

# **P $\neq$ NP under a constructive interpretation of Peano Arithmetic<sup>1</sup>**

Bhupinder Singh Anand<sup>2</sup>

We show that all provable arithmetical formulas are Turing-decidable as TRUE under the standard interpretation of a standard, first-order, Peano Arithmetic, PA. An immediate consequence is that the set of Gödel-formulas of PA is empty, and that PA has no non-standard models. We show that this implies, further, that P  $\neq$  NP.

## **1. Introduction**

In a paper presented to ICM 2002, Ran Raz comments [Ra02]:

“A Boolean formula  $f(x_1, \dots, x_n)$  is a tautology if  $f(x_1, \dots, x_n) = 1$  for every  $x_1, \dots, x_n$ . A Boolean formula  $f(x_1, \dots, x_n)$  is unsatisfiable if  $f(x_1, \dots, x_n) = 0$  for every  $x_1, \dots, x_n$ . Obviously,  $f$  is a tautology if and only if  $\sim f$  is unsatisfiable.

Given a formula  $f(x_1, \dots, x_n)$ , one can decide whether or not  $f$  is a tautology by checking all the possibilities for assignments to  $x_1, \dots, x_n$ . However, the time needed for this procedure is exponential in the number of variables, and hence may be exponential in the length of the formula  $f$ . ...

---

<sup>1</sup> Created: Saturday, 25<sup>th</sup> March 2006, 8:21:29 AM IST. Updated Monday, 2<sup>nd</sup> October 2006, 1:05:46 AM IST, by re@alixcomsi.com. A .pdf file of this essay before the current update is available at <http://arXiv.org/abs/math.GM/0603605>.

<sup>2</sup> The author is an independent scholar. E-mail: re@alixcomsi.com; anandb@vsnl.com. Postal address: 32, Agarwal House, D Road, Churchgate, Mumbai - 400 020, INDIA. Tel: +91 (22) 2281 3353. Fax: +91 (22) 2209 5091.

$P \neq NP$  is the central open problem in complexity theory and one of the most important open problems in mathematics today. The problem has thousands of equivalent formulations. One of these formulations is the following:

Is there a polynomial time algorithm  $A$  that gets as input a Boolean formula  $f$  and outputs 1 if and only if  $f$  is a tautology?  $P \neq NP$  states that there is no such algorithm.”

Now, Gödel has defined a formula,  $[R(x)]$ , such that:

- (i)  $[R(x)]$  is constructible in standard, first-order, Peano Arithmetic, PA;
- (ii) we can prove, meta-mathematically, that  $[R(x)]$  translates as an arithmetical tautology,  $R(x)$ , under the standard interpretation (Appendix C) of the Arithmetic;
- (iii)  $[R(x)]$  is not provable in the Arithmetic.

The question arises: Is  $R(x)$  Turing-decidable as TRUE?

If we assume, first, the thesis that every total arithmetical relation that is Turing-decidable as TRUE is PA-provable, then  $R(x)$  is not Turing-decidable as TRUE, and, so,  $P \neq NP$ .

If we assume, however, that there is a total arithmetical relation that is Turing-decidable as TRUE, but which is not PA-provable, then this implies that there is a non-trivial<sup>3</sup>, non-standard, model of PA, say  $M'$ , in which, if  $[R(x)]$  is unprovable, then  $\sim R(s)$  holds for some  $s$  in the domain of  $M'$  that is not a natural number.

---

<sup>3</sup> We define a trivial, non-standard, model of Peano Arithmetic as one obtained by adding to it, for example, a new individual constant  $[b]$ , and corresponding axioms such as  $[b] \neq [0]$ ,  $[b] \neq [1]$ ,  $[b] \neq [2]$ , ...,  $[b] \neq [n]$ , .... (cf. [Me64], p117).

We conclude that, if PA has no non-trivial, non-standard models, then, under the above expression of the PvNP problem,  $P \neq NP$ .

In the rest of the paper, we show that, if PA is a standard, first-order, Peano Arithmetic, as defined in Appendix A ([Me64], p57), and Appendix B ([Me64], p103), then PA has no non-trivial, non-standard, models.<sup>4</sup>

## **2. The standard interpretation, M, of first-order, Peano Arithmetic, PA**

Let PA be a standard, first-order, Peano Arithmetic.

Since the axioms of PA are taken to interpret as intuitively true under its standard interpretation, M (Appendix C), and the rules of inference preserve truth under the standard interpretation, M defines a model, say  $\{N, M\}$ , of PA.<sup>5</sup>

This model is the intuitive arithmetic of the whole numbers as expressed by Dedekind's semi-axiomatic formulation of the Peano Postulates ([Me64], p102), where N denotes the set of non-negative integers.

## **3. A constructive, Turing-decidable, interpretation, M\*, of PA**

Consider, now, the constructive interpretation, M\*, of PA where a PA-formula such as, say,  $[R(x)]$ , is satisfied under M\* if, and only if, it interprets as a total arithmetical relation that is Turing-decidable as always TRUE in M.

**Definition:** A total number-theoretical relation,  $R(x_1, x_2, \dots, x_n)$ , when treated as a Boolean function, is defined as Turing-decidable in M if, and only if, there is a

---

<sup>4</sup> In an unpublished, arXived, paper, “The Göbbellian Syndrome”, I argue, independently, that PA has no non-trivial, non-standard, models. <<http://arxiv.org/ftp/math/papers/0507/0507046.pdf>>

<sup>5</sup> By Tarski's definitions of the satisfiability, and truth, of the formulas of a formal language under an interpretation ([Me64], p49-53).

Turing-machine  $T$  such that, for any given natural number sequence,  $(a_1, a_2, \dots, a_n)$ ,  $T$  will compute  $R(a_1, a_2, \dots, a_n)$  as either TRUE, or as FALSE.

By Tarski's definitions of the satisfiability and truth of the formulas of a formal language under an interpretation, we then have that:

(a)  $[(\forall x)R(x)]$  is true under  $M^*$  if, and only if,  $[R(x)]$  is satisfied in  $M^*$ ;

(b)  $[\sim(\forall x)R(x)]$  is true under  $M^*$  if, and only if,  $[(\forall x)R(x)]$  is not true in  $M^*$ .

In other words,  $[\sim(\forall x)R(x)]$  is true under  $M^*$  if, and only if,  $[(\forall x)R(x)]$  interprets as an arithmetical relation that is NOT Turing-decidable as TRUE in  $M$ .

We now note that, if PA is consistent, then:

(i) The axioms of PA are Turing-decidable as TRUE under interpretation in  $M$ ;

(ii) The rules of inference of PA preserve Turing-decidability.

Hence the theorems of PA are Turing-decidable as TRUE under interpretation in  $M$ .

The argument can also be expressed more formally as follows:

**Theorem 1:** The theorems of a consistent PA are Turing-decidable as TRUE in  $M$ .

**Proof:** We assume that  $[P(x_1, x_2, \dots, x_n)]^6$  is a theorem of PA, and  $p$  it's Gödel-number.

We, then, consider Gödel's ([Go31a], p17-22):

(i) primitive recursive relation,  $B_w(x)$ , which holds, if, and only if,  $x$  is the Gödel-number of a proof-sequence in PA;

---

<sup>6</sup> We note that this includes the case where  $[P]$  may not have any free variables.

- (ii) primitive recursive function,  $Sb(p [(x_1, x_2, \dots, x_n)][(a_1, a_2, \dots, a_n)])$ , which is the Gödel-number of the PA-formula  $[P(a_1, a_2, \dots, a_n)]$ , where  $p$  is the Gödel-number of the PA-formula  $[P(x_1, x_2, \dots, x_n)]$ , and  $[(a_1, a_2, \dots, a_n)]$  is any formal sequence of terms of PA;
- (iii) primitive recursive relation,  $xBy$ , which holds if, and only if,  $x$  is the Gödel-number of a proof-sequence of PA, and,  $y$  is the Gödel-number of the last formula in the sequence.

Now, every total function (or relation - treated as a Boolean function) is recursive if, and only if, it is Turing-computable ([Me64], Corollary 5.13, p233).

We can, thus, define a Turing machine,  $T_p$ , such that  $T_p$  will compute  $\{Bw(k) \& kB(Sb(p [(x_1, x_2, \dots, x_n)][(a_1, a_2, \dots, a_n)]))\}$  as TRUE (treated as a Boolean function), for any natural number  $k$ , and any formal sequence  $[(a_1, a_2, \dots, a_n)]$  of terms of PA, if, and only if,  $[P(a_1, a_2, \dots, a_n)]$  is provable in PA, and FALSE otherwise.

Hence, the PA-theorem,  $[P(x_1, x_2, \dots, x_n)]$ , is Turing-decidable as TRUE in M.

Since  $[P(x_1, x_2, \dots, x_n)]$  is the general case, it follows that the theorems of PA are Turing-decidable as TRUE in M.  $\square$

**Corollary 1.1:**  $M^*$  defines a model,  $\{N, M^*\}$ , of PA.

Since the above holds for any recursively definable extension, P, of PA, we thus have:

**Corollary 1.2:** Every recursively definable extension, P, of PA, has a model which implies that the theorems of P are Turing-decidable as TRUE in M.

#### 4. The set of Gödel-formulas of PA

**Definition:** We define a formula of PA, say  $[(\forall x)R(x)]$ , as a Gödel-formula of PA if, and only if:

- (i) both,  $[(\forall x)R(x)]$  and  $[\sim(\forall x)R(x)]$ , are not PA-provable;
- (ii) the PA-formula,  $[R(n)]$ , is PA-provable for every substitution of a term, say  $[n]$ , of PA, for the variable  $[x]$ , of PA, in the PA-formula  $[R(x)]$ .

It now follows that, if the set, say  $G(\text{PA})$ , of the Gödel-formulas of PA, is non-empty, and, both,  $[(\forall x)R(x)]$  and  $[\sim(\forall x)R(x)]$ , are PA-unprovable, then:

- (a) addition of  $[(\forall x)R(x)]$  as an axiom to PA would, first, not invite inconsistency; and, second, if  $\text{PA}+[(\forall x)R(x)]$  can be interpreted in a recursively definable language L to yield a non-trivial, non-standard, model of PA, then Corollary 1.2 would imply that the interpretation of  $[R(x)]$  in L itself interprets - over some model K of L - as a number-theoretic relation that is Turing-decidable as TRUE in  $M^7$ .

---

<sup>7</sup> The argument is not that either of M,  $M^*$  is a model of  $\{\text{PA}+[(\forall x)R(x)]\}$ , but that we can define  $Bw(x)$ ,  $Sb(p(x, y, \dots))(a, b, \dots)$ , and  $xBy$  for  $\{\text{PA}+[(\forall x)R(x)]\}$  such that, by Corollary 1.2,  $[R(x)]$  interprets as a TRUE Turing-decidable relation, in any recursively definable model, say  $M^{**}$ , of  $\{\text{PA}+[(\forall x)R(x)]\}$ , over the natural numbers that correspond - in the domain of  $M^{**}$  - to the numerals of  $\{\text{PA}+[(\forall x)R(x)]\}$ .

Thus, if the theorem,  $[(\forall x)R(x)]$ , of  $\{\text{PA}+[(\forall x)R(x)]\}$ , interprets as the theorem,  $[(\forall x)((x \in \omega) \rightarrow R(x))$ , in some non-trivial, non-standard, interpretation, say  $M^{**}$ , of PA, then, by Corollary 1.2, this implies that the arithmetical relation,  $R(x)$ , is Turing-decidable as TRUE over  $\omega$ .

Similarly, if the theorem,  $[\sim(\forall x)R(x)]$ , of  $\{\text{PA}+[\sim(\forall x)R(x)]\}$ , interprets as the theorem,  $[\sim(\forall x)((x \in \omega) \rightarrow R(x))$ , in some, non-trivial, non-standard interpretation, say  $M^{***}$ , of PA, then, by Corollary 1.2 - and Tarski's definitions of the satisfiability and truth of the formulas of a language under an interpretation - this implies that the arithmetical relation,  $R(x)$ , is not Turing-decidable as TRUE over  $\omega$ .

- (b) addition of  $[\sim(\forall x)R(x)]$  as an axiom to PA would, first, not invite inconsistency; and, second, if  $PA+[(\sim \forall x)R(x)]$  can be interpreted in a recursively definable language  $L'$  to yield a non-trivial, non-standard, model of PA, then Corollary 1.2 would imply that the interpretation of  $[R(x)]$  in  $L'$  itself interprets, over some model  $K'$  of  $L'$  - as a number-theoretic relation that is not Turing-decidable as TRUE in  $M$ .

Since we cannot have a number-theoretical relation which can be interpreted as both Turing-decidable as TRUE in  $M$ , and NOT Turing-decidable as TRUE in  $M$ , it follows that:

**Theorem 2:** If PA is consistent, then PA has no non-standard model, and  $G(PA)$  is empty.

## 5. Conclusions

- (i) There are no formally undecidable arithmetical propositions.
- (ii) There are no non-standard models of PA.
- (iii)  $P \neq NP$ .

## Appendix A: Logical Symbols, Axioms, and Rules of Inference of PA

The primitive logical symbols of PA are:

$\rightarrow$        $\&$        $\vee$        $\sim$        $\forall$        $x, y, \dots$        $a, b, \dots$

implies      and      or      not      for all      variables      constant terms

If  $A, B, C$  are well-formed formulas of PA, then the logical axioms of PA are:

- (1)  $A \rightarrow (B \rightarrow A)$ ;

- (2)  $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C));$
- (3)  $(\sim B \rightarrow \sim A) \rightarrow ((\sim B \rightarrow A) \rightarrow B);$
- (4)  $(\forall x)A(x) \rightarrow A(t)$ , if  $A(x)$  is a well-formed formula of PA, and  $t$  is a term of PA free for  $x$  in  $A(x)$ ;
- (5)  $(\forall x)(A \rightarrow B) \rightarrow (A \rightarrow (\forall x)B)$ , if  $A$  is a well-formed formula of PA containing no free occurrences of  $x$ .

The rules of inference of PA are:

- (i) Modus Ponens:  $B$  follows from  $A$  and  $A \rightarrow B$ ;
- (ii) Generalisation:  $(\forall x)A$  follows from  $A$ .

By Tarski's definitions of the satisfiability and truth of the formulas of PA under an interpretation, when the rules of inference are applied to true well-formed formulas of PA under a given interpretation, then the results of these applications are also true (i.e., every theorem of PA is true in any model of PA).

## Appendix B: Primitive Symbols and Proper Axioms of PA

- (a) PA has a single predicate letter,  $A^2_1$  (as usual, we write “ $t = s$ ” for  $A^2_1(t, s)$ );
- (b) PA has one individual constant  $a_1$  (written, as usual, “0”);
- (c) PA has three function letters  $f^1_1, f^2_1, f^2_2$ . We shall write “ $t'$ ” instead of  $f^1_1(t)$ ; “ $t+s$ ” instead of  $f^2_1(t, s)$ ; and “ $t*s$ ” instead of  $f^2_2(t, s)$ .

The proper axioms of PA are:

- (S1)  $(x_1 = x_2) \rightarrow ((x_1 = x_3) \rightarrow (x_2 = x_3));$

$$(S2) \quad (x_1 = x_2) \rightarrow (x_1' = x_2');$$

$$(S3) \quad 0 \neq (x_1)';$$

$$(S4) \quad ((x_1)' = (x_2)') \rightarrow (x_1 = x_2);$$

$$(S5) \quad (x_1 + 0) = x_1;$$

$$(S6) \quad (x_1 + x_2)' = (x_1 + x_2)';$$

$$(S7) \quad (x_1 * 0) = 0$$

$$(S8) \quad (x_1 * (x_2)') = ((x_1 * x_2) + x_1);$$

(S9) For any well-formed formula  $F(x)$  of PA:

$$F(0) \rightarrow ((\forall x)(F(x) \rightarrow F(x')) \rightarrow (\forall x)F(x)).$$

### **Appendix C: The standard interpretation, M, of PA ([Me64], p107)**

The standard interpretation, M, of PA, is taken to be the intuitive arithmetic of the natural numbers, as expressed by Dedekind's semi-axiomatic formulation of the Peano

Postulates, where:

- (i) the integer 0 is the interpretation of the PA-symbol “ 0 ”;
- (ii) the successor operation (addition of 1) is the interpretation of the PA-symbol “ ’ ”;
- (iii) ordinary addition and multiplication are the interpretations of the PA-symbols “ + ” and “ \* ”;
- (iv) the interpretation of the PA-symbol “ = ” is the identity relation.

## References

- [Go31a] Gödel, Kurt. 1931. *On formally undecidable propositions of Principia Mathematica and related systems I*. Translated by Elliott Mendelson. In M. Davis (ed.). 1965. *The Undecidable*. Raven Press, New York.
- [Me64] Mendelson, Elliott. 1964. *Introduction to Mathematical Logic*. Van Norstrand, Princeton.
- [Ra02] Raz, Ran. 2002.  $P \neq NP$ , Propositional Proof Complexity, and Resolution Lower Bounds for the Weak Pigeonhole Principle. *ICM 2002, Vol. III*, 1–3.