Simple Sentences That Are Hard to Decide

ERICH GRÄDEL*

Mathematisches Institut, Universität Basel,
Rheinsprung 21, CH-4051 Basel, Switzerland

It was considered to be "typical for first order theories" that a restriction to sentences with only a limited number of quantifier alternations leads to an exponential decrease of complexity. Using domino games, which were treated in a previous paper to describe computations of alternating Turing machines, we prove that this is not always true. We present a list of theories, all of them decidable in \( \bigcup_{k \geq 0} \text{ATIME}(2^k, n) \), for which the subclasses with bounded quantifier alternations still have alternating exponential time complexity. In particular, this yields nondeterministic exponential time lower bounds for very simple prefix classes (with 2 or 3 alternations). Theories with such behaviour are the theory of Boolean algebras, the theory of polynomial rings over finite fields, the theory of idempotent rings, the theory of finite sets with inclusion, the theory of semilattices, the theory of Stone algebras, the theory of distributive \( p \)-algebras in the Lee-class \( B_p \), and the theories of natural numbers with divisibility or coprimeness.

1. INTRODUCTION

In the last twenty years a lot of research has investigated the complexity of the decision problem of mathematical theories (see Compton and Henson (1990) for a survey and a uniform treatment). Among decidable theories we can roughly distinguish three classes:

1. The simplest theories are the PSPACE-complete theories. It follows from a result of Stockmeyer (1977) that every theory which has a model with a nontrivial relation (e.g., equality) is hard for PSPACE. However, only very simple theories such as, e.g., the first order theory of equality, the theories of natural or rational numbers with order, etc., are known to be in PSPACE.

2. The most complicated decidable theories are not elementary recursive, i.e., they are not decidable in \( \text{NTIME}(\exp_k(n)) \) for any fixed \( k \). (The function \( \exp_k(n) \) is the \( k \)-fold iterated exponential function with base 2.) Examples of not elementary recursive theories are the theory of finite trees,

* This work was done while the author was staying at the University of Pisa, Italy and was supported by the Swiss National Science Foundation.
the theory of one unary function, the theory of linear orders, the theory of any pairing function, and the theory of natural numbers with addition and exponentiation.

(3) Most decidable theories are complete in some complexity class \( \bigcup_{c > 0} \text{ATIME}(\exp(cn), cn) \) or, in some cases, in \( \bigcup_{c > 0} \text{NTIME}(\exp(cn)) \). Well known examples are the theory of real addition, the theory of Boolean algebras \((k = 1)\), Presburger arithmetic, the theory of finite Abelian groups \((k = 2)\) and Skolem arithmetic \((k = 3)\).

In the sequel we concentrate on theories of the third class. The huge complexity bounds of these theories suggested the consideration of syntactically defined fragments of these theories; e.g., of the class of sentences with a given quantifier prefix. This is related to the problem of classifying prefix classes in first order logic with respect to decidability and complexity (special cases of Hilbert’s “Entscheidungsproblem,” see Börger (1984) for a survey) and is also justified by the observation that decision problems occurring in mathematical practice are usually formulated by formulae of quite simple structure. The investigations done in this area (see, for example, Reddy and Loveland (1978), Fürer (1982), Scarpellini (1984), Sontag (1985), and Graedel (1989)) showed, among other results, that in many theories the subclasses with bounded numbers of quantifier alternations have complexity that is one exponential step lower than the complexity of the whole theory. This was considered to be the “typical behaviour of first order theories” (see Fürer (1982)). To make more precise statements we have to introduce some notation:

**Definition.** For \( m \geq 1 \) a formula in prenex normal form is called a \( \Sigma_m \)-formula or a \( \Pi_m \)-formula if its quantifier prefix has at most \( m \) quantifier alternations with leading quantifier \( \exists \) or \( \forall \), respectively. For any theory \( \text{Th} \), \( \Sigma_m \cap \text{Th} \) denotes the set of \( \Sigma_m \)-sentences in \( \text{Th} \). Similarly, for a word \( Q_1, \ldots, Q_s \) over the alphabet \( \{\exists, \forall, \exists^*, \forall^*\} \), \([Q_1, \ldots, Q_s] \cap \text{Th} \) is the set of sentences in \( \text{Th} \) whose quantifier prefix is a subword of \( Q_1, \ldots, Q_s \).

For theories in \( \bigcup_{c > 0} \text{ATIME}(2^{cn}, n) \) the “typical behaviour” means that subclasses defined in such a way are contained in some level of the polynomial time hierarchy. Note that the class of \( \Sigma_m \)-sentences in any non-trivial theory is \( \Sigma_{m+1} \)-hard; this follows immediately from the arguments of Stockmeyer (1977). For the theory of real addition \( \text{RA} = \text{Th}(\mathbb{R}; +, \leq) \) we actually have completeness:

**Theorem 1.1** (Sontag 1985). For all \( m \geq 1 \)

\[
\Sigma_m \cap \text{RA} \text{ is } \Sigma_{m+1} \text{-complete}
\]

\[
\Pi_m \cap \text{RA} \text{ is } \Pi_{m+1} \text{-complete}.
\]
In this paper we present a list of counterexamples to this pattern: we prove that there are quite a number of mathematical theories, all of them contained in $\bigcup_{c > 0} \text{ATIME}(2^c n, n)$, for which the subclasses with bounded quantifier alternations still have exponential complexity. The most important of these examples is the theory of Boolean algebras proved to be $\bigcup_{c > 0} \text{ATIME}(2^c n, n)$-complete by Kozen (1980). Let $\text{sat}(\text{BA})$ be the set of sentences in the language of Boolean algebras which are true in some Boolean algebra. We will show

**Theorem 1.2.** There is a constant $c > 0$ such that for all $m \geq 1$

$$\Sigma_{m+1} \cap \text{sat}(\text{BA}) \notin \text{ATIME}(2^{cn/m}, m).$$

We will actually prove a slightly stronger result, namely that no set in $\text{ATIME}(2^{cn/m}, m)$ separates $\Sigma_{m+1} \cap \text{sat}(\text{BA})$ from the logically invalid sentences.

**Remark.** Here, as for all other theories treated in this paper and as in the paper of Kozen, it is assumed that we have an unlimited supply of variable symbols of length one.

Similar results will be shown for the theories of

1. polynomial rings over a finite field;
2. idempotent rings;
3. finite sets with inclusion;
4. natural numbers with divisibility;
5. natural numbers with coprimeness;
6. semilattices with 0;
7. Stone algebras;
8. distributive $p$-algebras in the Lee-class $\mathcal{B}_n$.

We prove these results by reductions from domino games—a generalization of the well known domino (tiling) problems—and by a methodology for interpretations which adapts widely used reduction techniques to the problems considered here. Domino games were introduced by Chlebus (1986) and, in the form used in this paper, by the author. Actually this paper contains the applications of the theoretical framework and the results in Grädel (1990). The necessary definitions and theorems on domino games are cited in Section 2. In Section 3 we show that simple formulae in the theory of polynomial rings over the field $\mathbb{F}_2$ encode the strategy problem for domino games on a playboard of exponential size. This will prove a variant of Theorem 1.2 for this theory. In Section 4 this lower bound is strengthened to an inseparability result. In Section 5 we describe the inter-
pretation method which is used in Section 6 to prove the results for the other theories.

**Remark.** The result for the theory of Boolean algebras was presented in preliminary form at the Symposium on Theoretical Aspects of Computer Science STACS 88, held in February 1988 in Bordeaux, France (see Grädel, 1988).

2. **DOMINO GAMES**

The classical domino problem, as introduced by Wang (1961), may be formulated as follows: Let $S$ be $\mathbb{N} \times \mathbb{N}$ or a finite square $\{0, \ldots, t\} \times \{0, \ldots, t\}$.

**Instance.** $\mathcal{D}$ consisting of a finite set $D$ and binary relations $H, V \subseteq D \times D$.

**Question.** Is there a tiling $\tau : S \rightarrow D$ such that for all $(x, y) \in S$

\[
\tau(x, y) = d_i \wedge \tau(x + 1, y) = d_j \Rightarrow (d_i, d_j) \in H
\]

\[
\tau(x, y) = d_i \wedge \tau(x, y + 1) = d_j \Rightarrow (d_i, d_j) \in V.
\]

A variant of this problem which is particularly convenient for the encoding of Turing machine computations is the origin constrained domino problem. We are given $\mathcal{D} = (D, D_0, H, V)$ where $D, H,$ and $V$ are as above, $D_0$ is a subset of $D$, and it is asked whether there is a tiling which places a tile from $D_0$ on the point $(0, 0)$.

For $S = \mathbb{N} \times \mathbb{N}$ both problems are undecidable (see Wang 1961, Berger 1966).

In Chlebus (1986) and Grädel (1988, 1990) this is generalized to the notion of domino games which describe computations of alternating Turing machines in the same way as domino-tilings encode the computations of deterministic and nondeterministic Turing machines. Thus domino games provide a convenient tool for proving lower bounds for ATIME-complexity classes. In this section we cite the definitions and results of Grädel (1990) that will be needed later.

We assume in the sequel that Turing machines and domino systems are encoded in a suitable way as strings over a finite alphabet and we identify them with their encodings. $S_t$ denotes the square $\{0, \ldots, t\} \times \{0, \ldots, t\}$.

**Definition.** A domino game $\langle \mathcal{D}, t \rangle$ is given by a domino system $\mathcal{D} = (D, D_0, H, V)$, where $D$ is the disjoint union of two subsets $E$ and $A$ and $D_0$ is a subset of either $E$ or $A$; tiles from $E$ and $A$ are called existential
and universal tiles, respectively; \( t \) is a natural number specifying the size of the playboard.

The game is played by two persons, \( \exists \) and \( \forall \), also referred to as the constructor and the saboteur. The constructor tries to build a tiling of the square \( S_t \); the saboteur wants to prevent him from achieving this goal. In the course of the game the players tile \( S_t \), row after row, according to the following rules:

1. Odd rows and tiled from the left to the right and even rows from the right to the left; so the game proceeds like a meander through \( S_t \).
2. The adjacency conditions imposed by \( H \) and \( V \) must be satisfied. If no player can place a next tile, the saboteur immediately wins.
3. The constructor (\( \exists \)) uses the tiles from \( E \), the saboteur (\( \forall \)) the tiles from \( A \). A player moves—and has to move—until he cannot place a next tile. Then the other player begins to move. Thus, whether \( D_o \) is contained in \( E \) or in \( A \) determines which player has the first move.
4. If \( S_t \) is entirely tiled, the constructor wins.

A move in \( < \Omega, t > \) means the placing of a whole sequence of tiles between two changes of players (not the placing of a single tile).

**Definition.** Let \( \text{GAME}(t, m) \) denote the set of all dominoes \( \Omega \) such that the constructor has a strategy to win the game \( < \Omega, t > \) in at most \( m \) moves; \( t \) may be a function of \( |\Omega| \).

**Theorem 2.1.** Let \( M \) be an alternating Turing machine, \( T(n) \) a time constructible function. There is a polynomial reduction taking every input \( x = x_0, \ldots, x_{n-1} \) to a domino system \( \Omega_x \) with \( O(\sqrt{n}) \) tiles (which can therefore be encoded by a string of length \( O(n) \)) such that for all \( m \):

\[
M \text{ accepts } x \text{ in time } T(n) - 2 \text{ and with } m \text{ alternations } \iff \Omega_x \in \text{GAME}(T(n), m).
\]

**Corollary 2.2.** If \( T(n) \) is a time constructible function such that \( T(dn) = o(T(n)) \) for some \( d > 0 \), then there is positive constant \( c \) such that

\[
\text{GAME}(T(n), m) \notin \text{ATIME}(T(cn), m).
\]

Theorem 2.1 and Corollary 2.2 are proved in Grädel (1990).

**3. Polynomial Rings over Finite Fields**

**Definition.** Let \( F \) be a fixed finite field \( F_q \). The theory \( \text{sat}(F[X]) \) is the set of sentences in the language of a ring, with constants \( 0, 1, \ldots, q - 1 \) and
X_1, X_2, ..., which, for some n \in \mathbb{N}, are true when interpreted in the ring of multivariate polynomials over F which n indeterminates. We do not distinguish between polynomials which are equal when considered as functions from F^n to F—so we actually work in the ring F[X_1, ..., X_n]/(X_1^q - X_1) \cdots (X_n^q - X_n). Note that 0, 1, ..., q - 1 represent constant functions (not field elements!) and that X_i stands for the projection to the i-th coordinate (not for a variable!).

We will prove in Section 6 that sat(F[X]) can be decided in alternating exponential time since is interpretable in the theory of Boolean algebras. Here we consider the field F_2 and show that the subclasses with bounded quantifier alternations still have exponential lower complexity bounds.

**Theorem 3.1.** There is a positive constant c such that for all natural numbers m \geq 1

\[ [m + 1 \text{ Alternations}] \cap \text{sat}(F_2[X]) \not\in \text{ATIME}(2^{cm/m}, m). \]

**Proof.** We show that GAME(2^n, m) is poly-lin reducible to [m + 1 Alternations] \cap sat(F_2[X]); i.e., that given a domino system D, we can construct in polynomial time a sentence \psi_\delta of length O(|D|) with m + 1 quantifier alternations which is satisfiable iff the constructor has a forced win in m moves for the game \langle D, 2^n \rangle, i.e., the game defined by D on the square S = \{0, ..., 2^n - 1\} x \{0, ..., 2^n - 1\}. By Corollary 2.2 the theorem will follow. Recall from Theorem 2.1 that we may assume that D contains O(\sqrt{n}) tiles. For simplicity of exposition (but without loss of generality) we make the assumptions that changes of players occur only in odd rows (i.e., in rows that are tiled from left to right) and that no change happens in the first row. Thus a change of players, say from the constructor to the saboteur, occurs in the following situation: Points (a - 1, b) and (a, b - 1) are tiled by d, d', such that d \in E and for all dominoes d''

\[(d, d'') \in H \land (d', d'') \in V \implies d'' \in A.\]

(An analogous condition holds for a change from the saboteur to the constructor.) We say that such a pair (d, d') is a terminating pair.

Let D be a domino system (D, D_0, H, V) with D = E \cup A and let T be the set of terminating pairs in D. Furthermore, suppose that D_0 \subseteq E, i.e., that the constructor has the first move and that m is odd (i.e., the constructor also has the last move). The other cases are treated similarly.

1. Using binary representations the square S can be identified with F_2^n x F_2^n. Furthermore there is a natural identification of a polynomial with the set of points at which it evaluates to 1. Inclusion of f in g is described
by the formula $fg = f$ and abbreviated $f \leq g$. A projection $X_i$ corresponds to the set of those points for which the $i$th digit in the binary representation is 1.

Let the set of dominoes be $D = \{d_1, \ldots, d_r\}$. We describe a move of either player by an $(r + 1)$-tuple $(t, u) = (t_1, \ldots, t_r, u)$ of polynomials over $F^2$ in the variables $X_1, \ldots, X_n$, $Y_1, \ldots, Y_n$, i.e., by a sequence of functions from $F_2^n \times F_2^n$ to $F_2$ such that $t_j(a, b) = 1$ for exactly those points $(a, b)$ which are tiled by $d_j$ after the move and $u(a, b) = 1$ for the points that are left untiled. We will construct formulae which express that $(t, u)$ encodes a correct move in the game. First we build a formula $\text{MOVE}(t, u)$ which says that $(t, u)$ satisfy the following three conditions:

(i) Each point is mapped to 1 by exactly one of the polynomials $t_1, \ldots, t_r, u$;
(ii) The relations $D_0, H,$ and $V$ of the domino system are satisfied by $t_1, \ldots, t_r$;
(iii) The move is correctly terminated.

2. The first condition is expressed by the formula

$$A(t, u) \equiv \bigwedge_{i \neq j} (t_it_j = 0) \land \bigwedge_i (t_iu = 0) \land \left(u + \sum_{i=1}^r t_i = 1\right)$$

Note that $|A(t, u)| = O(n)$ since $r = O(\sqrt{n})$.

3. A polynomial $f$ corresponds to a single point if it maps precisely one element of $F_2^n \times F_2^n$ to 1; this is expressed by the formula

$$B(f) = (f \neq 0) \land \bigwedge_{i=1}^n (f \leq X_i \lor fX_i = 0) \land (f \leq Y_i \lor fY_i = 0).$$

Suppose that we have two polynomials $f, g$ interpreting points $(a, b)$ and $(a', b') \in S$. In order to describe tilings we need formulae $H(f, g)$ and $V(f, g)$ expressing that $f$ and $g$ are horizontally resp. vertically adjacent. Thus $H(f, g)$ must assure that $a' = a + 1$ and $b' = b$. But $a' = a + 1$ means that for some $i \leq n$, $a$ and $a'$ have binary representations $a_na_{n-1} \cdots a_{i+1}01\cdots1$ and $a_na_{n-1} \cdots a_{i+1}10\cdots0$, respectively. With regard to the fact that the $k$th digit in the binary representation of $a$ is 1 if $f \leq X_k$ and 0 if $fX_k = 0$ we can express $(a' = a + 1)$ by the formula

$$\bigwedge_{i=1}^n \left\{ \bigwedge_{j>i} (f \leq X_j \leftrightarrow g \leq X_j) \land (fX_i = 0 \land g \leq X_i) \land \bigwedge_{j<i} (f \leq X_j \land gX_j = 0) \right\}.$$
Unfortunately the displayed formula has length \(O(n^2)\). To overcome this problem we replace it with the equivalent formula

\[
\text{SUCC}_x(f, g) \equiv \exists h \left\{ F(f, h) \land \bigwedge_{i=1}^{n} \left[ (X_i \leq h \rightarrow (f \leq X_i \leftrightarrow gX_i = 0)) \right] \land (X_i \not\leq h \rightarrow (f \leq X_i \leftrightarrow g \leq X_i)) \right\}
\]

with

\[
F(f, h) \equiv X_1 \leq h \land \bigwedge_{i=2}^{n} (X_i \leq h \leftrightarrow (X_{i-1} \leq h \land f \leq X_{i-1})).
\]

(If \( f \) encodes the point \( (a, b) \) and \( a \) has binary representation \( a_n a_{n-1} \cdots a_{i+1} 01 \cdots 1 \), then the polynomial \( h \) corresponds to the union of the sets of points represented by the projections \( X_1, \ldots, X_i \).)

The equality of the \( y \)-coordinates \( b \) and \( b' \) is asserted by the formula

\[
\text{EQ}_y(f, g) \equiv \bigwedge_{i=1}^{n} (f \leq Y_i \leftrightarrow g \leq Y_i).
\]

Formulae \( \text{SUCC}_y(f, g) \) and \( \text{EQ}_y(f, g) \) are defined analogously with \( X_i \) and \( Y_i \) interchanged. Now \( H(f, g) \) and \( V(f, g) \) are defined by

\[
H(f, g) \equiv B(f) \land B(g) \land \text{SUCC}_x(f, g) \land \text{EQ}_x(f, g)
\]

\[
V(f, g) \equiv B(f) \land B(g) \land \text{EQ}_x(f, g) \land \text{SUCC}_x(f, g).
\]

These formulae have length \( O(n) \) and one existential quantifier. Note that they could be constructed with the same method as \( \forall \)-formulae.

4. With the formulae \( A, B, H, \) and \( V \) at hand we can express that \( t \) represents a correct tiling with respect to the conditions imposed by \( D_0, H, V \):

\[
\text{TIL}(t, u) = \forall f \forall g \left\{ B(f) \land B(g) \land (gu = 0)
\rightarrow \left[ \left( \bigwedge_{i=1}^{n} fX_i = 0 \land fY_i = 0 \rightarrow \bigvee_{d_j \in D_0} f \leq t_j \right)
\land \left( H(f, g) \rightarrow \bigvee_{(d_j, u_k) \in H} (f \leq t_j \land g \leq t_k) \right)
\land \left( V(f, g) \rightarrow \bigvee_{(d_j, d_k) \in V} (f \leq t_j \land g \leq t_k) \right) \right] \right\}.
\]
TIL(t, u) asserts every point which is to the right or above of an untiled point is also untiled, and that the tiled part of S is correctly tiled. It remains to encode the termination of the move. We construct a formula END(t, u) which, informally, says that for any untiled point (a, b) either the point (a - 1, b) is also untiled, or the points (a - 1, b) and (a, b - 1) are tiled by d and d', where (d, d') is a terminating pair; moreover if (a, b) is untiled then all points (a', b + 1) are also untiled:

\[
\text{END}(t, u) \equiv \forall f, \forall g \forall h \left\{ H(g, f) \land V(h, f) \land (f \leq u) \right. \\
\left. \rightarrow \left[ g \leq u \lor \bigvee_{(d, d') \in T} (g \leq t_i \land h \leq t_j) \right] \right\} \\
\land \left\{ f \leq u \land \text{SUCC}_x(f, g) \rightarrow g \leq u \right\}.
\]

The formula

\[
\text{MOVE}(t, u) \equiv A(t, u) \land \text{TIL}(t, u) \land \text{END}(t, u)
\]

is an \( \forall^2 \)-formula of linear length (because \( r = O(\sqrt{n}) \)) and it is true if the partial tiling defined by (t, u) looks like the situation after the move of one of the players.

5. In the course of the game the players define a sequence of m partial tilings \( \tau_1, ..., \tau_m \). These are described by \((r + 1)\)-tuples of polynomials \((t_1, u_1), ..., (t_m, u_m)\) such that the formulae MOVE(\( t_i, u_i \)) are satisfied. Furthermore \( \tau_i \) "extends" \( \tau_{i-1} \) in the sense that

(i) \( \tau_i \) differs from \( \tau_{i-1} \) only on points \((a, b)\) which were untiled before the \( i \)th move;

(ii) there is at least one point tiled by \( \tau_i \) but not by \( \tau_{i-1} \), unless \( \tau_{i-1} \) tiles the whole space already;

(iii) if \( i \) is odd (i.e., if \( \tau_i \) represents the constructor’s move), then only dominoes from \( E \) are used to change the tiling:

\[
\tau_i(a, b) \neq \tau_{i-1}(a, b) \rightarrow \tau_i(a, b) \in E.
\]

For the first move this is expressed by the formula

\[
\text{FIRST}(t_1, u_1) \equiv \text{MOVE}(t_1, u_1) \land \bigwedge_{d_j \in A} t_{i,j} - 0.
\]

For odd \( i \) larger than 1 we build the formula
HARD-TO-DECIDE SENTENCES

\( \exists\text{-MOVE}(t_{i-1}, u_{i-1}, t_i, u_i) \)
\[
= \text{MOVE}(t_i, u_i) \land \bigwedge_{d_j \in E} (t_{i-1, j} \leq t_{i, j}) \land \bigwedge_{d_j \in A} (t_{i-1, j} = t_{i, j}) \land ((u_{i-1} \neq 0) \rightarrow (u_{i-1} \neq u_i)).
\]

For moves of the saboteur a formula \( \forall\text{-MOVE} \) is defined similarly, with \( E \) and \( A \) interchanged.

6. Thus we can finally translate the claim that the constructor has a forced win in \( m \) moves into a formula of \( \text{Th}(F^2[X]) \):

\[
\psi_D \equiv \exists t_1 \forall t_2 \cdots \exists t_m \left[ \bigwedge_{i \text{ even}} \forall\text{-MOVE}(t_{i-1}, u_{i-1}, t_i, u_i) \rightarrow \text{FIRST}(t_1, u_1) \land \bigwedge_{i \text{ odd} \ i > 1} \exists\text{-MOVE}(t_{i-1}, u_{i-1}, t_i, u_i) \land (u_m = 0) \right].
\]

All variable sequences \((t_i, u_i)\) are relativized to correct moves and \( u_m = 0 \) ensures that \( S \) is entirely tiled after the last move. \( \psi_D \) thus says—as required—that the constructor has a winning strategy for the game \( \langle D, 2^n \rangle \) in \( m \) moves. Furthermore \( \psi_D \) has \( m + 1 \) quantifier alternations and length \( O(mn) \) (if all variables are considered as symbols of length one). Now the theorem follows from Corollary 2.2. | |

Setting \( m = 1 \) we obtain a nondeterministic exponential lower bound already for the sentences in \( \text{sat}(F^2[X]) \) with only two alternations; in fact, a close examination of the proof shows that already the prefix class \( \exists^*\forall^5 \) suffices:

**Corollary 3.2.** There is a positive constant \( c \) such that

\[ [\exists^*\forall^5] \cap \text{sat}(F^2[X]) \notin \text{NTIME}(2^{cn}). \]

**Remark.** Scrutiny of the proof of Theorem 3.1 reveals that in the construction of the formula \( \psi_D \) only atoms of the types \( f \leq g, f \leq X_i, \) and \( fX_i = 0 \) are used. The only exception is the formula

\[
A(t, u) \equiv \bigwedge_{i \neq j} (t_i t_j = 0) \land \bigwedge_i (t_i u = 0) \land \left( u + \sum_{i=1}^r t_i = 1 \right)
\]
which expresses that \( t_1, \ldots, t_r, u \) partition the set \( \mathbb{F}_2^n \times \mathbb{F}_2^n \). But \( A(t, u) \) could be replaced by the equivalent formula

\[
\overline{A}(t, u) \equiv \forall v \left[ \bigwedge_{i \neq j} (\{(v \leq t_i \land v \leq t_j) \lor (v \leq t_i \land v \leq u)\} \rightarrow v = 0) \right. \\
\left. \land \left( \left( \bigwedge_{i=1}^r v t_i = 0 \right) \rightarrow v \leq u \right) \right].
\]

The additional \( \forall \)-quantifier does not change the prefix of \( \psi_p \).

Since \( fX_i = 0 \) is equivalent to \( f \leq (1 + X_i) \) we conclude the following useful

**Fact.** To prove results similar to Theorem 3.1 and Corollary 3.2 for another mathematical theory \( \text{Th} \) it suffices to interprete (in an appropriate way that will be explained later) the constants \( X_i \), their additive inverses \( (1 + X_i) \) and the relation \( (f \leq g) \) in \( \text{Th} \).

## 4. INSEPARABILITY RESULTS

Let \( \mathcal{C} \) be a complexity class. We say that two disjoint sets \( A, B \) are \( \mathcal{C} \)-inseparable if there exists no set in \( \mathcal{C} \) which contains \( A \) and is disjoint from \( B \). Clearly the \( \mathcal{C} \)-inseparability of \( A \) and \( B \) implies that \( A \notin \mathcal{C} \).

**Lemma 4.1.** Suppose that \( A \) and \( B \) are \( \text{ATIME}(T(n), m) \)-inseparable and that \( T(dn) = o(T(n)) \) for some \( d > 0 \). If \( C \) and \( D \) are two disjoint sets and if there exists a poly-lin reduction \( f \) such that \( f(A) \subseteq C \) and \( f(B) \subseteq D \) then there exists a constant \( c > 0 \) such that \( C \) and \( D \) are \( \text{ATIME}(T(cn), m) \)-inseparable.

The proof is obvious.

**Idempotent Rings.** We now show that Theorem 3.1 can be strengthened to an inseparability result. For this purpose it is useful to note that \( \mathbb{F}_2[X] \) is a special case of an idempotent ring, i.e., a ring with unit in which every element is equal to its square. It follows immediately that the ring is commutative and has characteristic two. Furthermore an idempotent ring that is freely generated by \( n \) elements is isomorphic to the polynomial ring \( \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2 - X_1) \cdots (X_n^2 - X_n) \) (i.e., the ring of Boolean functions with \( n \) indeterminates); in particular every idempotent ring contains \( \mathbb{F}_2 \) as
a subring. It is an easy exercise to axiomatize the class of idempotent rings by an $\forall^3$-formula in the language of a ring with constants 0 and 1.

Let $\text{inv}$ be the set of logically invalid formulae; thus a sentence in the language of $F_2[X]$ is in $\text{inv}$ iff it is false in every structure $(R, +, \cdot, 0, 1, X_1, X_2, \ldots, Y_1, Y_2, \ldots)$. Then the inseparability form of Theorem 3.1 is

**Theorem 4.2.** There is a positive constant $c$ such that for all $m \geq 1$

\[ [m+1 \text{ Alternations}] \cap \text{sat}(F_2[X]) \] and $\text{inv}$ are $\text{ATIME}(2^{cn/m}, m)$-inseparable.

In particular, $[\exists^*, \forall^*] \cap \text{sat}(F_2[X])$ and $\text{inv}$ are $\text{NTIME}(2^{cn})$-inseparable.

**Proof.** In the proof of Theorem 3.1 we defined a reduction mapping a domino system $\mathcal{D}$ to a sentence $\psi_D$ which is satisfiable in $F_2[X]$ if and only if the constructor has a forced win for the game $\langle \mathcal{D}, 2^n \rangle$ in $m$ moves. However, the formula $\psi_D$ is not logically invalid, even if the saboteur wins the game defined by $\mathcal{D}$. For instance, $\psi_D$ is satisfiable—for every $\mathcal{D}$—if the underlying structure is a field.

Therefore, we conjoin to $\psi_D$ an $\forall^*$-axiom $\alpha_n$ which is valid in $F_2[X]$ and which ensures that every model $M$ of $\alpha_n$ looks sufficiently like $F_2[X]$ such that $M \models \psi_D$ implies that also $F_2[X] \models \psi_D$. Moreover $\alpha_n$ will have linear length and will be constructible in polynomial time. To simplify notation, let $m = 2n$ and $Z_1, \ldots, Z_m = X_1, \ldots, X_n, Y_1, \ldots, Y_n$.

The axiom $\alpha_n$ is a conjunction of two subformulae. The first of these is the axiom for idempotent rings. The second says that the elements $Z_1, \ldots, Z_m$ form an algebraically independent set over $F_2$. Since every algebraic relation $F(Z_1, \ldots, Z_m) = 0$ implies that at least one product $f_1 \cdots f_n$, where $f_i = Z_i$ or $f_i = 1 + Z_i$, vanishes, this is achieved by

\[
\forall f_1 \cdots \forall f_m \left( \bigwedge_{i=1}^{m} (f_i = Z_i \lor f_i = 1 + Z_i) \right) \rightarrow (f_1 \cdots f_m \neq 0).
\]

Thus, if $\psi_D$ is in $\text{sat}(F_2[X])$, then so is $\psi_D \land \alpha_n$. On the other hand, let $\psi_D$ be satisfiable in any model $M$ of $\alpha_n$. Every point of the square $\{0, \ldots, 2^n\} \times \{0, \ldots, 2^n\}$ is represented in $M$ by some product $f_1 \cdots f_m$, where $f_i = Z_i$ or $f_i = 1 + Z_i$ for all $i$. With exactly the same arguments as in the proof of Theorem 3.1, it then follows that the game $\langle \mathcal{D}, 2^n \rangle$ is won by the constructor in $m$ moves. In particular, it follows that $\psi_D$ is also true in $F_2[X]$. In other words, if $\psi_D$ is false in $F_2[X]$, then $\psi_D \land \alpha_n$ is invalid. The theorem follows.

Let $\text{sat}(\mathcal{D})$ be the sentences that are satisfiable in some idempotent ring. Since $\varphi(X_1, \ldots, X_n) \in \text{sat}(F_2[X])$ implies that $\exists X_1 \cdots \exists X_n \varphi \in \text{sat}(\mathcal{D})$ we infer
Corollary 4.3. There is a positive constant c such that for all $m \geq 1$

$$\sum_{m+1} \cap \text{sat}(\mathcal{R}) \text{ and } \text{inv} \text{ are ATIME}(2^{cn/m}, m)$$

inseparable.

The same results holds for the theory of finite idempotent rings.

5. Interpretations

Interpretations are a widely used tool to transfer results on decidability and complexity from one problem to another. In order to apply it to prefix classes in mathematical theories and to simplify the proofs in the following section it is useful to make some general observations: If $\text{Th}$ and $\text{Th}'$ are theories formulated in languages $\mathcal{L}$ and $\mathcal{L}'$, then an interpretation is a mapping taking well-formed formulae $\psi \in \mathcal{L}$ to $\psi' \in \mathcal{L}'$ such that $\psi' \in \text{Th}'$ iff $\psi \in \text{Th}$. For our purpose it is important

(i) that $\psi'$ be efficiently (i.e., polynomial time or log-space) computable from $\psi$ and $|\psi'| = O(|\psi|)$; and

(ii) that we keep the quantifier prefix of $\psi'$ under control.

First we introduce some notation: Let $\mathcal{L}$ be a relational language with relation symbols $P_1, \ldots, P_r$ of arities $i_1, \ldots, i_r$ (if the theory contains functions we replace them by their graphs). Let $\psi, D(x)$, and $Q_k(x_1, \ldots, x_k)$ be formulae with $\psi \in \mathcal{L}'$. Then we denote by

- $[P_j \equiv Q_j]\psi$ the formula $\psi$ with every occurrence of the relation $P_j$ replaced by $Q_j$;

- $[\text{Rel} \equiv D(x)]\psi$ the formula obtained from $\psi$ by relativizing all quantifiers to $D(x)$, i.e., by replacing all subformulae $\exists x \phi$ by $\exists x(D(x) \land \phi)$ and all subformulae $\forall x \phi$ by $\forall x(D(x) \rightarrow \phi)$.

Note that $[P_j \equiv Q_j]\psi$ and $[\text{Rel} \equiv D(x)]\psi$ need not be in $\mathcal{L}$ anymore.

The most simple examples of interpretations from a theory $\text{Th}$ to another theory $\text{Th}'$ are given by formulae $D(x), Q_1(x_1, \ldots, x_i), \ldots, Q_r(x_1, \ldots, x_i)$ in the language of $T'$. A formula $\psi \in \mathcal{L}$ is then mapped to

$$\psi' \equiv [\text{Rel} \equiv D(x)][P_1 \equiv Q_1] \cdots [P_r \equiv Q_r] \psi.$$

In some cases the elements of the models for $\text{Th}$ must be interpreted by $k$-tuples of elements rather than by single elements of a model for $\text{Th}'$. This is indicated by the notation $\psi = [\text{Rel} \equiv D(x_1, \ldots, x_k)]\psi$ and means that $\psi'$ is obtained from $\psi$ by replacing each quantified variable $Qx$ by $Qx_1, \ldots, Qx_k$ and relativizing the whole sequence to $D(x_1, \ldots, x_k)$.

Furthermore, if the theory $\text{Th}$ contains constants which do not
correspond in a natural way to constants in Th' then these must be introduced by existentially quantified variables.

This kind of interpretation is the basis of many undecidability proofs for mathematical theories (see, e.g., Eršov, Lavrov, Taimanov, and Taitslin (1965)). For transferring complexity bounds from one decidable theory to another there appears the additional difficulty that formulae of different length must be interpreted differently. It is thus convenient to generalize the notion of interpretation to a family of mappings \( I = (I_n)_{n \in \mathbb{N}} \) where each \( I_n \) is an interpretation in the sense above and is applied to the formulae of length \( n \). The main problem is to assure that the interpretation does not increase the length of the formulae too much; note that even if the formulae \( D_n \) and \( Q_{n,i} \) have linear length the length of the interpreted formulae will in general be quadratic. There are several ways to address this problem. A elegant and powerful approach is the concept of iterative interpretations, introduced by Compton and Henson (1990), where \( D_n \) and \( Q_{n,i} \) are defined iteratively (iterative definitions can be considered as approximations to implicit definitions). We choose here a different approach which is less general but which allows to control also the quantifier structure of the interpreted formulae: As much information as possible is pulled out of the formulae \( D, Q_1, ..., Q_r \) into an axiom \( z \). Then \( D \) and the \( Q_i \) remain fixed and only the axiom varies with \( n \).

**DEFINITION.** For two languages \( \mathcal{L}, \mathcal{L}' \) an interpretation \( I: \mathcal{L} \to \mathcal{L}' \) is given by a sequence of axioms \( \{ \alpha_n(z_1, ..., z_{i_n}) \}_{n \in \mathbb{N}} \) and by fixed formulae \( D(\bar{x}), Q_1(\bar{x}_1, ..., \bar{x}_{i_1}), ..., Q_r(\bar{x}_1, ..., \bar{x}_{i_r}) \) in \( \mathcal{L}' \). The axioms \( \alpha_n \) must be constructible in time \( n^{O(n)} \) and must have length \( O(n) \); the variables \( z_i \) interpret constants \( c_1, ..., c_{i_n} \) of \( \mathcal{L} \). \( I \) maps formulae \( \psi \) of length \( n \) to

\[
\psi' = \exists z_1 \cdots \exists z_{i_n}

(x_n \land [Rel \equiv D][P_1 \equiv Q_1] \cdots [P_r \equiv Q_r][c_1 \equiv z_1] \cdots [c_{i_n} \equiv z_{i_n}] \psi).
\]

Obviously \( \psi' \) is constructible in polynomial time from \( \psi \) and has length \( O(n) \).

Suppose that \( I \) is an interpretation mapping \( \psi \) to \( \psi' \) such that \( \psi' \in \text{Th}' \) iff \( \psi \in \text{Th} \). Then a lower complexity bound for \( \text{Th}' \) can be carried over to \( \text{Th}' \). If \( \text{sat}(\text{Th}) \) is any set of satisfiable formulae in \( \mathcal{L} \) for which we even have an inseparability result, i.e., if no set in a "well-behaved" complexity class \( \mathcal{C} \) separates sat(Th) from the invalid formulae, then we do not even need the axioms \( \alpha_n \). It suffices to have formulae \( D, Q_1, ..., Q_r \), such that

\[
\psi' = \exists z_1 \cdots \exists z_{i_n}[\text{Rel} \equiv D][P_1 \equiv Q_1] \cdots [P_r \equiv Q_r][c_1 \equiv z_1] \cdots [c_{i_n} \equiv z_{i_n}] \psi \in \text{sat}(\text{Th}')
\]

whenever \( \psi \in \text{sat}(\text{Th}); \) this implies a similar inseparability result
for sat(\(\text{Th}'\)). Indeed, if \(\psi\) is invalid, then so is \(\psi'\) (for arbitrary \(D, Q_i\)'s and \(z_i\)'s).

Under certain conditions such interpretations also preserve simple quantifier structures:

Suppose e.g., that the axioms \(x_n\) are \(\Sigma_{m'}\)-formulae for some fixed \(m'\), that \(D\) is an existential formula, and that \(Q_1, \ldots, Q_r\) are quantifier-free. Then the corresponding interpretation maps \(\Sigma_{m'}\)-formulae to \(\Sigma_{m'}\)-formulae for all \(m \geq m'\).

6. Applications to Other Mathematical Theories

Using the interpretation method described in the previous section we transfer exponential lower bounds and inseparability results for simple prefix classes from the theory of polynomial rings over \(\mathbb{F}_2\) and the theory of idempotent rings to other mathematical theories.

6.1. The Theory of Boolean Algebras

Let sat(BA) be the class of sentences in the language of Boolean algebras—containing the functions \(\cap, \cup\) and \(^\sim\) for intersection, union, and complement and the constants 0 and 1—which are satisfied by some Boolean algebra.

There is a natural equivalence between Boolean algebras and idempotent rings in the sense that every idempotent ring can be considered as a Boolean algebra via

\[
[a \cup b = a + b - ab], \quad [a \cap b = ab]; \quad [\bar{a} = 1 + a]
\]

and vice versa via

\[
[a + b \equiv (a \cap b) \cup (\bar{a} \cap b)]; \quad [ab \equiv a \cap b].
\]

So we conclude

**Theorem 6.1.** There is a positive constant \(c\) such that for all \(m \geq 1\)

\(\Sigma_{m+1} \cap \text{sat}(\text{BA})\) and \(\text{inv}\) are \(\text{ATIME}(2^{cn/m}, m)\)-inseparable.

In particular, \([\exists^* \forall^*] \cap \text{sat}(\text{BA})\) and \(\text{inv}\) are \(\text{NTIME}(2^{cn})\)-inseparable.

6.2. Polynomial Rings over Any Finite Field

The set \(S\) of all idempotent elements in an arbitrary commutative ring \(R\) with unit can be made an idempotent ring by redefining addition \((x + y)_S := (x + y - 2xy)_R\). In the ring \(F_q[X]\) the elements \(f^{q-1}\) are idempotent and form a subring which is isomorphic to \(F_2[X]\).
We thus can define an interpretation from \( \text{sat}(F_2[X]) \) to \( \text{sat}(F_q[X]) \) by mapping any sentence \( \psi \) to

\[
\psi' \equiv [\text{Rel}(f) \equiv (f^2 = f)][f + g \equiv f + g - 2fg][X_i \equiv X_i^{q-1}] \psi.
\]

If \( \psi \) is satisfiable in \( F_2[X] \) then \( \psi' \in \text{sat}(F_q[X]) \); if \( \psi \) is invalid, then so is \( \psi' \). Thus, Theorem 4.2 also holds for \( \text{sat}(F_q[X]) \).

Note that the theories of idempotent rings and of Boolean algebras are complete in \( \bigcup_{c > 0} \text{ATIME}(2^{cn}, n) \). This was proven by Kozen (1980). For \( \text{sat}(F_q[X]) \), we prove the same upper complexity bound by interpreting it in the theory of Boolean algebras:

A polynomial \( f \) in \( F_q[X_1, ..., X_n] \) is identified with a partition \( \{f_a \mid a \in F\} \) of \( F_q^n \), where \( f_a := f^{-1}(a) \). To interpret a formula \( \psi \) from the language of \( F_q[X] \) in the theory of Boolean algebras we thus associate with a quantified variable \( Qf \) a sequence \( Qf_0, ..., Qf_{q-1} \) relativized to the formula

\[
D(f_0, ..., f_{q-1}) \equiv \bigwedge_{i \neq j} (f_i \cap f_j = 0) \wedge \bigcup_i f_i = 1,
\]

expressing that the \( f_a \) (\( a \in F_q \)) partition the universe. Then addition and multiplication of polynomials can be expressed in the language of Boolean algebras via

\[
\left[ (h = f + g) \equiv \bigwedge_{c \in F_q} \left( h_c = \bigcup_{a + b = c} (f_a \cap g_b) \right) \right];
\]

\[
\left[ (h = fg) \equiv \bigwedge_{c \in F_q} \left( h_c = \bigcup_{ab = c} (f_a \cap g_b) \right) \right].
\]

Note that all these formulae are quantifier-free and do not depend on \( n \).

What remains is the interpretation of the constants. The interpretation of the constant functions offers no problem since they correspond to sequences \( c_{i,0}, ..., c_{i,q-1} \) with \( c_{i,j} = 1 \) if \( i = j \) and \( c_{i,j} = 0 \) otherwise. The projections \( X_i \) are interpreted by sequences \( x_j = x_{i,0}, ..., x_{i,q-1} \) satisfying \( D(x_{j,0}, ..., x_{j,q-1}) \). In addition we must ensure that all intersections \( (x_{i,0} \cap \cdots \cap x_{r,v}) \) for \( i_1, ..., i_r \in F_q \) are non-empty. This is expressed by the axiom

\[
\alpha_n \equiv \forall u_1 \cdots \forall u_n \left\{ \bigwedge_{i=0}^n \bigvee_{j \in F_q} u_i = x_{i,j} \rightarrow (u_1 \cap \cdots \cap u_n \neq 0) \right\}.
\]

Clearly \( \alpha_n \), \( D(f_0, ..., f_{q-1}) \), and the formulae for addition and multiplication define an interpretation from \( \text{sat}(F_q[X]) \) to \( \text{sat}(BA) \) which does not increase the number of quantifier alternations. Thus we have proved
**Theorem 6.2.** For all finite fields $F$

$$\text{sat}(F[[X]]) \in \bigcup_{c > 0} \text{ATIME}(2^{cn}, n).$$

At the end of Section 3 we remarked that it suffices to interpret the constants $X_i$ and $1 + X_i$ and the relation $(f \leq g)$ of the theory of the polynomial ring $F_2[[X]]$ into another theory to obtain results in the style of Theorem 3.1. We exploit this fact to prove lower bounds for theories which are closely related to Boolean algebras but have less expressive power:

6.3. *The Theory of Finite Sets with Inclusion* $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$

and

6.4. *The Theory of Natural Numbers with Divisibility* $\text{Th}(N_{\geq 0}, |, 1)$

It was shown by Volger (1983) that $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$ and $\text{Th}(N_{\geq 0}, |, 1)$ are complete in $\bigcup_{c > 0} \text{ATIME}(2^{cn}, n)$.

**Theorem 6.3.** Let $\text{Th}$ be $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$ or $\text{Th}(N_{\geq 0}, |, 1)$. Then there is a positive constant $c$ such that

(i) $\Sigma_{m+1} \cap \text{Th} \notin \text{ATIME}(2^{c m/m}, m)$ for all natural numbers $m \geq 2$

(ii) $[\exists \forall \forall \exists] \cap \text{Th} \notin \text{NTIME}(2^c)$.

**Proof.** First we interpret sentences $\psi$ from $\text{sat}(F_2[[X]])$ in $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$ whose quantifier-free part is built up with only constants $X_1, \ldots, X_n, (1 + X_1), \ldots, (1 + X_n)$ and atoms $(f \leq g)$. A model of $\psi$ is described by a set $m$, the constants $X_i$ and $1 + X_i$ by subsets $x_i$ and $x_i' = m - x_i$ of $m$, such that all intersections $u_1 \cap \cdots \cap u_n$ for $u_i = x_i$ or $u_i = x_i'$ are non-empty. This is expressed by the axiom

$$\alpha(m, x_1, x_1', \ldots, x_n, x_n')$$

$$\equiv \bigwedge_{i=1}^{n} [(x_i \subseteq m \land x_i' \subseteq m) \land \forall u((u \subseteq x_i \land u \subseteq x_i') \rightarrow u = \emptyset)$$

$$\land \forall u((x_i \subseteq u \land x_i' \subseteq u) \rightarrow m \subseteq u)]$$

$$\land \forall u_1 \cdots \forall u_n ([\bigwedge_{i=1}^{n} u_i = x_i \lor u_i = x_i'] \rightarrow \exists v [v \neq \emptyset \land \bigwedge_{i=1}^{n} v \subseteq u_i]).$$

Quantifiers are relativized to subsets of $m$ and atoms $f \leq g$ correspond to inclusions $f \subseteq g$. Thus the interpretation maps $\psi$ to

$$\psi' \equiv \exists m \exists x_1 \exists x_1' \cdots \exists x_n \exists x_n' \{a \land [\text{Rel}(f) \equiv (f \leq m)][(f \leq g) \equiv (f \leq g)]\psi\}.$$
Clearly $\psi \in \text{sat}(F_2[\{X\}])$ if and only if $\psi' \in \text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$. Since $\alpha$ has prefix $\forall^* \exists$ the theorem follows for $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$.

Next we interpret $\psi'$ in $\text{Th}(\mathbb{N}_{>0}, |, 1)$. Note that a natural number $z$ is squarefree iff it satisfies the formula

$$\beta(z) \equiv \forall u \forall p (p \mid u \land p \neq 1 \land p \neq u \land u \mid z \rightarrow \exists v (v \mid u \land v \neq 1 \land v \neq u \land v \neq p)).$$

All sets occurring in $\psi'$ are subsets of some fixed set $m$. We identify $m$ with the set of prime divisors of a squarefree natural number and thus set-inclusion with divisibility. Hence we can interpret $\psi'$ by

$$\psi'' \equiv \exists z \{ \beta(z) \land [\text{Rel}(x) \equiv (x \mid z)]((x \subseteq y) \equiv (x \mid y)][\emptyset \equiv 1] \psi' \}.\]$$

This proves the theorem also for $\text{Th}(\mathbb{N}_{>0}, |, 1)$. 1

6.5. The Theory of Natural Numbers with the Coprimeness Predicate $\text{Th}(\mathbb{N}_{>0}, \perp, 1)$

This theory is also contained in $\bigcup_{c>0} \text{ATIME}(2^{cn}, n)$ since it is interpretable in $\text{Th}(\mathbb{N}_{>0}, |, 1)$ via

$$[(x \perp y) \equiv \forall u ((u \mid x \land u \mid y) \rightarrow u = 1)].$$

It is more complicated to interpret appropriate formulae in $\text{Th}(\mathbb{N}_{>0}, \perp, 1)$ than in the theory of natural numbers with divisibility which causes a slightly weaker result for this theory:

**Theorem 6.4.** There is a positive constant $c$ such that

$$\Sigma_{m+2} \cap \text{Th}(\mathbb{N}_{>0}, \perp, 1) \notin \text{ATIME}(2^{cn/m}, m) \text{ for all natural numbers } m \geq 1.$$

**Proof.** As in the proof for $\text{Th}(\mathbb{N}_{>0}, |, 1)$ we will interpret the formula $\psi'$ from $\text{Th}(P_{\text{fin}}, \subseteq, \emptyset)$ constructed above. There is, however, no way to express squarefreeness in $\text{Th}(\mathbb{N}_{>0}, \perp, 1)$. Thus the set $m$ is identified with the set of primes which divide some arbitrary number $z$. A subset of $m$ is interpreted now by a pair $(x, x')$ of coprime numbers, such that any prime dividing $z$ divides either $x$ or $x'$ and vice versa. This is expressed by the formula

$$D(x, x') \equiv x \perp x' \land \forall u (u \perp x \land u \perp x' \leftrightarrow u \perp z).$$

Note that the correspondence between sets and pairs of natural numbers is not unique. Before $\psi'$ is interpreted in $\text{Th}(\mathbb{N}_{>0}, \perp, 1)$ all occurrences of
atoms \((x = y)\) should be replaced by \((x \subseteq y) \land (y \subseteq x)\). Finally the interpretation maps \(\psi'\) to

\[
\psi'' \equiv \exists z [\text{Rel} \equiv D(x, x')] [(x \subseteq y) \equiv (x \perp y')] [\emptyset \equiv (1, z)] \psi'.
\]

By elementary transformations it can be arranged that the \(\forall\)-quantifier occurring in \(D(x, x')\) increases the number of quantifier alternations only by 1. For the case \(m = 1\), where \(\psi'\) has an \(\exists^*\forall^*\exists\)-prefix the last existentially quantified variable needs not be relatived by \(D\). Hence \(\psi'\) is transformed to a \(\Sigma_3\)-formula.

Lower complexity bounds for (prefix classes of) the theory of Boolean algebras can also be extended to theories of lattices or semilattices in which Boolean algebras are defined by simple formulae. For the theories of lattices in general and for many extensions such as the theory of distributive lattices, modular lattices, etc., this is not a very interesting observation since these theories are undecidable. There are, however, some examples of lattice theories which are decidable in alternating exponential time:

6.6. The Theory of Semilattices with 0

A semilattice is a structure \((L; \cap, 0)\), where \(\cap\) is a commutative, associative, and idempotent function and \(a \cap 0 = 0\) for all \(a\). Let \(\text{sat}(SL)\) be set of sentences which are true in some semilattice. We extend the theory of semilattices by the axiom

\[
x \equiv \forall x \exists y \forall z [x \cap y = 0 \land (x \cap z = 0 \rightarrow y \cap z = z) \land (y \cap z = 0 \rightarrow x \cap z = z)]
\]

which expresses: (i) that the semilattice is pseudocomplemented, i.e., that for every \(x\) there exists a (unique) pseudocomplement \(x^*\) which contains all \(z\) disjoint from \(x\); (ii) that \(x^{**} = x\). It is well known (see, e.g., Grätzer, 1978) that for every pseudocomplemented semilattice \(L\), the set \(L^* = \{x^* \mid x \in L\}\) is a Boolean algebra with \(a \cup b := (a^* \cap b^*)^*\). Since \(\alpha\) enforces that \(L = L^*\), every model of \(\alpha\) is a Boolean algebra. In particular it is possible to interpret \(\text{Th}(P_{\alpha n}, \subseteq, \emptyset)\) in \(\text{sat}(SL)\). Since \(\alpha\) is an \(\forall \exists \forall\)-sentence it follows that

**Theorem 6.5.** There is a positive constant \(c\) such that

\[
\Sigma_{m+1} \cap \text{sat}(SL) \notin \text{ATIME}(2^{cn/m}, m) \text{ for all natural numbers } m \geq 3.
\]

An \(\text{ATIME}(2^{cn}, n)\) upper complexity bound for this theory has been verified by Weispfenning (1985).
6.7. Stone Algebras

Or, more generally,

6.8. Distributive p-Algebras in the Lee Class $\mathcal{B}_n$

A distributive p-algebra $A$ is a distributive lattice containing basides $\cap$ and $\cup$ a unary function $*$ for pseudocomplementation. $A$ is in $\mathcal{B}_n$ if it satisfies the Lee-identity

$$I_n \equiv \forall x_1 \cdots \forall x_n [(x_1 \cap \cdots \cap x_n)^*$$
$$\cup (x_1^* \cap \cdots \cap x_n)^* \cup \cdots \cup (x_1 \cap \cdots \cap x_n^*)^* = 1].$$

For $n = 1$ the identity takes the form $\forall x(x^* \cup x^{**} = 1)$ and is called the Stone-identity; the algebras in $\mathcal{B}_1$ are called Stone algebras. Weispfenning (1985) proves that the theory of Stone algebras and the theory of $\mathcal{B}_2$ are both in $\bigcup_{c > 1} \text{ATIME}(2^c n, n)$. Extension to the higher Lee classes $\mathcal{B}_n$ ($n > 2$) is announced for a subsequent paper.

Since every Lee class $\mathcal{B}_n$ contains all Boolean algebras, Theorem 6.1 also holds for these theories.

Received June 9, 1988; final manuscript received February 21, 1990

REFERENCES


