\( \mathcal{P} \) is not equal to \( \mathcal{NP}^* \)

Sten-Åke Tärnlund†

June 29, 2015

Abstract

A new axiom of Turing’s theory of computing is used to prove that \( SAT \) is not in \( \mathcal{P} \). Thus, \( \mathcal{P} \) is not equal to \( \mathcal{NP} \), follows directly. A computer-oriented version verifies the results, elsewhere, using a theorem-prover.

1 Introduction

It is proved that computing whether each propositional formula is satisfiable is not in \( \mathcal{P} \), which is the set of problems having a solution in polynomial computing time, in the size of the input, using a deterministic Turing machine. Equivalently, Theorem 1 \( SAT \not\in \mathcal{P} \). But, \( SAT \in \mathcal{NP} \) – a set of problems having a solution in polynomial computing time, in the size of the input, using a non-deterministic Turing machine. Therefore, Theorem 2 \( \mathcal{P} \not= \mathcal{NP} \) cf. Cook [2].

Chiefly, the results follow from the new Axiom 1 Tärnlund [10], of Turing’s theory of computing [14] that rises the information about computing. For example, the complexity of a proof from Axiom 1 could be measured both by the number of head moves of a Turing machine, and the number of symbols in the proof. This opens into a proof of the crucial Lemma 1. If \( SAT \in \mathcal{P} \) then all sufficiently large tautologies \( F \) on disjunctive normal form (DNF) have a formal propositional proof of polynomial size – in the size of \( F \) – in Robinson resolution systems [8]. Then, \( SAT \not\in \mathcal{P} \), by Lemma 1 and Haken’s theorem [3].

The human-oriented proofs are informal, in Hilbert’s proof theory [5], about formal proofs from Axiom 1 in Robinson resolution systems. For convenience, they are presented in a Kleene G4 system, but they could be presented in Robinson resolution systems without G4.

In fact, these human-oriented results have been converted into a computer-oriented version and are verified, Tärnlund [12], using a theorem prover Vampire of Riazanov and Voronkov [7].

The postulates of predicate logic (including propositional logic), a consistent subset of Theory B, Section 2, and number theory are used to reach these results.

Methods of Clark and Tärnlund [1] have been helpful.

†Copyright © 2015, Sten-Åke Tärnlund, Stockholm Sweden, gmail: stenake.
1The proof ideas are similar to former editions, Tärnlund [10] [11] [12] [13].
2 \( PF_n \) for a tautology on DNF expressing \( n \) pigeons in \( n+1 \) holes have an empty hole.

**Theorem.** (Haken) There exists a constant \( c, c > 1 \), so that, for sufficiently large \( n \), every resolution proof of \( PF_n \), contains at least \( c^n \) different clauses.
2 Axiom 1

Theory B, Tärnlund [12], axiomatizes Turing’s theory of computing in predicate calculus. A new single Axiom 1 defines a universal Turing machine in (2)–(5), using a $U$-predicate – a relationship of a two-way tape $x, s, z$ with its head at the symbol $s$, a state $q$, Turing machines $j, i$, and output $u$. Axiom 1 has five parts: (1) $U$ defines a predicate $T(i, a, u)$, i.e., Turing machine $i$ – a list of quintuples – computes $u$ for input $a$ (and terminates); (2) $U$ halts at state 0; (3) $U$ reads $s$, writes $r$, moves the head one element to the left, goes from state $q$ to state $p$, and resets to $i$; (4) is similar to (3), but the head moves to the right; and (5) $U$ searches a quintuple of $j$ for $s$ and $q$. The intended domains are: a set $S$ of symbols, a set $Q$ of states, a set $D$ of head moves, a set $R$ of right tapes, a set $L$ of left tapes, and a set $M$ of codes of Turing machines, $i j \in M a z \in R u x \in L s v r s' \in S p q q' \in Q d \in D$.

Axiom 1 for $U(\emptyset, \emptyset, a, 1, i, i, u)$  \[ \supset T(i, a, u) \].

The free variables have the generality interpretation. $\emptyset$, 0, and 1 are constants and $\cdot$ is an infix term for lists.

3 Complexity measures

Let the computing time be the number of moves of the head, on the tape, of a Turing machine in a computation, cf. Hartmanis and Stearns [4].

Kleene’s G4 system is used to analyse proofs, cf. Proposition 1 footnote 5.

Definition 1 $\vdash B \rightarrow T(i, a, u)$ in $z$ if and only if there exists a formal deduction of $T(i, a, u)$ from $B$ in computing time less than or equal to $z$ all $i \in M a \in R u \in L z \in Z^+$.

Definition 2 Let $W$ be the nonempty set of all deterministic Turing machines computing whether $G$ is satisfiable – writing the output 0 – or not – writing the output 1 – for all propositional formulas $G$.

Definition 3 If $SAT \in P$ then $\vdash B \rightarrow \exists u T(i, G, \emptyset, u)$ in $c \cdot |G|^n$ some $c n \in Z^+ i \in W$ all propositional formulas $G$.

Let $b$ be the name of some $i \in W$ assumed to exist in Definition 3 (6). Then, using Axiom 1 and (6), and let $TAUT$ be the set of tautologies.

Corollary 1 $T(b, \neg F, \emptyset, 0, 1) \supset F$ all $F \in TAUT$.  

---

3Axiom 1 is a slight simplification of a formula in Tärnlund [9].
4In Theory B the input and the output are coded as lists, i.e., $G, \emptyset, 0, 0$, and $0, 1$. 

2
Axiom, Corollary, and Definition give the following result.

**Corollary 2** If $\text{SAT} \in \mathcal{P}$ then $\vdash B \rightarrow F$ in $c \cdot |F|^n$ some $c \in \mathbb{Z}^+$ all $F \in \text{TAUT}$ on DNF.

Let the size of a proof be the number of symbols in the proof.

**Definition 4** $|\vdash R F| \in \mathcal{O}(|F|^m)$ if the size of an existing formal proof of $F$ in Robinson resolution systems has a polynomial upper bound $\mathcal{O}(|F|^m)$ all $m \in \mathbb{Z}^+$ sufficiently large $F \in \text{TAUT}$ on DNF.

## 4 Lemma and a proof

Lemma written informally in Section is formalized next using Definition.

**Lemma 1** If $\text{SAT} \in \mathcal{P}$ then $|\vdash R F| \in \mathcal{O}(|F|^n)$ some $n \in \mathbb{Z}^+$ all sufficiently large $F \in \text{TAUT}$ on DNF.

**Proof.** Assume that $\text{SAT} \in \mathcal{P}$.

Thus, by Corollary

$$\vdash B \rightarrow F$$

in $c \cdot |F|^n$ some $F \in \text{TAUT}$ on DNF.

Let $U_{j,k}$ be the short name for a propositional predicate $U$ from Axiom. Let $j$ be the computing time and, for each $j$, let $k$ count the atoms to find a quintuple of $b, j, k \in \mathbb{N}$. Let $T$ be $T(b, \neg F, \emptyset, 0, 1)$.

Then, there is Kleene G4 proof, by (8), but there is a Robinson resolution proof too, and it is computed in Proof tree 1.

**Proof tree 1** A resolution proof in computing time $j + 1 \leq c \cdot |F|^n$.

\[
\begin{align*}
B, U_{j,k} & \rightarrow U_{j,k} \\
B, U_{j+1,0} & \rightarrow U_{j+1,0} \\
\vdots \\
B, U_{0} & \rightarrow U_{0} \\
B & \rightarrow U_{1,0} \\
B, T & \rightarrow T \\
B, U_{1,0} & \rightarrow U_{0,0} \\
B, F & \rightarrow F \\
B, U_{0,0} & \rightarrow T \\
B, T & \rightarrow F, \text{ Corollary} \\
\vdash B \rightarrow F \text{ in } c \cdot |F|^n
\end{align*}
\]

\footnote{Robinson resolution systems give, by induction on the computing times.}

**Proposition 1** If a Turing machine $i$ for input $a$ computes output $u$ in polynomial computing time $c \cdot |a|^n$ then $B \vdash \mu T(i, u, a)$ in $c \cdot |a|^n$ all $i \in M$ all $a \in \mathcal{L}$ all $u \in \mathcal{L}$ all $c \in \mathbb{Z}^+$.

Axiom and Corollary are logic programs, and $F, \ldots, U_{j+1,0}$ are goals, cf. Kowalski. Proof tree can be seen as a resolution proof, without Kleene’s G4.
In Proof tree 1, a formal propositional resolution proof of $F$ is computed in computing time $c \cdot |F|^n$ in Robinson resolution systems. The formulas from Axiom 1 are instantiated to propositional formulas. The proof is written:

$$U_{(j+1)0}, U_{(j+1)1} \supset U_{j+k_1}, U_{j+k_2} \supset U_{j(k_j-1)}, \ldots, U_{j+n} \supset U_{(j-1)(k_{j-1})},$$

$$\ldots, U_{20}, U_{20} \supset U_{1k_1}, U_{2k_1}, \ldots, U_{11}, U_{11} \supset U_{10},$$

$$U_{10}, U_{10} \supset U_{00}; U_{00} \supset T, T \supset F, F.$$  \hspace{1cm} (9)

For $b$ in (6), let $f : TAUT \rightarrow Z^+$ be the map whose value at $F$ is the computing time, i.e., $z + 1 \leq c \cdot |F|^n$, let $r$ be the map whose value at $z + 1$ is the Robinson resolution proof of $F$, and let $h$ be the map whose value at $z + 1$ is a partial proof. Then, the map $\Delta$ is defined such that $\Delta(F)$ is (9).

**Definition 5**  \hspace{1cm} $\Delta = r \circ f$.

$r(1) = (U_{10}, U_{10} \supset U_{00}; U_{00} \supset T, T \supset F, F)$.

$h(z + 1) = (U_{(z+1)0}, U_{(z+1)1} \supset U_{zk_2}, U_{zk_2}, U_{zk_2} \supset U_{z(k-z-1)}; U_{z(k-z-1)}, 0 \leq q < k_z$ all $z \in N$ some $k_z \in Z^+$).

First, Axiom 1, Definition 5, induction on the computing times, and number theory give,

$$\text{If } \vdash B \rightarrow F \text{ in } c \cdot |F|^n \text{ then } \Delta(F).$$

Hence, using (5),

$$\Delta(F).$$  \hspace{1cm} (11)

By induction on the computing times, the formal definition of a propositional Robinson resolution proofs, cf. Tärnlund 10, gives,

$$\Delta(F) \text{ is a propositional Robinson resolution proof of } F \text{ on DNF.}$$  \hspace{1cm} (12)

Therefore,

$$\vdash \forall F \in TAUT \text{ on DNF.}$$  \hspace{1cm} (13)

Second, for each size of $b$ there are sufficiently large $F \in TAUT$ such that $|b| < |F|$. The size of each propositional predicate of Axiom $B$ in $\Delta(F)$ has a polynomial upper bound $c \cdot |F|^n$, $k_z < |F|$, and the computing time $z < c \cdot |F|^n$.

Thus, by Axiom 1, Definition 5, (11), and number theory,

$$|\Delta(F)| \in O(|F|^2n+1).$$  \hspace{1cm} (14)

Hence, by Definition 4 and (11),(14),

$$|\vdash \forall F| \in O(|F|^2n+1).$$  \hspace{1cm} (15)

Discharging the assumption (7) ends the proof. Therefore,

If $SAT \in P$ then $|\vdash \forall F| \in O(|F|^n)$ some $n \in Z^+$ all sufficiently large $F \in TAUT$ on DNF.

\footnote{It is assumed that the first quintuple of $b$, in (6), is (1.s.p.r.d).}
5 \(\text{SAT} \notin \mathcal{P} \text{ and } \mathcal{P} \neq \mathcal{NP}\)

Lemma \[1\] and Haken’s theorem cf. footnote \[2\] give, by reductio ad absurdum,

**Theorem 1** \(\text{SAT} \notin \mathcal{P}\).

However, \(\text{SAT} \in \mathcal{NP}\), cf. Section \[1\]. Therefore,

**Theorem 2** \(\mathcal{P} \neq \mathcal{NP}\).

**Corollary 3** \(\text{TAUT} \notin \mathcal{P}\).

**Acknowledgment**

Hanna-Nina Ekelund, Niklas Ekelund, Andreas Hamfelt, Torsten Palm, Bo Steinholtz, Carl-Anton Tärnlund, and the participants of The Stockholm-Uppsala Logic Seminar 3 February 2010 thank you all.

**References**


