Some Structural Properties of SAT

LIU Tian (~l)
Department of Computer Science and Technology, Peking University, Beijing 100871, P.R. China
E-mail: tianliu@263.net
Received March 1, 1999; revised July 16, 1999.

Abstract The following four conjectures about structural properties of SAT are studied in this paper. (1) SAT ∈ \( P^{\text{SPARSE} \cap \text{NP}} \); (2) SAT ∈ \( \text{SRTD}_{tt} \); (3) SAT ∈ \( \text{Pbt} \text{APP} \); (4) \( F_{\text{P}^\text{SAT}} = F_{\text{P}^\text{SAT}} \). It is proved that some pairs of these conjectures imply \( P = NP \), for example, if SAT ∈ \( P^{\text{SPARSE} \cap \text{NP}} \) and SAT ∈ \( \text{Pbt} \text{APP} \), or if SAT ∈ \( \text{SRTD}_{tt} \) and SAT ∈ \( \text{Pbt} \text{APP} \), then \( P = NP \). This improves previous results in literature.

Keywords structural complexity, SAT, sparse set, approximable set, truth-table reduction, non-adaptive search reducible to decision.

1 Introduction

Consider the following four hypotheses about structural properties of SAT:

(1) SAT ∈ \( P^{\text{SPARSE} \cap \text{NP}} \). Namely SAT is polynomial time Turing reducible to a sparse NP set.

(2) SAT ∈ \( \text{SRTD}_{tt} \). Namely SAT is polynomial time non-adaptive search reducible to decision, i.e., there exists a polynomial time procedure which on inputting \( x \) nonadaptively queries oracle SAT and outputs a satisfying assignment for every \( x \in \text{SAT} \). Here “non-adaptively” means that all queries are generated independently, i.e., all queries to be queried must have been generated before any answer is gotten from the oracle.

(3) SAT ∈ \( \text{Pbt} \text{APP} \). Namely SAT is polynomial time truth-table reducible to a \( k \)-approximable set for some constant \( k \). Here a truth-table reduction is a Turing reduction with only non-adaptive queries.

(4) \( F_{\text{P}^\text{SAT}} = F_{\text{P}^\text{SAT}} \). Namely the power of an unbounded number of non-adaptive queries to SAT is strictly the same as the power of a logarithm number of adaptive queries to SAT when using SAT as an oracle to compute functions in polynomial time. Here “adaptive” means that queries are generated one by one and dependently, i.e., the next query can be generated according to the answers to the previous queries.

These four hypotheses have been extensively studied in structural complexity theory. Assume \( P = NP \) then all these four hypotheses are true. So, any absolute disproof to any one of these four hypotheses implies that \( P \neq NP \) and hence such a disproof is very hard to obtain. Because of this reason, previous research work has focused on the relationships between these four hypotheses and other important complexity theory hypotheses such as \( P = NP \)p-4, \( PH \) collapses\p-5,6] and \( NP \) is small\p-7,8]. For example, the following results are known.

On hypothesis (1) SAT ∈ \( P^{\text{SPARSE} \cap \text{NP}} \), it is known that

- \( \{ \text{SAT} ∈ \text{P}^{\text{SPARSE}} \} \Rightarrow \{ \text{PH collapses} \}\p-5,6]\)
- \( \{ \text{SAT} ∈ \text{P}^{\text{SPARSE} \cap \text{NP}} \} \Rightarrow \{ \text{PH} = \text{P}^{\text{NP}} \}\p-9]\)
- \( \{ \text{SAT} ∈ \text{P}^{\text{SPARSE}} \} \Rightarrow \{ P = NP \}\p-10]\)
- \( \{ \text{SAT} ∈ \text{P}^{\text{SPARSE}} (c < 1) \} \Rightarrow \{ NP \text{ is small} \}\p-11]\)
- \( \{ \text{SAT} ∈ \text{P}^{\text{SPARSE}} \} \Rightarrow \{ F_{\text{P}^{\text{SAT}}} = F_{\text{P}^{\text{SAT}}} \}\p-12]\).

This work is supported by the key project fund of China’s Ninth Five-Year Plan and the Science Foundation of Peking University.
On hypothesis (2) \( \text{SAT} \in SRTD_{tt} \), it is known that
- \( \text{SAT}^O \in SRTD_{tt}^O \), for random oracle \( O \)[11]
- \( (\text{SAT}^A \in SRTD_{tt}^A) \land (PH^A \text{ is proper}), \) for some oracle \( A \)[12]
- \( \text{SAT}^B \notin SRTD_{tt}^B \), for some oracle \( B \)[13].

On hypothesis (3) \( \text{SAT} \in \text{P}^{\text{APP}} \), it is known that
- \( (\text{SAT} \in \text{P}^{\text{APP}}) \Rightarrow (PH \text{ collapses})^{[4-6,14]} \)
- \( (\text{SAT} \in \text{P}^{\text{APP}} (c < 1)) \Rightarrow (P = NP)^{[4]} \)
- \( (\text{SAT} \in \text{P}^{\text{APP}}) \Rightarrow (NP \text{ is small})^{[8]} \)
- \( (\text{SAT} \in \mathcal{P}^{\text{APP}}) \Rightarrow \left( \mathcal{P}^{\text{SAT}} = \mathcal{P}^{\text{SAT}} \right)^2. \)

This is to say by our notations (3) \( \Rightarrow (4) \).

On hypothesis (4) \( \mathcal{P}^{\text{SAT}} = \mathcal{P}^{\text{log}} \), it is known that
- \( \left( \mathcal{P}^{\text{SAT}} = \mathcal{P}^{\text{log}} \right) \Rightarrow ((\text{FewP} = P) \land (NP = \mathcal{R})) \Rightarrow (PH \text{ collapses})^{[5,6,15-17]} \).

Of course, the most important complexity hypothesis is \( P = NP \). So the conjectures "\( (i) \Rightarrow (P = NP) \)" for \( i = 1, 2, 3, 4 \) are of special interests. Although much effort has been made, today these conjectures are still open. Here it should be stressed that in this paper "conjectures" are statements which are about the relationships between hypotheses and may be proved by our current proof techniques, while "hypotheses" are statements about properties of sets which are with little hope to be proved. So the topics of this paper are about conjectures "\( (i) \Rightarrow (P = NP) \)" rather than directly about hypotheses "\( (i) \)". In this paper, it is proved that either "\( (i) \Rightarrow (P = NP) \)" or "\( (j) \Rightarrow (P = NP) \)" is true for some pairs of \( (i) \) and \( (j) \). In fact, it is proved that "\( (i) \land (j) \Rightarrow (P = NP) \)" is true for the following pairs of \( (i) \) and \( (j) \).
- \( ((1) \land (3)) \Rightarrow (P = NP). \) This improves a result in [1].
- \( ((1) \land (4)) \Rightarrow (P = NP). \)
- \( ((2) \land (3)) \Rightarrow (P = NP). \) This improves a result in [2].
- \( ((2) \land (4)) \Rightarrow (P = NP). \)

The importance of this theorem is as follows. Note that

\[
(A \land B) \Rightarrow C \equiv \neg(A \land B) \lor C \equiv \neg A \lor \neg B \lor C \\

\equiv (A \Rightarrow C) \lor (B \Rightarrow C)
\]

This is to say that if "\( (i) \land (j) \Rightarrow (P = NP) \)" is true then either "\( (i) \Rightarrow (P = NP) \)" or "\( (j) \Rightarrow (P = NP) \)" is true. So by our results it is known that at least one of the two conjectures "\( (i) \Rightarrow (P = NP) \)" and "\( (j) \Rightarrow (P = NP) \)" is true for above pairs of \( (i) \) and \( (j) \), though it is not explicitly known which one is true. Note that "\( (2) \Rightarrow (P = NP) \)" cannot be proved by any relativizable methods\[^{[11-13]}\], so in some degree our results reach the limit of relativizable methods. Our results and methods also improve some previous results and methods, these are stated in the section of main results.

This paper is organized as follows. In Section 2, our notions and notations are described. In Section 3, definitions are given and our main results are presented. In Section 4, a short conclusion is given.

## 2 Preliminaries

For backgrounds in structural complexity theory, see [18] and [19]. Our notions and notations are standard as in [18]. Let \( \Sigma = \{0, 1\} \) be a fixed alphabet, \( \Sigma^* \) be the set of all strings of finite length, \( \Sigma^n \) be the set of all strings of length \( n \), and \( \Sigma^\leq n \) be the set of all strings of length \( \leq n \). \( |x| \) denotes the length of a string \( x \). \( |A| \) denotes the cardinality of a set \( A \). \( \mathcal{N} \) is the set of all natural numbers. \( \text{Poly} = \{n^k + k|k| \text{ is an integer}\} \) is the standard enumerating of all polynomials. \( \langle \cdot, \cdot \rangle \) is the standard pairing function, which can be extended to more than two variables, for example, \( \langle x_1, x_2, x_3 \rangle = \langle \langle x_1, x_2 \rangle, x_3 \rangle \). These functions are