the line of Fagin's Theorem [4] which states that *existential second order logic* (ESO) captures the class NP, this paper studies the following natural question: what is (are) the most simple ESO sentence(s) that define(s) some NP-complete problem(s)? This question is somewhat related to two recent papers [6, 3] that completely classified prefix classes of ESO over strings and graphs (and more generally over *relational structures*) with respect to their ability to express either some NP-complete problems or only tractable (i.e., PTIME) ones. For example, it is easy to express an NP-complete problem over graphs, such as 3-colourability, in *existential monadic second-order logic* (EMSO) with only *two* first-order variables. In contrast, one notices that ESO formulas that use only *relation* ESO variables and only *one* first-order variable can only define easy (degenerate) properties on *relational structures*. The situation completely changes if *function* symbols are allowed either in the input signature or among the ESO symbols. For example, ESO formulas with *only one first-order variable* x of one of the forms (1-2):

$$(1) \quad \exists \overline{f}\ \forall x \quad \psi(x, \overline{f}, E)$$
$$(2) \quad \exists \overline{U}\ \forall x \quad \psi(x, \overline{f}, \overline{U})$$

where ψ is quantifier-free, $\overline{f}$ and $\overline{U}$ are lists of unary function symbols and of monadic relation symbols respectively, and E is a binary relation symbol, can express some NP-complete problems. More precisely, [8] have recently proved that formulas of form (1) exactly define graph problems (such as the Hamiltonian cycle problem) that are recognizable in nondeterministic linear time $O(n)$ where n is the number of vertices in the graph, and [1] states that any problem is linearly reducible to SAT iff it is linearly reducible to some problem expressible by some formula of the form (2) (see also [11]).

1.2 Minimal formulas for NP-complete problems

In this paper, we study the problem MIN_0 defined by the *very simple* EMSO formula φ_0 of the particular form (2) that follows.

Notation 1. *Let φ_0 denote the $\{f,g\}$-formula in* conjunctive normal form *(CNF)*

$$\begin{array}{ll}\varphi_0: & \exists U\ \forall x \quad \psi_0(x), \text{ where } \psi_0 \text{ is the conjunction}\\ \psi_0: & (Ux \vee Ufx) \wedge (\neg Ux \vee \neg Ufx \vee \neg Ugx),\end{array}$$

and f, g are unary function symbols. Let δ_0 denote the following formula in disjunctive normal form *(DNF) which is logically equivalent to φ_0:*

$$\delta_0: \quad \exists U\ \forall x \quad (Ux \wedge \neg Ufx) \vee (Ux \wedge \neg Ugx) \vee (\neg Ux \wedge Ufx).$$

The problem $\textsc{Min}_0$ *is defined as the set of finite models $\langle D, f, g\rangle$ of φ_0, or equivalently, of δ_0.*

We shall also study the following subproblems of $\textsc{Min}_0$:

Notation 2. *The problems* $\textsc{Min}_1$ *and* $\textsc{Min}_2$ *are resp. defined as* $\textsc{Min}_1 = \{\langle D, f, g\rangle$ *where f, g are permutations:* $\langle D, f, g\rangle \in \textsc{Min}_0\}$, *and* $\textsc{Min}_2 = \{\langle D, f, g\rangle$ *such that the graph $G(D, f, g)$ is planar:* $\langle D, f, g\rangle \in \textsc{Min}_1\}$, *where $G(D, f, g)$ is the graph (V, E) defined by $V = D$ and $E = \{(x, fx) : x \in D\} \cup \{(x, gx) : x \in D\} \cup \{(fx, gx) : x \in D\}$.*

Our main results are the following:

Theorem 1. $\textsc{Min}_0$ *and its subproblems* $\textsc{Min}_1$ *and* $\textsc{Min}_2$ *are NP-complete.*

Theorem 2 (Minimality). *φ_0 (resp. δ_0) is, for several syntactic criteria enumerated in Table 1, the* minimal *EMSO formula in CNF (resp. in DNF) of the form $\exists \overline{U}\ \forall \overline{x}\ \psi$ (where ψ is quantifier-free and $\overline{x}$ is a list of first-order variables) that defines an NP-complete problem under the hypothesis $P \neq NP$.*

input signature	2 unary functions	CNF (φ_0)	number of clauses	2
number of EMSO symbols	1		length	5
number of FO variables	1	DNF (δ_0)	number of anticlauses	3
number of distinct atoms	3		length	6

Table 1. Minimal syntactic criteria of EMSO formulas for NP-complete sets

Notation 3. *The* atoms *of a formula are its atomic subformulas. In particular, the distinct atoms of φ_0 (or δ_0) are Ux, Ufx and Ugx. The* length *of a formula is the total number of occurrences of atoms in it. The disjuncts of a DNF formula are called its* anticlauses.

Theorem 3 (Unicity). *φ_0 (resp. δ_0) is – up to symmetries detailed below – the* unique *minimal EMSO formula in CNF (resp. in DNF) of the form $\exists \overline{U}\ \forall \overline{x}\ \psi$ that defines an NP-complete problem.*

Remark 1. *The symmetrical formulas involved in Theorem 3 are obtained by any permutation of terms x, fx and gx and of U and $\neg U$ in φ_0 (resp. δ_0).*

1.3 Minimal formulas for #P-complete problems

Besides NP-completeness, another important concept of the theory of complexity is #P-completeness [14]. It is also natural to look for a minimal logical formula that defines some #P-complete problem. In this regard, it is well known that the generic reduction from any NP problem to SAT can (easily) be made parsimonious with a bijective and PTIME-computable correspondence between solutions. That means that problem SAT not only "simulates" the decision process of any problem in NP but also "reproduces" the number of its solutions and the "structure" of this set of solutions.

Notation 4. *For any problem M in NP, let us denote by $\#M$ the "natural" counting problem associated to M, i.e., the problem of counting its "natural" solutions. E.g., $\#\textsc{Sat}$ is the function that associates with each* SAT *instance F the number of assignments I such that $I \models F$; similarly, $\#\textsc{Min}_1$ is the function which associates to each instance $\mathcal{S} = \langle D, f, g\rangle$ of $\textsc{Min}_1$ the number $\#\{U \subseteq D : (\mathcal{S}, U) \models \forall x \quad \psi_0(x)\}$.*

We believe that:

Conjecture 1. *There exists* no parsimonious *reduction from $\#\textsc{Sat}$ to $\#\textsc{Min}_1$ (resp. $\#\textsc{Min}_2$).*

Nevertheless, we prove in this paper that:

Theorem 4. *There is some* weakly parsimonious *reduction from $\#\textsc{Sat}$ to $\#\textsc{Min}_1$ (resp. $\#\textsc{Min}_2$).*

Recall that for two counting problems #A and #B, a *weakly parsimonious* reduction from #A to #B is an ordered pair (r, μ) where r is a PTIME reduction from A to B and μ is a PTIME-computable function valued in positive integers such that for each instance w of A, we have $\#\{S : S \text{ is a solution of problem A for } w\} = \mu(w) \times \#\{s : s \text{ is a solution of problem B for } r(w)\}$.

In regard to Conjecture 1 concerning Formula φ_0, it is natural to look for another simple EMSO formula defining a problem to which SAT (and hence any NP problem) *parsimoniously* reduces. Let φ_{nand} denote the $\{f, g\}$-formula:

$$\begin{array}{ll} \varphi_{\text{nand}}: & \exists U\ \forall x \quad \psi_{\text{nand}}(x), \text{ where } \psi_{\text{nand}} \text{ is the "NAND" formula} \\ \psi_{\text{nand}}: & Ux \iff \neg(Ufx \wedge Ugx), \end{array}$$

which is equivalent to the conjunction of clauses:

$$(Ux \vee Ufx) \wedge (Ux \vee Ugx) \wedge (\neg Ux \vee \neg Ufx \vee \neg Ugx).$$

Clearly, ψ_{nand} (resp. φ_{nand}) implies ψ_0 (resp. φ_0). The formula φ_{nand} defines the following problems:

Notation 5. *The problems $\textsc{Nand}_1$ and $\textsc{Nand}_2$ are resp. defined as $\textsc{Nand}_1 = \{\langle D, f, g\rangle$ where f, g are permutations of the finite set D: $\langle D, f, g\rangle \models \varphi_{\text{nand}}\}$, and $\textsc{Nand}_2 = \{\langle D, f, g\rangle$ such that f, g are permutations of the finite set D and the graph $G(D, f, g)$ is planar: $\langle D, f, g\rangle \models \varphi_{\text{nand}}\}$.*

In contrast to Conjecture 1, we can prove that:

Theorem 5. **(i)** *$\#\textsc{Sat}$ parsimoniously reduces to $\#\textsc{Nand}_1$ (resp. $\#\textsc{Nand}_2$).* **(ii)** *If Conjecture 1 holds and $P \neq NP$, then φ_{nand} is (up to symmetries) the* unique minimal *EMSO formula for which (i) holds, i.e., that defines a problem over permutation structures $\langle D, f, g\rangle$ to which $\#\textsc{Sat}$ parsimoniously reduces.*

Surprisingly, our completeness proofs are rather simple and the reductions involved in Theorems 1 and 5 are essentially the same one reduction $\rho : F \mapsto \mathcal{S}(F)$ described in the next section.

2 Proof of the completeness results

2.1 The structures involved

Let us recall the three kinds of instances of our problems.

Definition 1. *A* function structure *is a finite structure $\langle D, f, g\rangle$ where $f, g : D \longrightarrow D$ are unary functions. A function structure $\langle D, f, g\rangle$ is a* permutation structure *(resp. is a planar permutation structure) if f, g are permutations of D (resp. are permutations of D such that the graph $G(D, f, g)$ is planar).*

Remark 2. *A permutation structure is naturally given by its f- and g-*circuits.

Definition 2 (Planar formula and PLAN-SAT). *Let F be a propositional formula in CNF. Let $G(F)$ denote the following bipartite graph (V, E) where V is the disjoint union of the set of variables and the set of clauses of F, and E is the set of pairs (v, C) such that v is a variable that occurs in clause C.*

F is a planar formula if $G(F)$ is a planar graph, and PLAN-SAT *is defined as the satisfiability problem of planar formulas.*

In our proofs of completeness, we will use the NP-complete problem PLAN-SAT [12].

2.2 A gadget

We are going to describe a reduction $\rho : F \mapsto \mathcal{S}(F)$ that associates to each SAT (resp. PLAN-SAT) instance F a permutation structure $\mathcal{S}(F)$ that contains many occurrences of the following gadget denoted True.

Definition 3. True *or* True(α, β, γ) *is the gadget depicted on the left of Fig. 1.*

The symbolization means that the gadget True plays the rôle of the Boolean constant "true" (or "1"). More formally, the following lemma expresses that in any case, $U(\gamma)$ *can* and *should* be true whereas the value of $U(g\gamma)$ (the "pending" g-edge of γ) is *free*.

Lemma 1. *Let* True(α, β, γ) *be a gadget included in a permutation structure $\mathcal{S} = \langle D, f, g\rangle$ and $U : D \longrightarrow \{0, 1\}$ be a monadic predicate*[1]*.*

1. *If $(\mathcal{S}, U) \models \varphi_0$ then we have $U(\alpha) = 1$, $U(\beta) = 0$ and $U(\gamma) = 1$;*
2. *Conversely: if $U(\alpha) = 1$, $U(\beta) = 0$ and $U(\gamma) = 1$, then the expanded structure $(True, U)$ satisfies φ_{nand} (and hence φ_0); in other words, $\varphi_{\text{nand}}(x)$ is satisfied by each element $x = \alpha, \beta, \gamma$ independently of the value of $U(g\gamma)$.*

Proof. Easy and left to the reader. □

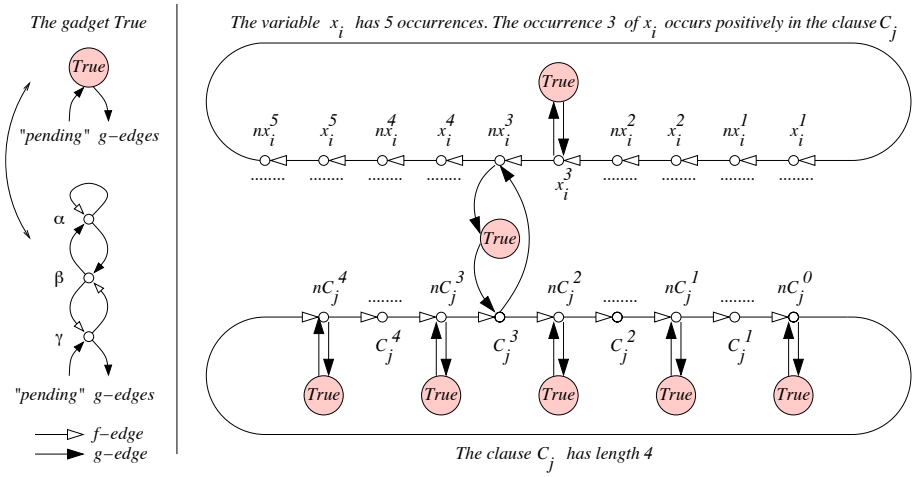

Fig. 1. The gadget True and the reduction around variable x_i and clause C_j

[1] For convenience, we confuse truth values "true" and "false" with 0 and 1 and assimilate a monadic predicate $U \subseteq D$ to its characteristic function $U : D \longrightarrow \{0, 1\}$.

2.3 Our reduction

Let us now construct our reduction $\rho : F \mapsto \mathcal{S}(F)$ where F is a SAT (resp. PLAN-SAT) instance, i.e., a conjunction of clauses $F = C_1 \wedge C_2 \wedge \cdots \wedge C_q$. In the description of the permutation structure $\mathcal{S}(F)$, we freely make use of the following notation:

Notation 6. *Whenever there exists some gadget $True(\alpha, \beta, \gamma)$ such that $g(x) = \gamma$ and $g(\gamma) = y$, we will often write $g(x) = True$ and $g(True) = y$ by commodity.*

Let us now describe the f- and g-circuits of our permutation structure $\mathcal{S}(F)$:

- For each variable x_i with r occurrences in F, construct the f-circuit:

$$(x_i^1, nx_i^1, x_i^2, nx_i^2, \cdots, x_i^{r-1}, nx_i^{r-1}, x_i^r, nx_i^r),$$

  where both vertices x_i^k, nx_i^k correspond to the k^{th} occurrence of x_i in F.
- For each clause $C_j = \lambda_1 \vee \cdots \vee \lambda_\ell$ in F, construct the f-circuit of odd length:

$$(nC_j^\ell, C_j^\ell, nC_j^{\ell-1}, C_j^{\ell-1}, \cdots, nC_j^1, C_j^1, nC_j^0),$$

  where the C_j^k and nC_j^k are new elements corresponding to the "prefix" of length k of the clause C_j defined as $prefix_k(C_j) = \lambda_1 \vee \cdots \vee \lambda_k$; Also construct the $\ell+1$ g-circuits (nC_j^k, True) for $0 \leq k \leq \ell$ using $\ell + 1$ new distinct gadgets True.
- If the k^{th} literal of C_j is the h^{th} occurrence – resp. negation of the h^{th} occurrence – of x_i, construct the g-circuits $(C_j^k, nx_i^h, \text{True})$ and (x_i^h, True) – resp. $(C_j^k, x_i^h, \text{True})$ and (nx_i^h, True) – using two new distinct gadgets True.

This completes the description of $\mathcal{S}(F)$ which is represented on the right of Fig. 1. The following lemma is obvious by the construction of $\mathcal{S}(F)$.

Lemma 2. *F is a planar formula iff $\mathcal{S}(F)$ is a planar permutation structure.*

2.4 Properties of the reduction

The following fact whose proof is straightforward will be useful in our study of the f-circuits of $\mathcal{S}(F)$ that correspond to the variables (resp. clauses) of F.

Fact 1. *Let $\mathcal{S} = \langle D, f, g \rangle$ be a permutation structure and $U : D \longrightarrow \{0, 1\}$ be a monadic predicate such that $(\mathcal{S}, U) \models \forall x\ \psi_0(x)$. Then, for every $a \in D$ such that $(\mathcal{S}, U) \models U(ga)$ (i.e., $U(ga) = 1$), it holds $U(a) = 1 - U(fa)$.*

Lemma 3. *If $\mathcal{S}(F)$ satisfies φ_0 then F is satisfiable.*

In order to prove Lemma 3, we need the following two claims:

Claim 1 (Existence of a witness literal for each clause). *Let U be a predicate such that $(\mathcal{S}(F), U) \models \forall x\ \psi_0(x)$. For each clause C_j, there exists at least one literal λ in C_j for which it holds: $U(nx_i^h) = 0$ if $\lambda = x_i$, and $U(x_i^h) = 0$ if $\lambda = \neg x_i$, where λ is the h^{th} occurrence of x_i.*

Claim 2 (Coherence of occurrences of the same variable). *Let U be a predicate such that $(\mathcal{S}(F), U) \models \forall x\ \psi_0(x)$. For each variable x_i occurring r times, it holds:*

$$U(x_i^1) = 1 - U(nx_i^1) = U(x_i^2) = 1 - U(nx_i^2) = \cdots = U(x_i^r) = 1 - U(nx_i^r).$$

We first prove Claims 1 and 2, and then deduce Lemma 3.

Proof (of Claim 1). Assume that the claim is false. Then there is a clause C_j such that for each literal λ, it holds $U(nx_i^h) = 1$ if $\lambda = x_i$ and $U(x_i^h) = 1$ if $\lambda = \neg x_i$. This implies $U(ga) = 1$ for each element a of the f-circuit of C_j, and hence $U(a) = 1 - U(fa)$ by Fact 1, which is impossible since the length of this f-circuit is odd. □

Proof (of Claim 2). It is an immediate consequence of Fact 1, applied to each element a of the f-circuit of x_i since we always have $g(a) = \text{True}$, and thus $U(ga) = 1$. □

Proof (of Lemma 3). Define the assignment I of the variables F as $I(x_i) = U(x_i^h) = 1 - U(nx_i^h)$, for each variable x_i and any $1 \leq h \leq r$, which is coherent by Claim 2. Claim 1 ensures that in each clause C_j of F, there is some literal λ such that $I(\lambda) = 1$. Hence, $I \models C_j$ and $I \models F$. □

Lemma 4 states the most precise property of our reduction $\rho : F \mapsto \mathcal{S}(F)$.

Lemma 4. *There is a bijective correspondence $I \mapsto U_I$ of the set of satisfying assignments $\{I : I \models F\}$ onto the set of monadic predicates $\{U : (\mathcal{S}(F), U) \models \forall x\ \psi_{\text{nand}}(x)\}$.*

For each I such that $I \models F$, let us construct its associated monadic predicate U_I, on the domain D of $\mathcal{S}(F)$. The correction will be ensured by Claim 3 and its converse Claim 4:

- Set $U_I(\alpha) = 1$, $U_I(\beta) = 0$ and $U_I(\gamma) = 1$ for each gadget $\text{True}(\alpha, \beta, \gamma)$ in $\mathcal{S}(F)$: this is justified by Lemma 1;
- For each variable x_i of F, set $U_I(x_i^h) = I(x_i)$ and $U_I(nx_i^h) = 1 - I(x_i)$, for each h;
- For each clause $C_j = \lambda_j^1 \vee \cdots \vee \lambda_j^\ell$, set $U_I(nC_j^0) = 1$, and for $k = 1, \cdots, \ell$, set $U_I(C_j^k) = \mathit{value}(\mathit{prefix}_k(C_j), I)$, and $U_I(nC_j^k) = 1 - \mathit{value}(\mathit{prefix}_k(C_j), I)$, where $\mathit{prefix}_k(C_j) = \lambda_j^1 \vee \cdots \vee \lambda_j^k$ and in particular $C_j = \mathit{prefix}_\ell(C_j)$.

In the following, we essentially use the well-known fact that all the Boolean connectives can be expressed by means of the NAND one only. More precisely, $1 - v = \text{NAND}(v, 1)$ and $\text{OR}(v, v') = \text{NAND}(1 - v, 1 - v')$.

Claim 3. $(\mathcal{S}(F), U_I) \models \forall x\ \psi_{\text{nand}}(x)$.

Proof. For each element a of the f-circuit of any variable x_i, we have $U_I(ga) = 1$ and $U_I(a) = 1 - U_I(fa)$, and hence $(\mathcal{S}(F), U_I) \models U(a) \iff \text{NAND}(U(fa), U(ga))$.

For every clause C_j of length ℓ, one easily obtains the following equalities for $1 \leq k \leq \ell$ if $C_j^k = C_j^{k-1} \vee x_i^h$:

- $U_I(nC_j^k) = 1 - U_I(C_j^k) = \text{NAND}(U_I(C_j^k), 1)$, and
- $U_I(C_j^k) = \text{NAND}(U_I(nC_j^{k-1}), U_I(nx_i^h))$;

and similarly in the case $C_j^k = C_j^{k-1} \vee \neg x_i^h$. This proves $(\mathcal{S}(F), U_I) \models \psi_{\text{nand}}(a)$ for every element $a \neq nC_j^0$ in the f-circuit of C_j. Finally, this also holds for $a = nC_j^0$ since $U_I(nC_j^\ell) = \mathit{value}(\neg C_j, I) = 0$ and, as a consequence, $U_I(nC_j^0) = 1 = \text{NAND}(U_I(nC_j^\ell), 1)$ as required. This completes the proof of Claim 3. □

It remains to prove the converse of Claim 3.

Claim 4. *Let U be a monadic predicate such that $(\mathcal{S}(F), U) \models \forall x\ \psi_{\text{nand}}(x)$. Then there is an assignment I, of course unique, such that $U = U_I$ and $I \models F$.*

Proof. It is a variant of the proof of Lemma 3 and is left to the reader. This completes the proof of Lemma 4. □

Lemmas 2, 3 and 4 together imply the following:

Corollary 1. (**i**) SAT *(resp.* PLAN-SAT*) reduces to problem* MIN_1 *(resp.* MIN_2*) by the reduction* $\rho : F \mapsto \mathcal{S}(F)$. (**ii**) #SAT *(resp.* #PLAN-SAT*) parsimoniously reduces to problem* $\#\text{NAND}_1$ *(resp.* $\#\text{NAND}_2$*).*

So, we have proved Theorems 1 and 5(i), by making use of the known result that #SAT parsimoniously reduces to #PLAN-SAT [12].

A careful analysis of our reduction $\rho : F \mapsto \mathcal{S}(F)$ from SAT (PLAN-SAT) to MIN_1 (MIN_2) shows that the only part of $\mathcal{S}(F)$ where this reduction is not parsimonious are the f-circuits of the clauses of F when at least two literals of some clause of F are true together. On the other hand, it is known that the problem $\frac{1}{3}$-SAT (also denoted one-in-three-SAT, see [5]) and its planar restriction PLAN-$\frac{1}{3}$-SAT defined below are equivalent to SAT and PLAN-SAT under parsimonious reductions (see [9]).

Definition 4. *Let* $\frac{1}{3}$-SAT *(resp.* PLAN-$\frac{1}{3}$-SAT*) denote the satisfiability problem of a conjunction of* $\frac{1}{3}$*-clauses (resp. planar* $\frac{1}{3}$*-clauses) of the form* $\frac{1}{3}(a,b,c)$ *whose meaning is "exactly one of the three variables* a, b, c *is true".*

Theorem 4 is a straightforward consequence of the following lemma:

Lemma 5. $\#\frac{1}{3}$-SAT *(resp.* #PLAN-$\frac{1}{3}$-SAT*) reduces to* $\#\text{MIN}_1$ *(resp.* $\#\text{MIN}_2$*) under a* weakly parsimonious *reduction.*

Proof. Let $F \mapsto F'$ be the trivial parsimonious and planarity-preserving reduction from $\frac{1}{3}$-SAT (resp. PLAN-$\frac{1}{3}$-SAT) to SAT (resp. PLAN-SAT) that replaces every $\frac{1}{3}$-clause $\frac{1}{3}(a,b,c)$ by the logically equivalent conjunction

$$(a \vee b \vee c) \wedge (\neg a \vee \neg b) \wedge (\neg b \vee \neg c) \wedge (\neg c \vee \neg a).$$

One notices that in each clause of this conjunction, except one of length two, e.g. $C = \neg a \vee \neg b$, exactly one literal is true and both literals of C are true. Let us now consider the composed reduction $\rho' : F \mapsto \mathcal{S}(F')$ from $\frac{1}{3}$-SAT (PLAN-$\frac{1}{3}$-SAT) to MIN_1 (MIN_2). If F contains q $\frac{1}{3}$-clauses then it holds

$$\#\{U : (\mathcal{S}(F'), U) \models \forall x\ \psi_0(x)\} = 2^q \times \#\{I : I \models F\}.$$

This is easily justified by a careful analysis of the f-circuits of clauses (of F') in $\mathcal{S}(F')$: one sees that each $\frac{1}{3}$-clause of F gives exactly 2 "local configurations" of the (union of four) f-circuits of the four corresponding clauses of F'. □

3 Proofs of minimality and unicity

3.1 Minimality of φ_0 and δ_0 in Theorem 2

W.l.g., for the sake of simplicity, we only consider EMSO formulas without equality, and without composition of functions, of the form: $\varphi : \exists \overline{U}\ \forall \overline{x}\ \psi$, where $\overline{U}$ (resp. $\overline{x}$) is a list of monadic relation symbols (resp. first-order variables) and ψ is quantifier-free.

Proof. We prove the minimality of:

• *the input signature* (= 2 unary function symbols)*:* A famous theorem of Courcelle [2], asserts that any MSO property of bounded tree-width structures can be checked in deterministic linear time. In particular, any EMSO property of σ-structures with $\sigma = \{f, U_1, \cdots, U_k\}$ where f is a unary function symbol and $U_1, \cdots, U_k$ are monadic relation symbols is checkable in linear time.

• *the number of EMSO symbols* (= 1)*:* Immediate since any first-order (FO) property is AC_0 and thus is PTIME.

• *the number of FO symbols* (= 1)*:* trivial.

• *the number of clauses in* φ_0 (= 2)*:* If an ESO formula φ in CNF has only one clause then it defines a trivial "yes"-problem.

• *the length of* φ_0 (= 5)*:* If the length of φ in CNF is at most 4 then φ either: (*i*) contains only clauses of length at most 2, or (*ii*) contains only one clause (of length 3 or 4), or (*iii*) contains exactly one clause of length 3 and one clause of length 1.

In case (*i*), φ is ESO-Krom and, as a consequence, defines a PTIME problem [7]. In case (*ii*), φ defines a trivial "yes-problem". Finally, in case (*iii*), one observes that the clause of length 3 either contains at most one positive literal or contains at most one negative literal. Hence, φ is either ESO-Horn or ESO-Anti-Horn, and thus defines in both cases a PTIME problem [7].

• *the number of distinct atoms* (= 3)*:* If φ in CNF contains at most 2 distinct atoms, then its clauses are trivially of length at most 2, and φ is ESO-Krom.

• *the number of anticlauses in* δ_0 (= 3)*:* Notice that any formula φ in DNF that contains at most 2 disjuncts is equivalent to a CNF formula that consists of clauses of length at most 2.

• *the length of* δ_0 *in DNF* (= 6)*:* If φ in DNF contains an anticlause of length 1, then it is a trivial "yes-problem". Thus, if φ in DNF defines an NP-complete problem, it consists of at least 3 anticlauses of length ≥ 2. □

3.2 Unicity up to symmetries of φ_0 and δ_0 in Theorem 3

Let us prove the unicity of φ_0 (the proof of δ_0 is similar). Let φ be an EMSO formula in CNF, without equality, that satisfies the conditions of Table 1 and defines an NP-complete problem over permutation structures $\langle D, f, g\rangle$. (The proof is similar but somehow longer in case of function structures.) φ is of the form $\exists U\ \forall x\ \psi(f, g, U, x)$, where ψ is a conjunction of two clauses C_1 and C_2 with $|C_1| + |C_2| = 5$ and $|C_1| < |C_2|$.

Proof. One notices that: (*i*) one clause consists of positive literals and the other one consists of negative literals: otherwise, φ would define a trivial "yes-problem", and (*ii*) $|C_1| = 2$ and $|C_2| = 3$: otherwise, C_1 would be unitary and φ would define a trivial "no-problem" since $\forall x\ C_1$ would be equivalent to $\forall x\ Ux$ or $\forall x\ \neg Ux$ (because f and g are permutations) and would contradict $\forall x\ C_2$ by point (*i*). These two points imply that φ should be one of the following two forms φ_0 or φ_0' up to permutations of f and g and of U and $\neg U$:

$$\begin{array}{lll} \varphi_0(f,g): & \exists U\ \forall x & (Ux\ \vee Ufx) \wedge\ (\neg Ux\ \vee \neg Ufx \vee \neg Ugx) \\ \varphi_0'(f,g): & \exists U\ \forall x & (Ugx \vee Ufx) \wedge (\neg Ugx \vee \neg Ufx \vee\ \neg Ux). \end{array}$$

Formulas φ_0 and φ_0' essentially define the same problem over permutation structures (resp. planar permutation structures) $\langle D, f, g\rangle$: By replacing x by $g^{-1}x$ in the matrix of the formula φ_0, we immediately get the equivalence:

$$\langle D, f, g\rangle \models \varphi_0(f, g) \iff \langle D, f', g'\rangle \models \varphi_0'(f', g'),$$

where $f' = g^{-1}$ and $g' = fg^{-1}$. This also makes sense for planar permutation structures since $G(D, f, g)$ is planar iff $G(D, f', g')$ is planar. □

It remains to prove Theorem 5(*ii*), more precisely reformulated as follows: Assume Conjecture 1 and P $\neq$ NP. Then φ_{nand} is (up to permutations of x, fx, gx and of U and $\neg U$) the *unique minimal* EMSO $\{f, g\}$-formula in CNF of the form $\exists U\ \forall x\ \psi(x)$ with atoms Ux, Ufx and Ugx that defines a problem over permutation structures to which #SAT *parsimoniously* reduces. More precisely, φ_{nand} has a minimal number of clauses (= 3), and a minimal length (= 7).

3.3 Minimality of φ_{nand} in Theorem 5(ii)

Proof. We proove the minimality of:

• *the number of clauses* $(= 3)$*:* Clearly, any EMSO formula of the required form that defines an NP-complete problem with exactly two clauses has exactly one purely negative clause and one purely positive clause, and has at least one clause of length 3 and no clause of length 1; so, the other one has length 2 or 3. This gives only two possible forms: our minimal formula φ_0 (and its symmetrical variants), and φ_{nae} defined as:

$$\begin{array}{ll} \varphi_{\text{nae}}: & \exists U\ \forall x \quad \psi_{\text{nae}}(x), \text{ where } \psi_{\text{nae}} \text{ is the "not-all-equal" formula} \\ \psi_{\text{nae}}: & (Ux \vee Ufx \vee Ugx) \wedge (\neg Ux \vee \neg Ufx \vee \neg Ugx). \end{array}$$

One easily sees that for any function structure $\mathcal{S}$, the number $\#\{U : (\mathcal{S}, U) \models \forall x\ \psi_{\text{nae}}(x)\}$ is *even* because ψ_{nae} is invariant by inversion of U and $\neg U$. So, no reduction from SAT to the problem defined by φ_{nae} (if such a polynomial reduction exists) can be parsimonious with the standard way of counting solutions.

• *the length* $(= 7)$*:* It is a consequence of the fact that there should be at least two clauses each of length ≥ 2, and at least one of length 3. □

3.4 Unicity of φ_{nand} in Theorem 5(ii)

Proof. Clearly, any formula that meets our minimality conditions, i.e., that has three clauses and length 7, has exactly one clause of length 3 and two clauses of length 2. Moreover, one notices that:

(i) At least one clause is purely positive and at least one is purely negative;
(ii) No 2-clause subsumes the 3-clause;
(iii) Each 2-clause must disagree with the 3-clause on the sign of every literal: otherwise, if we write the 3-clause as $(\ell_1 \vee \ell_2 \vee \ell_3)$, either the 2-clause is of the form $(\ell_1 \vee \ell_2)$ and then its subsumes the 3-clause, or the 2-clause is of the form $(\overline{\ell_1} \vee \ell_2)$ and then a resolution step over ℓ_1 induces the 2-clause $(\ell_2 \vee \ell_3)$ that in turn subsumes the 3-clause. This contradicts (ii);
(iv) The 2-clauses have exactly one atom in common: They clearly have at least one since there are only three atoms available. Now, if they have two, they disagree on the sign of either one literal or two literals. If we have $(\ell_1 \vee \ell_2) \wedge (\ell_1 \vee \overline{\ell_2})$, then a resolution step over ℓ_2 induces the 1-clause (ℓ_1). If we have $(\ell_1 \vee \ell_2) \wedge (\overline{\ell_1} \vee \overline{\ell_2})$, then $\ell_1 \iff \overline{\ell_2}$ and the 3-clause reduces either to a 2-clause or to "true" by replacing ℓ_1 by $\overline{\ell_2}$;
(v) The 3-clause must be monotone. Otherwise, by (i), the two 2-clauses must be monotone of opposite sign: Let then ε be the majoritary sign of the 3-clause. The 2-clause of sign ε cannot disagree on the sign of every literal with the 3-clause, since this latter has only one literal of sign $\overline{\varepsilon}$. This contradicts (iii);
(vi) Both 2-clauses are monotone, of the same sign, opposite to the sign of the 3-clause: This is a direct consequence of (iii) and (v).

Clearly, Remarks (iv), (v) and (vi) together leave exactly ψ_{nand} and its symmetrical variants as the only candidates. □

4 Conclusion and open problems

Exhibiting "the" minimal EMSO formula that defines an NP-complete problem over function structures is the main contribution of this paper. This also hold for restrictions to permutations structures or even to planar permutation structures. A striking point is the unicity (up to symmetries) of our formula. This delineates a very neat frontier in logic between NP-complete problems and tractable ones. There remain several open problems:

The main one is Conjecture 1. Its proof, if true, seems very difficult except if it can be shown that the counting problem $\#\text{MIN}_1$ (resp. $\#\text{MIN}_2$) has some combinatorial property, to be compared, e.g., to the known fact that the number of Hamiltonian cycles visiting an arbitrary edge in a cubic graph is even (see [13]).

Another interesting objective consists in looking for a necessary and sufficient decidable condition for which any EMSO formula of the form $\exists \overline{U}\ \forall \overline{x}\ \psi(\overline{U}, \overline{f}, \overline{x})$ and of unary signature $\overline{f}$ expresses an NP-complete problem over $\overline{f}$-structures (resp. over permutation $\overline{f}$-structures, or over planar permutation $\overline{f}$-structures.)

Other problems of less importance are the following: Does the EMSO formula φ_{nae} of subsection 3.3 define a PTIME or NP-complete problem over permutation structures? Notice that φ_{nae} defines a trivial a PTIME problem over planar permutation structures since the problem NAE-SAT is PTIME for planar instances [10].

Analogue of Conjecture 1 for function structures: Is there a parsimonious reduction from $\#\text{SAT}$ to $\#\text{MIN}_0$?

References

[1] R. Barbanchon and E. Grandjean. Local problems, planar local problems and linear time. In *Computer Science Logic*, volume 2471 of *LNCS*, pages 397–411. Springer, 2002.

[2] B. Courcelle. On the expression of graph properties in some fragments of monadic second-order logic. In N. Immermann and P. Kolaitis, editors, *Descriptive Complexity and Finite Models*, pages 33–62. American Mathematical Society, 1997.

[3] T. Either, G. Gottlob, and Y. Gurevitch. Existential second order logic over strings. *JACM*, 41(1):77–131, 2000.

[4] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *Complexity and Computation*, 7:43–73, 1974.

[5] M. R. Garey and D. S. Johnson. *Computers and Intractability*. W.H. Freeman and Co., 1979.

[6] G. Gottlob, P. G. Kolaitis, and T. Schwentick. Existential second-order logic over graphs: Charting the tractability frontier. *FOCS*, pages 664–674, 2000.

[7] E. Grädel. Capturing complexity classes by fragments of second order logic. *TCS*, 101(1):35–57, 1991.

[8] E. Grandjean and F. Olive. Graph properties checkable in linear time in the number of vertices. *JCSS (to be published)*, 2003.

[9] H. B. Hunt III, M. V. Marathe, V. Radhakrishnan, and R. E. Stearns. The complexity of planar counting problems. *SIAM Journal on Computing*, 27(4):1142–1167, 1998.

[10] J. Kratochvíl and Z. Tuza. On the complexity of bicoloring clique hypergraphs of graphs. *SODA*, pages 40–41, 2000.

[11] C. L. Lautemann and B. Weinzinger. Monadic-NLIN and quantifier-free reductions. In *CSL, 8th annual conference of the EACSL, Lect. Notes Comput. Sci.*, volume 1683 of *LNCS*, pages 322–337, 1999.

[12] D. Lichtenstein. Planar formulae and their uses. *SIAM Journal on Computing*, 11(2):329–343, 1982.

[13] C.H. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, MA, 1994.

[14] L. G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.