Dichotomy theorem for the generalized unique satisfiability problem

Miki Hermann, Laurent Juban

Dichotomy Theorem for the Generalized Unique Satisfiability Problem

Miki Hermann and Laurent Juban

CRIN (CNRS) and INRIA-Lorraine, BP 239, 54506 Vandœuvre-lès-Nancy, France.
{hermann, juban}@loria.fr

Abstract. The unique satisfiability problem, that asks whether there exists a unique solution to a given propositional formula, was extensively studied in the recent years. This paper presents a dichotomy theorem for the unique satisfiability problem, partitioning the instances of the problem between the polynomial-time solvable and coNP-hard cases. We notice that the additional knowledge of a model makes this problem coNP-complete. We compare the polynomial cases of unique satisfiability to the polynomial cases of the usual satisfiability problem and show that they are incomparable. This difference between the polynomial cases is partially due to the necessity to apply parsimonious reductions among the unique satisfiability problems to preserve the number of solutions. In particular, we notice that the unique not-all-equal satisfiability problem, where we ask whether there is a unique model such that each clause has at least one true literal and one false literal, is polynomially solvable.

1 Introduction

The satisfiability problem SAT of a propositional formula in conjunctive normal form is a well-known **NP**-complete problem. Schaefer [Sch78] analysed the generalized satisfiability problem, where each clause is represented by an arbitrary logical relation. He presented a Dichotomy Theorem for the generalized satisfiability problem, exhibiting conditions under which the problem is polynomial-time solvable, otherwise the problem is **NP**-complete. A similar dichotomy theorem was presented in [CH96] for the problem #SAT of counting the number of models of a propositional formula. In particular, Creignou and Hermann show that if a decision satisfiability problem is intractable (**NP**-complete) then the corresponding counting satisfiability problem is also intractable (#P-complete).

The unique satisfiability problem UNIQUE SAT is defined as follows: given a propositional formula, is it true that it has a unique model (i.e., a unique satisfying truth assignment)? UNIQUE SAT is known to be **coNP**-hard [BG82], but it is not known whether it is in **coNP**. This problem is known to be only in **DP**, the class of languages equal to an intersection of two languages, one from **NP** and the other from **coNP**. UNIQUE SAT is therefore an intriguing problem from the point of vue of collapsing complexity classes (see [Pap94, Chapter 17] or [CKR95]). We associate to UNIQUE SAT the problem ANOTHER SAT defined as follows: given a propositional formula ϕ and a model m of ϕ, is it true that there

exists another model of ϕ different from m? It is clear that there is a certain relation between the two problems. If there is an instance of UNIQUE SAT that is true, then the corresponding instance of ANOTHER SAT must be false. Conversely, if an instance of ANOTHER SAT is true then the corresponding instance of UNIQUE SAT must be false. In this paper, we investigate the relation between UNIQUE SAT and ANOTHER SAT in terms of complexity. We study the polynomial-time solvable cases of both problems and compare it with the intractable cases. We also relate the intractable cases between the two problems.

Several polynomial-time solvable cases of UNIQUE SAT were studied in the literature. Minoux [Min92] noticed that for any subclass of polynomial-time solvable instance of the satisfiability problem with constants, UNIQUE SAT is also polynomially solvable. In particular, Hansen and Jaumard [HJ85] proposed a linear time UNIQUE SAT algorithm for 2SAT formulas, whereas several efficient UNIQUE SAT algorithms for Horn formulas were presented in the papers [Min92,BFS95,Pre93], ranging from quadratic to linear time. It would be interesting to know whether the four polynomial cases of SAT (namely Horn, anti-Horn, affine, and 2SAT formulas) are the only polynomial cases of UNIQUE SAT. Another interesting question is to know how the polynomial-time solvable cases of UNIQUE SAT and ANOTHER SAT relate to each other.

Both problems UNIQUE SAT and ANOTHER SAT involve some rudimentary counting. For this reason we cannot relate general unique satisfiability problems through ordinary polynomial many-one reductions. It is not enough to relate these problems through counting (sometimes also called weakly parsimonious) reductions (see [Pap94, Chapter 18], [Koz92], or [CH96] for a definition). Roughly speaking, a counting reduction R associates one solution of an input x to a constant number of solutions of the instance $R(x)$. Hence, in general, a counting reduction may reduce an instance x of a problem A with a unique solution to an instance $R(x)$ of a problem B with more solutions. Therefore we need to apply only reductions that exactly preserve the number of solutions between instances of the problems UNIQUE SAT and ANOTHER SAT, respectively. The number of solutions between instances is exactly preserved by the parsimonious reductions. Notice in this connection that it was not always possible to derive #P-hardness lower bounds for generalized satisfiability counting problems in [CH96] using only parsimonious reductions. Creignou and Hermann were obliged to apply weakly parsimonious reductions in the presence of the so-called complementive formulas. This indicates that complementive logical relations will be of special interest for the UNIQUE SAT and ANOTHER SAT problems.

2 Preliminaries

Let us recall some basic definitions and notions concerning complexity classes, reductions, and complete problems. More information can be found in the monographs [GJ79,Pap94]. Some parts of these preliminaries are taken from [Sch78] or [CH96] and are quoted only for self-containment of the paper.

We assume the knowledge of the following notions and notation. **NP** is the class of decision problems (languages) that can be solved in polynomial time

by a *nondeterministic* Turing machine, **coNP** is the class of decision problems (languages) whose complements are in the class **NP**. For example, the problem SAT of deciding the satisfiability of a propositional formula in conjunctive normal form is in **NP**, whereas the UNSAT problem of deciding whether a propositional formula is unsatisfiable is in **coNP**.

Let A and B be two decision problems (languages). A polynomial-time many-one *reduction* from A to B is a polynomial-time computable function R from string to strings, such that for all inputs x the following holds: $x \in A$ if and only if $R(x) \in B$. For our purposes we will need *parsimonious reductions* that preserve the number of solutions. A polynomial reduction R from A to B is parsimonious if, for all $x \in A$, there is an equality between the number of solutions of x and $R(x)$. In particular, if there is a unique solution of the instance x of a problem A and there is a parsimonious reduction R from A to B then the instance $R(x)$ of the problem B has a unique solution, too.

Let C be a complexity class. A decision problem A is **C-hard** if for all problems $B \in$ C there exists a polynomial-time reduction from B to A. If in addition A is a member of C, then we say that the problem A is **C-complete**.

Let $S = \{R_1, \ldots, R_m\}$ be a finite set of logical relations. A logical relation is defined to be any subset of $\{0,1\}^k$ for some integer $k \geq 1$. An S-formula is any conjunction of clauses, each of the form $R_i(\mathbf{v})$, where $\mathbf{v}$ is a vector of not necessarily distinct variables. We overload the symbol R for a logical relation and the corresponding formula. The *unique S-satisfiability problem* UNIQUE SAT(S) is the problem of deciding whether a given S-formula has a unique model. The *another S-model problem* ANOTHER SAT(S) is the problem of deciding whether a given S-formula has another model different from a given model m. The problems UNIQUE SAT$_c(S)$ and ANOTHER SAT$_c(S)$ are the variations of UNIQUE SAT and ANOTHER SAT, respectively, where the Boolean constants are allowed to occur in the formulas (e.g., R(x,0,z) is allowed). The problems UNIQUE 3SAT and ANOTHER 3SAT are the versions of UNIQUE SAT and ANOTHER SAT, respectively, where every clause of the propositional formula contains three literals. The main result of our paper characterizes the complexity of UNIQUE SAT(S) and ANOTHER SAT(S) as properties of the logical relations in the set S.

If x is a variable, $\bar{x}$ denotes its negation. If ϕ is a formula, $\mathcal{V}ar(\phi)$ denotes the set of variables occurring in ϕ. We denote by Sat(ϕ) the set of truth assignments (models) m: $\mathcal{V}ar(\phi) \to \{0,1\}$ that satisfy ϕ. We denote a model $m = (b_1, \ldots, b_n)$ as a string $b_1 \cdots b_n$ of its concatenated values. Let $m, m_1, m_2 \in$ Sat(ϕ) be models of the formula ϕ. We define the following four operations on models:

- $\bar{m}$ is defined by $\bar{m}(x) = 1$ iff $m(x) = 0$ and $\bar{m}(x) = 0$ otherwise,
- $m = m_1 \oplus m_2$: $m(x) = 1$ iff $m_1(x) \neq m_2(x)$ and $m(x) = 0$ otherwise,
- $m = m_1 \wedge m_2$: $m(x) = 1$ iff $m_1(x) = m_2(x) = 1$ and $m(x) = 0$ otherwise,
- $m = m_1 \vee m_2$: $m(x) = 0$ iff $m_1(x) = m_2(x) = 0$ and $m(x) = 1$ otherwise.

Two formulas ϕ and ψ are *logically equivalent* if and only if they have the same variable domains and their sets of models coincide. Two formulas ϕ and ψ are *quasi-equivalent* [CH96] if and only if there exists a bijection between the sets Sat(ϕ) and Sat(ψ), such that each pair of models m and m' in the bijec-

tion coincides on the common variables of the formulas ϕ and ψ, i.e, such that $m(x) = m'(x)$ holds for every variable $x \in \mathrm{Sat}(\phi) \cap \mathrm{Sat}(\psi)$. As a consequence, the sets of models $\mathrm{Sat}(\phi)$ and $\mathrm{Sat}(\psi)$ have the same cardinality. The notion of quasi-equivalence is important in the presence of parsimonious and counting reductions, as it was shown in [CH96], since it preserves the number of solutions.

If ϕ is a formula, v is a variable, and l is a literal or a Boolean constant, then $\phi[l/v]$ denotes the formula obtained from ϕ by replacing each occurrence of v by l. If V is a set of variables, then $\phi[l/V]$ denotes the result of substituting l for every occurrence of each variable in V. We denote by $[\phi]$ the logical relation defined by the formula ϕ, when the variables are taken in lexicographic order. The relation 1-in-3 is the logical relation $\{001, 010, 100\}$.

The set of quasi-equivalent S-formulas with constants, $\mathcal{G}en(S)$, is the smallest set of formulas such that

- for all logical relations $R \in S$ and all vectors of variables $\mathbf{v}$, $R(\mathbf{v}) \in \mathcal{G}en(S)$,
- for all formulas $\phi, \psi \in \mathcal{G}en(S)$ and all variables x, y, the following formulas are all in $\mathcal{G}en(S)$: $\phi \wedge \psi$, $\phi[y/x]$, $\phi[0/x]$, $\phi[1/x]$, and
- if $\phi \in \mathcal{G}en(S)$ and ψ is quasi-equivalent to ϕ then also $\psi \in \mathcal{G}en(S)$.

Hence, $\mathcal{G}en(S)$ is the smallest set of quasi-equivalent S-formulas closed under conjunction, renaming, and substitution by a Boolean constant, whereas $\mathcal{G}en_b(S)$ is the smallest set of quasi-equivalent S-formulas closed under conjunction, renaming, and substitution by the Boolean constant b. The set of quasi-equivalent S-formulas without Boolean constants is denoted by $\mathcal{G}en_{nc}(S)$.

We define the set of all *relation representable* by quasi-equivalent S-formulas *with Boolean constants* as $\mathcal{R}ep(S) = \{[\phi] \mid \phi \in \mathcal{G}en(S)\}$ and the set of all *relations representable* by quasi-equivalent S-formulas *without Boolean constants* as $\mathcal{R}ep_{nc}(S) = \{[\phi] \mid \phi \in \mathcal{G}en_{nc}(S)\}$. $\mathcal{R}ep_b(S)$ is the set of all relations that are representable by quasi-equivalent S-formulas with the Boolean constant b only.

We adopt the usual syntactic characterization of logical relations and formulas. A Horn formula is a formula in conjunctive normal form with at most one positive literal per clause. Dually, an anti-Horn formula is a formula in conjunctive normal form with at most one negative literal per clause. A k-cnf formula, for a positive integer k, is a propositional formula in conjunctive normal form with k literals per clause. We say that a logical relation R is

- **0-valid** if $(0 \cdots 0) \in R$, **1-valid** if $(1 \cdots 1) \in R$;
- **Horn** if $R(\mathbf{v})$ is logically equivalent to a Horn formula, **anti-Horn** if $R(\mathbf{v})$ is logically equivalent to an anti-Horn formula;
- **affine** if the formula $R(\mathbf{v})$ is logically equivalent to a system of linear equations over the smallest Boolean ring $\mathbb{Z}_2$;
- **2SAT** if the formula $R(\mathbf{v})$ is logically equivalent to a 2-cnf formula;
- **complementive** if for every model $(a_1 \cdots a_n) \in R$ there exists the complementary model $(1 - a_1 \cdots 1 - a_n) \in R$.

3 General unique satisfiability problem

Theorem 1 (Dichotomy Theorem). *Let S be a finite set of logical relations. If S satisfies one of the conditions (1) to (6) below, then* ANOTHER SAT(S) *and* UNIQUE SAT(S) *are polynomial-time solvable. Otherwise,* ANOTHER SAT(S) *is* ***NP****-complete and* UNIQUE SAT(S) *is* ***coNP****-hard.*

1. *Every relation in S is 0-valid and 1-valid.*
2. *Every relation in S is complementive.*
3. *Every relation in S is Horn.*
4. *Every relation in S is anti-Horn.*
5. *Every relation in S is affine.*
6. *Every relation in S is 2SAT.*

Notice that UNIQUE SAT(S) becomes **coNP**-complete if either every relation in S is 0-valid or every relation in S is 1-valid, since then it can be expressed as the complement of the problem ANOTHER SAT(S) with the given model $0\cdots0$ or $1\cdots1$, respectively. This result can be generalized to an arbitrary model. The problem UNIQUE SAT(S) with the additional information that there exists a model is just the complement of the problem ANOTHER SAT(S), and therefore it is **coNP**-complete.

Notice also that the problem UNIQUE NOT-ALL-EQUAL SAT, asking whether there is a unique model, such that in no clause are all literals evaluated to the same Boolean constant (i.e., $(0\cdots0)$ and $(1\cdots1)$ are excluded), is polynomial-time solvable, since the relation $nae = \{001, 010, 011, 100, 101, 110\}$ is complementive. Indeed, if m is a model of a complementive formula ϕ then also the dual $\bar{m}$ is a model of ϕ. Hence, a complementive formula has never an odd number of models. On the other hand, recall that the satisfiability problem NOT-ALL-EQUAL SAT is **NP**-complete.

The rest of the paper is devoted to the proof of the Dichotomy Theorem for UNIQUE SAT(S) and ANOTHER SAT(S).

Proposition 2. *Let S be a finite set of logical relations. If S satisfies one of the conditions (3) to (6) of Theorem 1, then $\mathcal{R}ep_b(S)$ satisfies the same condition. Otherwise, $\mathcal{R}ep_b(S)$ is the set of all logical relations.*

The proof of this proposition requires several intermediate results. First, we need a tool for detecting the polynomial cases. See [Sch78] or [CH96] for details.

Proposition 3. *Let R be a logical relation and let $\phi = R(\mathbf{v})$ be the corresponding formula. Then*

- *R is Horn iff $m_1, m_2 \in \mathrm{Sat}(\phi)$ implies $(m_1 \wedge m_2) \in \mathrm{Sat}(\phi)$;*
- *R is anti-Horn iff $m_1, m_2 \in \mathrm{Sat}(\phi)$ implies $(m_1 \vee m_2) \in \mathrm{Sat}(\phi)$;*
- *R is affine iff $m_1, m_2, m_3 \in \mathrm{Sat}(\phi)$ implies $(m_1 \oplus m_2 \oplus m_3) \in \mathrm{Sat}(\phi)$;*
- *R is 2SAT iff $m_1, m_2, m_3 \in \mathrm{Sat}(\phi)$ implies $(m_1 \vee m_2) \wedge (m_2 \vee m_3) \wedge (m_3 \vee m_1) \in \mathrm{Sat}(\phi)$.*

Lemma 4. *Let R be a logical relation. If R is not Horn then the set $\mathcal{R}ep_b(\{R\})$ contains the relations $[x \not\equiv y]$ or $[x \vee y]$ for each $b \in \{0,1\}$. If R is not anti-Horn then $\mathcal{R}ep_b(\{R\})$ contains the relations $[x \not\equiv y]$ or $[\bar{x} \vee \bar{y}]$ for each $b \in \{0,1\}$.*

Proof. We do the proof only for the case of R not being Horn and $b = 0$. The proof of the other cases is similar.

Let R be a logical relation which is not Horn and let $\phi = R(\mathbf{v})$ be the corresponding formula. We show that $\mathcal{R}ep_0(\{R\}) \cap \{[x \not\equiv y], [x \vee y]\} \neq \emptyset$. Following Proposition 3, there exist two models $m_1, m_2 \in \mathrm{Sat}(\phi)$ such that $(m_1 \wedge m_2) \notin \mathrm{Sat}(\phi)$. Moreover, we have that $m_1 \neq (0 \cdots 0)$ (since $(0 \cdots 0) \wedge m_2 = (0 \cdots 0) \in \mathrm{Sat}(\phi)$), $m_1 \neq (1 \cdots 1)$ (since $(1 \cdots 1) \wedge m_2 = m_2 \in \mathrm{Sat}(\phi)$), $m_1 \neq m_2$ (since it would imply $m_1 \wedge m_2 = m_1 \in \mathrm{Sat}(\phi)$), and there exists a variable $x \in \mathcal{V}ar(\phi)$ such that $m_1(x) = 1$ and $m_2(x) = 0$ (otherwise we get $m_1 \wedge m_2 = m_1 \in \mathrm{Sat}(\phi)$). Symmetrically, we have that $m_2 \neq (0 \cdots 0)$, $m_2 \neq (1 \cdots 1)$, and there exists a variable $y \in \mathcal{V}ar(\phi)$ such that $m_2(y) = 1$ and $m_2(y) = 0$.

Construct a new formula $\psi = \phi[0/V_0, x/V_x, y/V_y]$ where $V_0 = \{v \in \mathcal{V}ar(\phi) \mid m_1(v) = 0 \wedge m_2(v) = 0\}$, $V_x = \{v \in \mathcal{V}ar(\phi) \mid m_1(v) = 1\}$, and $V_y = \{v \in \mathcal{V}ar(\phi) \mid m_1(v) = 0 \wedge m_2(v) = 1\}$. The sets V_x and V_y are nonempty, hence the formula ψ contains both variables x and y. It is clear that V_0, V_x, and V_y are disjoint and $V_0 \cup V_x \cup V_y = \mathcal{V}ar(\phi)$. Clearly, $[\psi] \in \mathcal{R}ep_0(\{R\})$. The relation $[\psi]$ contains 01 and 10 but it does not contain 00. Hence, the relation $[\psi]$ is either $[\psi] = \{01, 10\} = [x \not\equiv y]$ or $[\psi] = \{01, 10, 11\} = [x \vee y]$, depending on whether $[\psi]$ contains 11 or not. □

Corollary 5. *If S contains some relation which is not Horn and some relation which is not anti-Horn then $\mathcal{R}ep_b(S)$ contains the relation $[x \not\equiv y]$.*

Proof. Let $R_1 \in S$ be a non-Horn relation. Then $\mathcal{R}ep_b(\{R_1\}) \cap \{[x \not\equiv y], [x \vee y]\} \neq \emptyset$ following Lemma 4. Let $R_2 \in S$ be a non anti-Horn relation. Similarly, $\mathcal{R}ep_b(\{R_2\}) \cap \{[x \not\equiv y], [\bar{x} \vee \bar{y}]\} \neq \emptyset$.

Assume that $[x \not\equiv y] \notin \mathcal{R}ep_b(S)$ holds. Then both relations $[x \vee y]$ and $[\bar{x} \vee \bar{y}]$ are included in $\mathcal{R}ep_b(S)$. Therefore $\mathcal{R}ep_b(S)$ contains also the relation $[(x \vee y) \wedge (\bar{x} \vee \bar{y})] = [x \not\equiv y]$, contradiction. Hence $\mathcal{R}ep_b(S)$ contains $[x \not\equiv y]$. □

Lemma 6 (Negated Substitution). *Let the relation $[x \not\equiv y]$ be included in $\mathcal{R}ep_b(S)$. If a formula ϕ belongs to $\mathcal{G}en_b(S)$ and u, v are variables, then the formula $\phi[\bar{u}/v]$ is contained in the set $\mathcal{G}en_b(S)$, too.*

Proof. By assumption, there exists a formula in $\mathcal{G}en_b(S)$ logically equivalent to $x \not\equiv y$, therefore we can construct the formula $\phi[u'/v] \wedge (u' \not\equiv u)$. The formulas $\phi[\bar{u}/v]$ and $\phi[u'/v] \wedge (u' \not\equiv u)$ are quasi-equivalent, when u' is a new variable not occurring in ϕ. □

Lemma 7 ([CH96]). *Let R be a non-affine relation. Then $\mathcal{R}ep(\{R, [x \not\equiv y]\})$ contains the relations $[x \vee y]$, $[\bar{x} \vee y]$, $[x \vee \bar{y}]$, and $[\bar{x} \vee \bar{y}]$.*

Let R be a b-valid and non-affine relation. Then the set $\mathcal{R}ep_b(\{R\})$ contains the relations $[x \vee y]$, $[\bar{x} \vee y]$, $[x \vee \bar{y}]$, and $[\bar{x} \vee \bar{y}]$.

Recall that the relation 1-in-3 is the logical relation $\{001, 010, 100\}$.

Lemma 8. *Let R be a non-2SAT relation. Then $\mathcal{R}ep_b(\{R, [x \not\equiv y], [x \vee y]\})$ contains the relation* 1-in-3*.*

Proof. We do the proof only for $b = 0$, the proof for $b = 1$ is similar.

Let R be a non-2SAT logical relation and let $\phi = R(\mathbf{v})$ be the corresponding formula. Following Proposition 3, there exist three models $m_1, m_2, m_3 \in \mathrm{Sat}(\phi)$ such that $(m_1 \vee m_2) \wedge (m_2 \vee m_3) \wedge (m_3 \vee m_1) \notin \mathrm{Sat}(\phi)$. Let ϕ' be a formula constructed from ϕ by replacing each variable $x \in \mathcal{V}ar(\phi)$, such that $m_1(x) = 1$ holds, by its negation $\bar{x}$. From the Negated Substitution Lemma follows that $\phi' \in \mathcal{G}en(\{R, [x \not\equiv y]\})$. Let m'_2 and m'_3 be models of ϕ' corresponding to the models m_2 and m_3 of ϕ. For each $i = 2, 3$, if $m_1(x) = 0$ then $m'_i(x) = m_i(x)$ else $m'_i(x) = \bar{m}_i(x)$.

Let V_0, V_x, V_y, and V_z be the following sets of variables: $V_0 = \{v \in \mathcal{V}ar(\phi') \mid m'_2(v) = 0 \wedge m'_3(v) = 0\}$, $V_x = \{v \in \mathcal{V}ar(\phi') \mid m'_2(v) = 1 \wedge m'_3(v) = 1\}$, $V_y = \{v \in \mathcal{V}ar(\phi') \mid m'_2(v) = 0 \wedge m'_3(v) = 1\}$, and $V_z = \{v \in \mathcal{V}ar(\phi') \mid m'_2(v) = 1 \wedge m'_3(v) = 0\}$. Construct the formula $\psi = \phi'[0/V_0, x/V_x, y/V_y, z/V_z]$.

Note that the sets V_x, V_y, and V_z are nonempty. Therefore $[\psi]$ contains the models 000, 101, and 110, but it does not contain 100 since the original relation R is not 2SAT. Construct the formula $\omega = \psi[\bar{x}/x] \wedge (\bar{x} \vee \bar{y}) \wedge (\bar{y} \vee \bar{z}) \wedge (\bar{z} \vee \bar{x})$. From Negated Substitution Lemma follows that $\omega \in \mathcal{G}en_0(\{R, [x \not\equiv y], [x \vee y]\})$ and that $[\omega] = \{011, 010, 100\}$, i.e., $[\omega]$ is the relation 1-in-3. □

Lemma 9. *$\mathcal{R}ep_b(\{$1-in-3$\})$ is the set of all logical relations, for each $b \in \{0, 1\}$.*

Proof. Let $R(x, y, z)$ be the formula corresponding to the relation 1-in-3. Let $\phi_0 = R(x, u_1, u_4) \wedge R(y, u_2, u_4) \wedge R(u_1, u_2, u_5) \wedge R(u_3, u_4, u_6) \wedge R(z, u_3, 0)$, $\phi_1 = R(x, u_1, u_4) \wedge R(y, u_2, u_4) \wedge R(u_1, u_2, u_5) \wedge R(u_3, u_4, u_6) \wedge R(z, u_3, u_7) \wedge R(u_7, u_8, 1)$, $\psi_0 = R(x, y, 0)$, and $\psi_1 = R(x, y, u_1) \wedge R(u_1, u_2, 1)$. It is easy to verify that the formulas ϕ_0 and ϕ_1 are quasi-equivalent to $x \vee y \vee z$, and similarly that the formulas ψ_0 and ψ_1 are quasi-equivalent to $x \not\equiv y$.

There exists a parsimonious reductions from the satisfiability problem SAT of a propositional formula in conjunctive normal form to the satisfiability problem 3SAT of a propositional formula in conjunctive normal form with 3 literals per clause (see, e.g. [Koz92]). Hence, for each SAT formula ϕ there exists a quasi-equivalent 3-cnf formula ϕ'. Now, for each $i = 0, 1$, the formulas ϕ_i and ψ_i, using also the Negated Substitution Lemma, allow us to convert the 3-cnf formula ϕ' to a quasi-equivalent formula in $\mathcal{G}en_i(\{R\})$. Therefore, for every propositional formula ϕ we have that $[\phi] \in \mathcal{R}ep_i(\{R\})$, i.e., that $\mathcal{R}ep_i(\{R\})$ is the set of all logical relations. □

We are now able to prove Proposition 2. The proof is essentially the same as of Theorem 3.0 in [Sch78].

Proof. We focus only on the case when S does not satisfy any of the conditions (3) to (6) of Theorem 1. The other cases are clear.

If S does not satisfy any of the conditions (3) to (6) then S contains a relation R_1 which is not Horn, a relation R_2 which is not anti-Horn, a relation R_3 which is not affine, and a relation R_4 which is not 2SAT. Corollary 5 implies that $[x \not\equiv y] \in \mathcal{R}ep_b(\{R_1, R_2\})$. From Lemma 7 follows that $[x \vee y] \in \mathcal{R}ep_b(\{R_1, R_2, R_3\})$. From Lemma 8 follows that the set $\mathcal{R}ep_b(\{R_1, R_2, R_3, R_4\})$ contains the relation 1-in-3. Therefore, by Lemma 9, $\mathcal{R}ep_b(\{R_1, R_2, R_3, R_4\})$ is the set of all logical relations. Hence, also $\mathcal{R}ep_b(S)$ is the set of all relations. □

Theorem 10. *Let S be a finite set of logical relations. If S satisfies one of the conditions (3) to (6) of Theorem 1 then* UNIQUE SAT$_c(S)$ *and* ANOTHER SAT$_c(S)$ *are polynomial-time solvable. Otherwise,* ANOTHER SAT$_c(S)$ *is* ***NP****-complete and* UNIQUE SAT$_c(S)$ *is* ***coNP****-hard.*

Proof. If every relation in S is Horn then every S-formula is a Horn propositional formula. To compute a model of a Horn formula in polynomial time, apply exhaustively the unit resolution, followed by setting the unresolved variable to 0 (see [DG84] for details). Dually, if every relation in S is anti-Horn then we compute a model of such S-formula in polynomial time by exhaustive unit resolution, followed by setting the unresolved variables to 1. If every relation in S is affine then such S-formula is equivalent to a system of linear equations over the ring $\mathbb{Z}_2$. Its solution can be found by Gauss' elimination in polynomial time. If every relation in S is 2SAT then a model of such S-formula can be found in polynomial time by the Davis-Putnam procedure.

Let $\phi(x_1, \ldots, x_n)$ be an S-formula. If S satisfies one of the polynomial conditions, we compute a model m of ϕ in the case of UNIQUE SAT in polynomial time by one of the previous methods. In the case of ANOTHER SAT the model m is already given. We can decide whether there is another model by the following polynomial-time algorithm:

$i \leftarrow 0$; *another* $\leftarrow$ *false*;
while $\neg$*another* $\wedge$ $(i < n)$ **do** $i \leftarrow i + 1$; *another* $\leftarrow$ $sat(\phi[\bar{m}(x_i)/x_i])$ **od**

The call $sat(\phi[\bar{m}(x_i)/x_i])$ means that we instantiate in the formula ϕ the variable x_i by the dual value of $m(x_i)$ and test whether this instance is satisfiable. The satisfiability of $\phi[\bar{m}(x_i)/x_i]$ can be computed in polynomial time since S satisfies one of the polynomial conditions. If *another* = *false* (there are no other models) then return *false* in the case of ANOTHER SAT and *true* for UNIQUE SAT. Otherwise, return *true* for ANOTHER SAT and *false* for UNIQUE SAT.

If S does not satisfy any of the polynomial conditions then we show that there exists a parsimonious reduction from UNIQUE 3SAT to UNIQUE SAT$_c(S)$, and from ANOTHER 3SAT to ANOTHER SAT$_c(S)$. Indeed, consider the relations $R_0 = [x \vee y \vee z]$, $R_1 = [\bar{x} \vee y \vee z]$, $R_2 = [\bar{x} \vee \bar{y} \vee z]$, and $R_3 = [\bar{x} \vee \bar{y} \vee \bar{z}]$. Let $\phi_i(x, y, z)$ be a formula in $\mathcal{G}en_b(S)$ quasi-equivalent to $R_i(x, y, z)$, for $i = 0, 1, 2, 3$. Such formulas exist by Proposition 2. Let ψ be a 3-cnf formula. Construct the formula ψ' by replacing each clause of ψ by a corresponding formula ϕ_i. This reduction is parsimonious.

For proving both lower bounds, we use the same construction as in [BG82]. Let $\alpha(x_1, \ldots x_n)$ be a 3-cnf formula. Construct the formula $\beta(x_0, x_1, \ldots x_n) = (x_0 \wedge x_1 \wedge \cdots \wedge x_n) \vee (\bar{x}_0 \wedge \alpha(x_1, \ldots, x_n))$. Transform β to conjunctive normal form (there is no exponential blow-up in this case), getting a 4-cnf formula. Transform β to a quasi-equivalent 3-cnf formula β' (see [Koz92]). It is clear that β has a unique model, namely $1 \cdots 1$, iff the formula α is unsatisfiable. If α represents an instance of UNSAT, the problem of unsatisfiability of a propositional 3-cnf formula that is **coNP**-complete, then this reduction proves the **coNP**-hardness of UNIQUE SAT$_c(S)$. If α represents an instance of 3SAT, the satisfiability problem of a propositional 3-cnf formula that is **NP**-complete, then this reduction proves the **NP**-hardness of ANOTHER SAT$_c(S)$. To prove membership of ANOTHER SAT$_c(S)$ in **NP**, guess an assignment m' different from m and check in polynomial time if m' satisfies the formula ϕ. □

Lemma 11 ([CH96]). *Let S be a nonempty finite set of logical relations. At least one of the following conditions holds:* (1) *Every relation in S is 0-valid.* (2) *Every relation in S is 1-valid.* (3) *$\mathcal{R}ep_{nc}(S)$ contains the relation $[\bar{x} \wedge y]$.* (4) *$\mathcal{R}ep_{nc}(S)$ contains the relation $[x \not\equiv y]$.*

Moreover, if $[\bar{x} \wedge y] \notin \mathcal{R}ep_{nc}(S)$ and $[x \not\equiv y] \in \mathcal{R}ep_{nc}(S)$ hold then every relation in S is complementive.

Proposition 12. *Let S be a finite set of logical relations. If the relations in S are neither all 0-valid, nor all 1-valid, nor all complementive, then there exists a parsimonious reduction from* UNIQUE SAT$_c(S)$ *to* UNIQUE SAT(S) *and from* ANOTHER SAT$_c(S)$ *to* ANOTHER SAT(S).

Proof. If the relations in S are neither all 0-valid, nor all 1-valid, nor all complementive, then $[\bar{x} \wedge y] \in \mathcal{R}ep_{nc}(S)$ or $[x \not\equiv y] \notin \mathcal{R}ep_{nc}(S)$ holds following Lemma 11. If $[\bar{x} \wedge y] \in \mathcal{R}ep_{nc}(S)$ holds then the proof is the same as in case 1 of Proposition 4.12 in [CH96]. If we have $[\bar{x} \wedge y] \notin \mathcal{R}ep_{nc}(S)$ then the relation $[x \not\equiv y]$ is contained in $\mathcal{R}ep_{nc}(S)$ following the first part of Lemma 11. But we have that $[x \not\equiv y] \notin \mathcal{R}ep_{nc}(S)$ since S contains a relation that is not complementive, following the second part of Lemma 11: contradiction. Hence $\mathcal{R}ep_{nc}(S)$ must contain the relation $[\bar{x} \wedge y]$. □

We have assembled now all the necessary tools to prove Theorem 1.

Proof. If every relation in S is 0-valid and 1-valid then every S-formula without constants has at least two models: $0 \cdots 0$ and $1 \cdots 1$. Hence, the solution of this instance for UNIQUE SAT and ANOTHER SAT is trivial.

Let every relation in S be complementive and let ϕ be an S-formula without constants. Following the definition of a complementive relation, if m is a model of ϕ then also its dual $\bar{m}$ is a model of ϕ. Hence, for this case UNIQUE SAT is alway false and ANOTHER SAT is always true. The rest of the polynomial cases is decided by the same algorithm as in Theorem 10.

Assume that S does not satisfy any of the polynomial conditions (1) to (6), i.e., that S contains a relation that is not both 0-valid and 1-valid, a relation

that is not complementive, a relation R_1 that is not Horn, a relation R_2 that is not anti-Horn, a relation R_3 that is not affine, and a relation R_4 that is not 2SAT. There are two cases to analyse.

Case 1: If S contains a relation which is not 0-valid and a relation which is not 1-valid, then there exists a parsimonious reduction from UNIQUE SAT$_c(S)$ to UNIQUE SAT(S) and from ANOTHER SAT$_c(S)$ to ANOTHER SAT(S) following Proposition 12. Since UNIQUE SAT$_c(S)$ is **coNP**-hard and ANOTHER SAT$_c(S)$ is **NP**-complete following Theorem 10, this proves that UNIQUE SAT(S) is **coNP**-hard and ANOTHER SAT(S) is **NP**-hard.

Case 2: If every relation in S is either 0-valid or 1-valid, but not both, and not complementive, then we have that $[x \not\equiv y] \in \mathcal{R}ep_b(\{R_1, R_2\})$ following Corollary 5, $[x \vee y] \in \mathcal{R}ep_b(\{R_3\})$ following Lemma 7, and the set $\mathcal{R}ep_b(\{R_1, R_2, R_3, R_4\})$ contains the logical relation 1-in-3 following Lemma 8. Let $R(x, y, z)$ be the formula representing the relation 1-in-3. If there exists a formula ϕ containing the Boolean constant b, construct the formula ϕ' by replacing the constant b by a new variable x_b. Create a new formula ψ as follows. If $b = 0$ then let $\psi = \phi' \wedge R(x_b, x_b, u)$, otherwise if $b = 1$ then let $\psi = \phi' \wedge R(x_b, u, u)$, where u is a new variable. It is clear that the formulas ϕ and ψ are quasi-equivalent. Hence, there exists a parsimonious reduction from UNIQUE SAT$_c(S)$ to UNIQUE SAT(S) and from ANOTHER SAT$_c(S)$ to ANOTHER SAT(S).

In both cases, since UNIQUE SAT$_c(S)$ is **coNP**-hard and ANOTHER SAT$_c(S)$ is **NP**-complete following Theorem 10, this proves that UNIQUE SAT(S) is **coNP**-hard and ANOTHER SAT(S) is **NP**-hard. Membership of ANOTHER SAT(S) in **NP** is proved as in Theorem 10, hence ANOTHER SAT(S) is **NP**-complete. □

4 Concluding remarks

The main result of the paper is a Dichotomy Theorem for the UNIQUE SAT and ANOTHER SAT problems (Theorem 1), showing that every instance of both problems is either polynomially solvable or it is **coNP**-hard, respectively **NP**-complete. We noticed that both considered problems have the same polynomial-time solvable instances. Moreover, we showed that the additional knowledge of the existence of a model pushes the problem UNIQUE SAT from the difference class **DP** down to **coNP**, making it **coNP**-complete. Compare it with the result in [VV86] that UNIQUE SAT is **DP**-complete under randomized reductions.

We also proved Minoux's claim (see [Min92]) that the SAT and UNIQUE SAT problems have the same polynomially solvable instances in the presence of propositional formulas with Boolean constants (Theorem 10). On the other hand, if we consider formulas without constants, the polynomially solvable instances of SAT and UNIQUE SAT are incomparable. There are polynomially solvable SAT instances with corresponding **coNP**-complete UNIQUE SAT instances (0-valid or 1-valid), whereas there are **NP**-complete SAT instances with corresponding polynomially solvable UNIQUE SAT instances (complementive). Among the latter we find the problem NOT-ALL-EQUAL SAT for which the satisfiability is **NP**-complete, but which has never a unique model.

References

[BFS95] K.A. Berman, J. Franco, and J.S. Schlipf. Unique satisfiability of Horn sets can be solved in nearly linear time. *Discrete Appl. Math.*, 60(1-3):77–91, 1995.

[BG82] A. Blass and Y. Gurevich. On the unique satisfiability problem. *Information and Control*, 55:80–88, 1982.

[CH96] N. Creignou and M. Hermann. Complexity of generalized satisfiability counting problems. *Information and Computation*, 125(1):1–12, 1996.

[CKR95] R. Chang, J. Kadin, and P. Rohatgi. On unique satisfiability and the threshold behavior of randomized reductions. *Journal of Computer and System Science*, 50(3):359–373, 1995.

[DG84] W.F. Dowling and J.H. Gallier. Linear-time algorithms for testing the satisfiability of propositional Horn formulae. *Journal of Logic Programming*, 1(3):267–284, 1984.

[GJ79] M.R. Garey and D.S. Johnson. *Computers and intractability: A guide to the theory of NP-completeness.* W.H. Freeman and Co, 1979.

[HJ85] P. Hansen and B. Jaumard. Uniquely solvable quadratic Boolean equations. *Discrete Appl. Math.*, 12(2):147–154, 1985.

[Koz92] D.C. Kozen. *The design and analysis of algorithms*, chapter 26: Counting problems and #P, pages 138–143. Springer-Verlag, 1992.

[Min92] M. Minoux. The unique Horn-satisfiability problem and quadratic Boolean equations. *Ann. of Math. and Artificial Intelligence*, 6(1-3):253–266, 1992.

[Pap94] C.H. Papadimitriou. *Computational complexity.* Addison-Wesley, 1994.

[Pre93] D. Pretolani. A linear time algorithm for unique Horn satisfiability. *Information Processing Letters*, 48(2):61–66, 1993.

[Sch78] T.J. Schaefer. The complexity of satisfiability problems. In *Proc. 10th STOC, San Diego (CA, USA)*, pages 216–226, 1978.

[VV86] L.G. Valiant and V.V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85–93, 1986.