P v.s. NP problem

Hideto Ishihara

November 12, 2016

Department of Mathematics, Graduate School of Science, Kyoto University
e-mail: h.isihara26@gmail.com

Abstract

Let the class P be the set of problems that are solved in polynomial
time and the class NP the set of problems that are checked in polynomial
time. We show that the class NP is not equal to the class P. The problem
is well-known as P v.s. NP problem. Our proof is a new approach. Hilbert
program is used.

Keywords: P v.s. NP problem, Hilbert program

1 Introduction

For Turing Machine (see [7]) the class P is defined as the set of problems that are
solved in polynomial time and the class NP is defined as the set of problems that
are checked in polynomial time (see [2]). The class P or NP is also defined with
the use of deterministic or nondeterministic Turing Machines. The following is
well-known as P v.s. NP problem (see e.g. [1]).

Theorem 1. The class NP is not equal to the class P.

A P-(resp. NP-)problem is a computational problem in the class P (resp.
NP). We construct a sequence of configurations of a nondeterministic Turing
Machine solving an NP-problem that is not a sequence of configurations of a
deterministic Turing Machine solving a P-problem and then prove the class NP
is not equal to the class P.

The proof proceeds as follows. First as mentioned above we shall construct
a sequence of configurations of a nondeterministic Turing Machines solving an
NP-problem.

Let ǂ be not in the input alphabet. First take a deterministic algorithm A solv-
ing a P-problem with all inputs are solutions. Assume ǂ does not appear in the
algorithm A. We construct an algorithm \(P_A\) from A in which we obtain \(x\#x\)
from the input \(x\) and then perform A to the latter \(x\) to obtain \(x\#1\). We construct
a nondeterministic algorithm $NP_A$ in which we perform $P_A$ to the input $x$ and then obtain $x$ or 1 (or possibly both) from $x \notin 1$. We say that two sets are not separated by deterministic Turing Machines solving P-problems if they are not separated by any deterministic Turing Machines solving P-problems. If a nondeterministic transition function solving an NP-problem has sets of outputs not separated by deterministic Turing Machines solving P-problems there exists an NP-problem which is not solved by a deterministic transition function and we are done. Two sets are indistinguishable if they are not separated by a formula of ZFC. Select at least in two ways $x$ or 1 (or possibly both) at the branches so that the resulting sets are indistinguishable. This is possible because (super) $\mathbb{R}$ is uncountable. The indistinguishable branches are contained in a set of those solving the same NP-problem not separated by deterministic Turing Machines solving P-problems. The NP-problem of the corresponding nondeterministic transition function is a desired one.

From above there exists an NP-problem that is not solved by a deterministic Turing Machine in polynomial time. Hence we conclude that the class NP is not equal to the class P. The assertion follows.

In [3] we established the foundation of mathematics virtually perfectly (we describe it in detail in this paper): It is virtually perfect to assume least restrictive assumptions with no troubles with experiments (Hilbert program). We remark that in defining the notions of length and size of an algorithm we assumed the logic outside ZFC and it is justified by Hilbert program virtually perfectly.

2 CA-concepts (history (review))

We develop CA-model theory and introduce CA-concept. CA-model theory detects the change of (CA-)models and a CA-scientific (resp. social) concept is a definition that is preserved under any change of CA-models (resp. not preserved under a change of CA-models).

**Definition 2.** CA-alphabet consists of

1. constant symbols $\bar{c}_1^\Lambda, M_\lambda, (\lambda \in \Lambda \text{ and } \Lambda \text{ is a finite set}), \bar{M}_{\lambda}^{\Theta^\lambda}, R_{\lambda^\Theta} (\theta^\lambda \in \Theta^\lambda \text{ and } \Theta^\lambda \text{ is a set}), (M_\lambda, R_{\lambda^\Theta})_{\lambda \in \Lambda}, \prod \{M_\lambda\}, (M_\lambda, R_{\lambda^\Theta})_{\lambda \in \Lambda} \leq (\delta \in \Delta \text{ and } \Delta \text{ is a set})$

2. individual variables $x_0^\Lambda, x_1^\Lambda, \ldots$

3. predicate symbols $\bar{e}_r, =_r, T_r, X_r$

4. function symbols (of type $\bar{\tau}_n \rightarrow \sigma (\tau_0, \sigma \neq 0)$) $\bar{f}_j (j \in J \text{ and } J \text{ is a set})$

5. logical symbols $\neg, \land, \lor, \rightarrow, +, \forall r, \exists r, \bot$

and

6. auxiliary symbols ( ), [ ].

**Remark 3.** $\bar{f}_j$ is a function symbol of $A_j (1 \leq A_j < \infty)$ variables.
Definition 4. TERM is the smallest set $X$ with the following properties. An element of TERM is called a term.
(1) Constant symbols of type $\neq o$ and individual variables of type $\neq o$ are elements of $X$
(2) $t_1, \ldots, t_{A_i} \in X$ are of type $\tau_1, \ldots, \tau_{A_i}$ and $f_j$ is of type $(\tau_{A_j}) \rightarrow \sigma \Rightarrow f_j((t_{A_j})) \in X$ is of type $\sigma$

Definition 5. FORM is the smallest set $X$ with the following properties. An element of FORM is called a formula.

Remark
Formulas are said to be of type $o$.
(1) $\bot \in X$
constant symbols of type $o \in X$
individual variables of type $o \in X$
t_1, t_2 of type $\tau \Rightarrow (t_1, t_2) \in X$
t_1, t_2 of type $\tau \Rightarrow (t_1 \equiv t_2) \in X$
t of type $\tau \Rightarrow T_\tau(t), X_\tau(t) \in X$
s of type $(\tau_1, \ldots, \tau_n)$ and $t_1, \ldots, t_n$ of type $\tau_1, \ldots, \tau_n \Rightarrow s(t_1, \ldots, t_n) \in X$

Note: These formulas are said to be atomic.
(2) $\phi, \psi \in X \Rightarrow (\phi \land \psi) \in X$ (where $\land = \land, \lor, \rightarrow, \leftrightarrow$)
(3) $\phi \in X \Rightarrow \neg \phi \in X$
(4) $\phi \in X \Rightarrow \forall x^T_\tau \phi, \exists x^T_\tau \phi \in X$

Definition 6. A formula is primitive if it is constructed from variables, $\{\in_\tau\}_\tau$, $\land, \lor, \rightarrow, \leftrightarrow, \neg, \{\forall_\tau\}, \{\exists_\tau\}$. (Variables of type $o$ are not involved.)

Definition 7. The set $FV(\phi)$ of free variables of a formula $\phi$ and the set $FV(t)$ of free variables of a term $t$ are defined by the following.
(1) $FV(x^T_\tau) := \{x^T_\tau\}$
$FV(c) := \phi$ if $c$ is a constant symbol
(2) $FV(f_j((t_{A_j}))) := \bigcup FV(t_{A_j})$
(3) $FV(t_1 \equiv t_2) = FV(t_1 \in t_2) := FV(t_1) \cup FV(t_2)$
$FV(T_\tau(t)) = FV(X_\tau(t)) := FV(t)$
$FV(s(t_1, \ldots, t_n)) := FV(s) \cup \bigcup FV(t_i)$
$FV(\bot) := \phi$
(4) $FV(\phi \land \psi) := FV(\phi) \cup FV(\psi)$ (where $\land = \land, \lor, \rightarrow, \leftrightarrow$
(5) $FV(\neg \phi) := FV(\phi)$
(6) $FV(\forall x^T_\tau \phi) = FV(\exists x^T_\tau \phi) := FV(\phi) \setminus \{x^T_\tau\}$

Definition 8. A bounded variable is a variable that is not free.

Definition 9. (CA-structure)
A CA-structure $M = (\{M_\lambda, R_{\lambda, \delta}\}_{\lambda \in \Lambda}, \leq_\delta)$ consists of the following.
(1) sets
$E_\sigma = \{0, 1\}$
$E_i(\neq \phi)$
$E_\tau = \mathcal{P}(E_{\tau_1} \times \cdots \times E_{\tau_n}) \tau = (\tau_1, \ldots, \tau_n)$ \textit{(power set)}

(2)
sets $M_\lambda, \lambda \in \Lambda$ \textit{(is a finite set)}
$E_i = \bigcup M_\lambda$

(3) a set $\tau \subset E_\tau \times E_\tau$

(4) a fixed set $X_i$ with the following properties
(a) It is proved that $X^0_i$ exists uniquely in ZFC.
(b) $X^0_i \subset X_i$
(c) $x \in X_i \land y \in x \rightarrow y \in X_i$
(d) $X_i$ is the smallest set with the above two properties

$X_\sigma = \{0, 1\}$
$X_\tau = \mathcal{P}(X_{\tau_1} \times \cdots \times X_{\tau_n}) \tau = (\tau_1, \ldots, \tau_n)$

(3) functions $F_j$ \textit{(} $X_j$ \textit{variables, of type $(\tau_{a_j}) \rightarrow \sigma$)} from $\prod_{1 \leq a_j \leq X_j} (E_{\tau_j} \cup X_{\tau_j})$
to $E_\sigma \cup X_\sigma$

(6)
$c^*_i$ elements in $E_\tau$
$M_\lambda$ elements in $E_{(i)}$
$M^{N_{\lambda, a^\lambda}}_\lambda \text{ elements in } E_{(i, \ldots, t)}$
$R_{\lambda, a^\lambda}$ elements in $E_{(i, \ldots, t)}$

$(M_\lambda, R_{\lambda, a^\lambda}) \prod_{\lambda \in \Lambda} \{M_\lambda\} \text{ elements in } E_{(i)}$
$(M_\lambda, R_{\lambda, a^\lambda})_{\lambda \in \Lambda, \substack{i \\ \leq \delta}} \text{ elements in } E_{(i, \ldots, (t))}$

(7) $\in_\tau \subset (E_\tau \cup X_\tau) \times (E_\tau \cup X_\tau)$ is a restriction of $\in$ in ZFC.

\textbf{Remark 10.} (1) Each $M_\lambda$ is called an universe.
(2) Each $R_{\lambda, a^\lambda}$ is called a relation in $M_\lambda$.
(3) Each $\leq \delta$ is called a relation among $(M_\lambda, R_{\lambda, a^\lambda})_{\lambda \in \Lambda}$.

\textbf{Definition 11.} A closed formula or a sentence is a formula without free variables.
A set $\Gamma$ of axioms is a set of sentences.

\textbf{Definition 12.} Where $t$ is a term of type $\tau$, for a formula $\varphi, \varphi[t/x^*_i]$ is defined by the following.

(1)

\begin{equation}
\varphi[t/x^*_i] := \begin{cases} 
    y^* i' & \text{if } y^* i' \neq x^*_i \\
    t & \text{if } y^* i' = x^*_i,
\end{cases}
\end{equation}
where $y_i^{\tau'}$ is a variable of type $\tau'$, and
\[ c^{\tau'}[t/x_i^\tau] := c^{\tau'}, \]
where $c^{\tau'}$ is a constant of type $\tau'$.

(2) $f_i((t_{a_i}))[t/x_i^\tau] := f_i((t_{a_i}[t/x_i^\tau]))$ (3) $\perp[t/x_i^\tau] := \perp$
\[ T_{\tau'}(t_1)[t/x_i^\tau] := T_{\tau'}(t_1[t/x_i^\tau]) \]
\[ X_{\tau'}(t_1)[t/x_i^\tau] := X_{\tau'}(t_1[t/x_i^\tau]) \]
\[ (t_1 =_{\tau'} t_2)[t/x_i^\tau] := t_1[t/x_i^\tau] =_{\tau'} t_2[t/x_i^\tau] \]
\[ (t_1 <_{\tau'} t_2)[t/x_i^\tau] := t_1[t/x_i^\tau] <_{\tau'} t_2[t/x_i^\tau] \]
\[ s(t_1, \ldots, t_n)[t/x_i^\tau] := s[t/x_i^\tau](t_1[t/x_i^\tau], \ldots, t_n[t/x_i^\tau]) \]

(4) $\phi \land \psi[t/x_i^\tau] := (\phi[t/x_i^\tau]) \land (\psi[t/x_i^\tau]) \quad \phi \lor \psi[t/x_i^\tau] := (\phi[t/x_i^\tau]) \lor (\psi[t/x_i^\tau])$

(5) $\forall_{\tau'} y \phi[t/x_i^\tau] := \begin{cases} \forall_{\tau'} y \phi[t/x_i^\tau] & \text{if } x_i^\tau \neq y^{\tau'} \\ \forall_{\tau'} x_i^\phi & \text{if } x_i^\tau = y^{\tau'} \end{cases}$

(6) $\exists_{\tau'} y \phi[t/x_i^\tau] := \begin{cases} \exists_{\tau'} y \phi[t/x_i^\tau] & \text{if } x_i^\tau \neq y^{\tau'} \\ \exists_{\tau'} x_i^\phi & \text{if } x_i^\tau = y^{\tau'} \end{cases}$

where $t$ is of type $\tau$.

**Remark 13.** We define $\phi[t/x_i^\tau]$ for a formula $t$ in the same way.

**Definition 14.** The language $L(M)$ of a CA-structure $M = ((M_\lambda, R_{\lambda\beta}), \leq_\delta)$ consists of:
- as predicate constants $=_{\tau}, \in_{\tau}, T_{\tau}, X_{\tau}$;
- as function symbols $F_i$;
- as constant symbols $a (a \in \mathcal{U})$,
\[ c_i, c_i^\kappa, M_\lambda, M_\lambda^{N_{\lambda\alpha}}, R_{\lambda\beta}, (M_\lambda, R_{\lambda\beta})_{\lambda \in \Lambda}, (M_\lambda, R_{\lambda\beta})_{\lambda \in \Lambda}, \leq_\delta, \prod(M_\lambda). \]
Here, $\mathcal{U}$ is the universe of $M$ as an ordinary structure. The language $L$ consists of the same sets but constant symbols $a$, which are not constituents of $L$.

**Definition 15.** A closed term is a term without free variables. The interpretation of the closed terms of $L(M)$ is the following map $^\tau M : \text{TERM}_c \rightarrow \mathcal{U}$.

(1) $^a M := c, \overset{\bar{a}}{M} := a$
(2) $(F_i((t_{a_i})))^M := F_i((t_{a_i}^M))$

**Definition 16.** Let $\text{SENT}$ be the set of sentences. The interpretation of a sentence $\phi$ of $L(M)$ in $M$ is the following map $^\tau M : \text{SENT} \rightarrow \{0, 1\}$.

(1) $^\perp M = 0$
(2) $^P M := P$ (P is a constant of type 0)
(2) We denote $t^M := [t]_M$ for a sentence $t$.

$$[t_1 = t_2]^M := \begin{cases} 1 & \text{if } t_1^M =_t t_2^M \text{ and } t_1^M, t_2^M \in E_t \cup X_t \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

$$[t_1 \in t_2]^M := \begin{cases} 1 & \text{if } t_1^M \in \tau t_2^M \text{ and } t_1^M, t_2^M \in E_t \cup X_t \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

$$[T_\tau(t)]_M := \begin{cases} 1 & \text{if } t^M \in E_t \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

$$[X_\tau(t)]_M := \begin{cases} 1 & \text{if } t^M \in X_t \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

$$[s(t_1, \ldots, t_n)]_M := \begin{cases} 1 & \text{if } (t_1^M, \ldots, t_n^M) \in s^M \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

(3)

$$[\varphi \land \psi]_M := \min([\varphi]_M, [\psi]_M)$$

$$[\varphi \lor \psi]_M := \max([\varphi]_M, [\psi]_M)$$

$$[\varphi \rightarrow \psi]_M := \max(1 - [\varphi]_M, [\psi]_M)$$

$$[\neg \varphi]_M := 1 - [\varphi]_M \quad (4)$$

$$[\forall x \varphi]_M := \min\{[\varphi[a/x]]_M \mid a \in E_t \cup X_t\}$$

$$[\exists x \varphi]_M := \max\{[\varphi[a/x]]_M \mid a \in E_t \cup X_t\} \quad (1)$$

Definition 17. Let $\Lambda = \{\lambda_1, \ldots, \lambda_N\}$. $\Gamma'$ is defined by the following.

(1) $\bot$

(2) $\forall x, y \forall \tau_1, z_1 \ldots \forall \tau_n, z_n [(x(z_1, \ldots, z_n) \leftrightarrow y(z_1, \ldots, z_n)) \rightarrow x =_\tau y] \quad (\tau = (\tau_1, \ldots, \tau_n))$

$\forall x, y [(x \leftrightarrow y) \rightarrow x =_\tau y]$

(3) $\forall \sigma, x_1 \ldots \forall \sigma, x_m \exists y \forall \tau_1, z_1 \ldots \forall \tau_n, z_n [y(z_1, \ldots, z_n) \leftrightarrow \varphi]$, where $\tau = (\tau_1, \ldots, \tau_n)$, $FV(\varphi) \subset \{x_1, \ldots, x_m, z_1, \ldots, z_n\}$ and $\varphi$ is a formula.

(4) $\tau = (\tau_1, \ldots, \tau_n, \tau_{n+1})$

$\forall \tau_1 \exists \tau_2 \forall x_1, \ldots, \forall x_n, \exists n+1, y, z_1(x_1, \ldots, x_n, y) \rightarrow \exists n+1, y, z(x_1, \ldots, x_n, y)]$

(5) $\forall x_1 \ldots \forall x_{\lambda x^\alpha} (R_{\lambda x^\alpha}(x_1, \ldots, x_{\lambda x^\alpha}) \rightarrow M_{\lambda x^\alpha}(x_1, \ldots, x_{\lambda x^\alpha}))$

(6) $\forall x_1 \ldots \forall x_{L_{\lambda x^\alpha}} (x_1, \ldots, x_{L_{\lambda x^\alpha}}) \rightarrow M_{\lambda x^\alpha}(x_1, \ldots, x_{L_{\lambda x^\alpha}})$

(7) $\forall x((M_{\lambda x^\alpha} \wedge \lambda \in \Lambda(x \leftrightarrow \bigwedge \{M_{\lambda x^\alpha} \mid \lambda \in \Lambda\} \ (\text{in an abuse of notation})$

(8) $\forall x_1 \ldots \forall y_{\lambda x^\alpha}(M_{\lambda x^\alpha}(y_1, \ldots, y_{\lambda x^\alpha}) \rightarrow \bigwedge y_{\lambda x^\alpha}(y_j])$
\( \forall x \gamma(x) \) is an individual variable of type \( \tau \)

**Definition 18.** For a formula \( \gamma \), \( \gamma^T \) is defined by the following.

1. \( \gamma^T := \varphi \) if \( \varphi \) is atomic
2. \( (\varphi \land \psi)^T := \varphi^T \land \psi^T \) \( (\varnothing = \land, \lor, \rightarrow, \leftrightarrow) \)
3. \( \neg \varphi^T := \neg (\varphi^T) \)
4. \( (\forall x \varphi)^T := \forall x \varphi^T \) \( (x = T, x \in X_\tau, \in) \)
5. \( (\exists x \varphi)^T := \exists x \varphi^T \) 

Let \( \Gamma \) be a set of sentences without \( X_\tau, \in \). Then defining

\[ \Gamma^T := \{ \gamma^T \mid \gamma \in \Gamma \} \]

\( \Gamma^T \cup \Gamma' \) is denoted by \( \Gamma \) (in an abuse of notation).

**Definition 19.** A CA-structure \( \mathbb{M} \) is a CA-model of a sentence \( \varphi \) if

\[ [\varphi]_{\mathbb{M}} = 1. \]

In this case we write \( \mathbb{M} \models \varphi \). A CA-structure \( \mathbb{M} \) is a CA-model of the axioms \( \Gamma \) if

\[ \varphi \in \Gamma \Rightarrow [\varphi]_{\mathbb{M}} = 1. \]

In this case we write \( \mathbb{M} \models \Gamma \). We write \( \models \varphi \) if \( \varphi \) holds. We write \( \Gamma \models \varphi \) (\( \varphi \) is a sentence) if

\[ \mathbb{M} \models \Gamma \Rightarrow \mathbb{M} \models \varphi. \]

**Remark 20.** CA-models were thought up to examine the change of models.

**Definition 21.** Where \( t \) is a term or a formula and \( x \) is an individual variable, \( t \) is free for \( x \) for a formula \( \varphi \) if

1. \( \varphi \) is atomic;
2. \( \varphi := \varphi_1 \square \varphi_2 \) or \( \neg \varphi_1 \square = \land, \lor, \rightarrow, \leftrightarrow \) and \( t \) is free for \( x \) in \( \varphi_1 \) \( (\text{and } \varphi_2) \); 
3. \( \varphi := \forall x \psi \) or \( \forall x \psi, y \notin FV(t) \) and \( t \) is free for \( x \) in \( \psi \), where \( x \neq y \).

**Definition 22.** We introduce the following derivation rules into formulas of a fixed language.

1. (1)
\[
\frac{\phi(x^+_i)}{\forall x^+_i \phi(x^+_i)}
\]

\( x^+_i \) is not free in any assumption before \( \phi(x^+_i) \)
\((2)\)

\[
\frac{\forall x^+_i \phi(x^+_i)}{\phi(t)}
\]

t is of type \( \tau \) and free for \( x^+_i \) in \( \varphi \)
\((3)\)

\[
\frac{\varphi(t)}{\exists x \phi(x)}
\]

t is of type \( \tau \) and \( x \) is a variable of type \( \tau \)
\((4)\)

\[
\exists \tau, x \phi(x) \quad \psi
\]

Remark 23. The other derivation rules are defined naturally.

Definition 24. Let \( \Gamma \) be a set of formulas and \( \varphi \) a formula. If \( \varphi \) is obtained from \( \Gamma \) by a finite number of applications of derivation rules, we say that there exists a derivation from \( \Gamma \) to \( \varphi \) and write

\[ \Gamma \vdash \varphi. \]

Definition 25. For the set \( \text{FORM}_{\text{prim}} \) of primitive formulas, a (class) function \( F' : \{ \varphi | \varphi \in \text{FORM}_{\text{prim}} \} \rightarrow \{ \text{well-formed formulas} \} \) is defined by the following.

1. \( F'(\varphi(x \in y)) := x \in y \)
2. \( F'(s(t_1, \ldots, t_n)) := (t_1, \ldots, t_n) \in s, \)
   where \( s, t_1, \ldots, t_n \) in LHS and those in RHS are suitable variables.
3. \( F'(\varphi \sqcap \psi) := F'(\varphi) \sqcap F'(\psi) \quad \sqcap = \land, \lor, \rightarrow, \leftrightarrow \)
4. \( F'(\neg \varphi) := \neg F'(\varphi) \)
5. \( F'(\forall x \phi(x)) := \forall x (x \in X \rightarrow F'(\phi(x))) \)
6. \( F'(\exists x \phi(x)) := \exists x (x \in X \land F'(\phi(x))) \)

Discussion 26. Let \( X_i \) be a set such that for a wff \( \psi \) of ZFC such that

\[ \text{ZFC} \vdash \exists ! x \psi(x), \]

true is that

\[ [\psi(x)[X_i/x]]_{\text{ZFC}} = 1. \]
For a primitive formula $\varphi$, $\varphi^X$ is defined by the following.

1. $(x \in y)^X := x \in y$
2. $(s(t_1, \ldots, t_n))^X := s(t_1, \ldots, t_n)$

where $s, t_1, \ldots, t_n$ are suitable variables.

2. $(\varphi \land \psi)^X := \varphi^X \land \psi^X$ ($\land = \land, \lor, \rightarrow, \leftrightarrow$)
3. $(\neg \varphi)^X := \neg \varphi^X$

(4) $(\forall x \varphi)^X := \forall x(\bar{X}_r(x) \rightarrow \varphi^X)$
(5) $(\exists x \varphi)^X := \exists x(\bar{X}_r(x) \land \varphi^X)$

For a primitive formula $\varphi$, we consider $\varphi^X \mapsto \mathcal{F}(\varphi)$ (a class function). For $\varphi^X$, the condition $\nabla_\tau$ is given by

$\nabla_\tau : \text{ZFC} \vdash \forall \mathcal{X}_\tau[\psi(\mathcal{X}_\tau) \rightarrow \exists! y(y \in \mathcal{X}_\tau \land \mathcal{F}(\varphi)(y))]$ (in an abuse of notation) holds true.

**Definition 27.** Define $D_0 = \{0, 1\}$

$D_\tau = M_{\lambda_1} \ldots M_{\lambda_N}$ or $M_{\lambda_N}$

$D_\tau = \mathcal{P}(D_{\tau_1} \times \ldots \times D_{\tau_n})$ $\tau = (\tau_1, \ldots, \tau_n)$.

In the definition of $D_\tau$, each $D_i$ is chosen independently. (We write one of such by $D_\tau$.)

**Definition 28.** For a CA-structure $\mathcal{M}_\tau$, we define $\mathcal{M}_R$ to be $\mathcal{M}$ together with a relation $R(\subset D_\tau^{R_n})$ in $D_\tau$. Assume there exists a constant symbol $\bar{D}_\tau$ corresponding to $D_\tau$. Let $\Gamma$ be a set of axioms. Below for $\gamma$, we assume the following holds.

$\Gamma \vdash \forall \tau x_1 \ldots \forall \tau x_m[\gamma(x_1, \ldots, x_m) \rightarrow \bigwedge_j \bar{D}_\tau(x_j)]$

$R$ is a definition defined by $\gamma$ of a particular CA-model $\mathcal{M}_0$ if on the language with a constant $\bar{R}$ as an element of the CA-alphabet, true is

$\mathcal{M}_0^R \models \forall \tau x_1 \ldots \forall \tau x_m(\bar{R}(x_1, \ldots, x_m) \leftrightarrow \gamma(x_1, \ldots, x_m))$.

Remark 29. Any constant of type $\tau$ ($\neq i, o$) is used instead of $\bar{D}_\tau$. More general argument is possible.

**Definition 30.** Note that for any CA-model of a set $\Gamma$ of axioms, there exists a definition defined by $\gamma$.

$\{R\}$ is a CA-scientific concept if the following holds.

1. Each $R$ is a definition defined by $\gamma$, that is, there exists $\mathcal{M}$ such that

$\mathcal{M} \models \Gamma$ and $\mathcal{M}_R \models \Gamma \cup \{\forall \tau x_1 \ldots \forall \tau x_m(\bar{R}(x_1, \ldots, x_m) \leftrightarrow \gamma(x_1, \ldots, x_m))\}$

hold and $\{R\}$ consists of all such definitions.

2. For each primitive formula $\varphi$ such that $\varphi^X$ satisfies $\nabla_\tau$, either

(a) for all CA-models $\mathcal{M}'$,

$\mathcal{M}_R' \models \forall \tau x[\bar{X}_r(x) \land \varphi^X(x) \land \bar{D}_\tau(x) \rightarrow \bar{R}(x)]$
holds, or 
(b) for all CA-models $M'$

$$M'_R \models \forall \tau x[X_\tau(x) \land \varphi^X(x) \land D_\tau(x) \to \neg R(x)]$$

holds.

**Definition 31.** In the same settings as Definition 30, a definition $\{R\}$ defined by $\gamma$ is a CA-social concept if $\{R\}$ is not a CA-scientific concept.

**Remark 32.** We often use another definition of CA-concepts such that $D_\tau(x)$ and $R(x)$ are replaced with $\forall \tau z(x(z) \to D_\tau(z))$ and $\forall \tau y(x(y) \to R(y))$.

**Remark 33.** From now on, we assume the constants $D_\tau$ etc. appearing in such arguments are chosen appropriately.

**Remark 34.** If a set $\Gamma$ of axioms has a CA-model in ZFC, $\Gamma$, or $\Gamma^T \cup \Gamma'$ is consistent provided that ZFC is consistent.

**Theorem 35.** Assume ZFC is consistent. Let $\Gamma$ be a consistent set of axioms. Add a predicate symbol $\bar{R}$ to the CA-alphabet. Assume each $R$ is a definition defined by $\gamma$. Let $\varphi$ be an arbitrary primitive formula such that $\varphi^X$ satisfies $\curvearrowright_x$. If one and only one of the following two conditions holds true for each choice of this (fixed) formula, $\{R\}$ is a CA-scientific concept.

1. $\Gamma \cup \{\forall \tau x(\bar{R}(x) \leftrightarrow \gamma(x))\} \vdash \forall \tau x[X_\tau(x) \land \varphi^X(x) \land \bar{D}_\tau(x) \to \bar{R}(x)]$
2. $\Gamma \cup \{\forall \tau x(\bar{R}(x) \leftrightarrow \gamma(x))\} \vdash \forall \tau x[X_\tau(x) \land \varphi^X(x) \land \bar{D}_\tau(x) \to \neg \bar{R}(x)]$

**Proof.** For any CA-model $M$ of $\Gamma$ and for any appropriate choice of $R$,

$$M_R \models \Gamma \cup \{\forall \tau x(\bar{R}(x) \leftrightarrow \gamma(x))\}$$

holds. Thus by assumption, any time

$$M_R \models \forall \tau x[X_\tau(x) \land \varphi^X(x) \land \bar{D}_\tau(x) \to \bar{R}(x)]$$

holds, or any time

$$M_R \models \forall \tau x[X_\tau(x) \land \varphi^X(x) \land \bar{D}_\tau(x) \to \neg \bar{R}(x)]$$

holds. Hence $\{R\}$ is a CA-scientific concept. \qed

**Corollary 36.** A CA-social concept can not be determined by $\Gamma$.

**Remark 37.** Intuitively, a CA-social concept is a definition which may exist, can not be determined and hence needs to be treated carefully in any argument.

### 3 CA-super concepts

Consider Higher Order Logic and its semantics. Write it down in the language of ZFC. We take as the real things the theorems on an arbitrary model derived from ZFC and the set-theoretic theorems corresponding to the formulation of HOL and the axioms. We call this theory CA-super model theory. The counterparts of CA-concepts are called CA-scientific or CA-social super concepts. All results in this paper related with CA-model theory are still true if we use CA-super model theory.
4 Definition of degree

Theorem 38. Let $X$, an universe, be a topological space constructed from $\phi$ uniquely. Then, the definitions $\mathbb{U} \subset X$ and $\mathbb{U}^c$ such that the set $\mathbb{U}$/the complement $\mathbb{U}^c$ is with an interior point are CA-social concepts.

Proof. We first prove the following.

Claim: The set of points which are shown to uniquely exist is dense in $X$.

Proof of Claim. Two sets are indistinguishable if they cannot be proved to be different. By taking the union of open sets that are indistinguishable, we obtain a fundamental system of neighbourhoods consisting of sets which is shown to uniquely exist. Thus it suffices to show that any topological space that is shown to uniquely exist has a point which is shown to uniquely exist. By well-ordering theorem, there exists a well-order which is shown to uniquely exist. (Take the union of indistinguishable well-orders.) Then, take the minimum element. 

Assume $\mathbb{U}$ is a CA-scientific concept. Fix a special standard CA-model that is shown to uniquely exist. Since $\mathbb{U}$ has an interior point, and the set of points which are shown to uniquely exist is dense in $X$, there exists a point $p \in \mathbb{U}$ that is shown to uniquely exist. Take $p' \in X$ which is shown to uniquely exist. Make another CA-model by interchanging these points. Then, by assumption, $p' \in \mathbb{U}$ in the standard one. Hence $\mathbb{U}$ contains a dense subset of $X$ in the standard CA-model but $\mathbb{U}^c$ is with an interior point: a contradiction. Hence $\mathbb{U}$ is a CA-social concept. A similar argument shows the other assertion.

In a (natural) physical theory with its universes given by topological spaces constructed from $\phi$ uniquely and possibly with some constants (CA-alphabet), it is suggested that the assumptions on $\mathbb{U}$ are virtually needed when we classify things by actual measurement (significant figure etc), that is, it is suggested that the impossibility of completely exact measurement and what we obtain by a measurement is a region with an interior point are sufficiently acceptable assumption. Intuitively, it is suggested that a physical definition should be related with the topological space $A$ that is experimentally measurable: there should exist a continuous function from $X$ (or $\mathbb{U}$) to $A$ (If it is not continuous, then, we introduce to $X$ the topology induced from the function and $A$). The image should be another definition. By the mentioned principle of measurement, this should be with an interior point and $\mathbb{U}$ should be. A natural dichotomous definition should correspond to $\mathbb{U} = X$ and there exists a continuous function. Thus, intuitively, the above theorem suggests that a natural (physical) dichotomous definition should be replaced with a definition of degree.

5 Learning

General physics: The following is stated intuitively. Assume we can construct a system of real numbers in the theory in problem. In theoretical physics, we
should take as many topological spaces constructed from $\phi$ uniquely as possible as the universes because the explanations of experiments are still the same. Then, the state corresponding to the selections of the parameters should be replaced with a function (solution) and the rules corresponding to the selections of the solutions should be replaced with the best function (Definition of degree). (Note: these are assumptions.) The assumptions on the state and the rules seem to be sufficiently acceptable. Applying a characteristic function of the region of the imaginary solutions to the best function, we obtain an equation $F$. Then the equation (The best function corresponds to $\{(t, \psi(t))_{\phi}, F(\psi)\}_{\phi}$, where $\psi$ is a solution.) naturally defines another best equation on the domain $T$ of the solution (The best function of the latter corresponds to $\{(t, (\psi(t), F(\psi)))_{\phi}\}_{\phi}$). Assume for simplicity $T$ is arcwise-connected (phase space time). Integrating the latter equation along curves, we obtain a conserved quantity. This possibly takes various values because we selected the best function. A CA-pseudoeenergy is such a quantity. Since, intuitively, it is suggested that the reactions we know are limited, the measurement is limited. In other words, the set of the complement of the set of the observed values of the CA-pseudoeenergy determined by the solution at a time (We assume the existence of the observer) is with an interior point (the limit of measurement). It is suggested that assuming this is thus sufficiently acceptable. On the other hand it is suggested that the distribution of the observed values of the CA-pseudoeenergy should be determined by a (state) function is sufficiently acceptable. (Intuitively, it is suggested that the reproducibility (see below) is necessary to explain the experiments; otherwise we cannot understand them.) Assuming that we have seen $I$ events in a region in problem among $L$ observations, thus, $\frac{1}{L}$ is convergent as $L \to \infty$; otherwise, the value is not determined as a nonnegative real number and we will lose the reproducibility. The distribution will be replaced with the probability one (the axioms of probability). Thus, we obtain a function expressing the observed values of the CA-pseudoeenergy (CA-pseudoquantization).

**Assumption:** Since in any (natural) physical theory having as many topological spaces constructed from $\phi$ uniquely as possible as the universes we should express the states of the object as functions, if the functions coincide, any (distribution of) physical quantities of it should coincide (reproducibility). In the above assumption that there exists an object that determines the distribution of the quantity is essential. By a similar argument as above any physical quantity is measured as a probability distribution if it is experimentally measurable.

We describe the brain mathematically. Intuitively it is suggested that the time a person remembers/does not remember something is with an interior point. Assuming this seems to be sufficiently acceptable. Then, memory with this intuition is not defined. We have to change our intuition.

**Term 39.** CA-pseudomemory is a structure (a solution of the fundamental equation of general physics) (of a brain).
The following is stated intuitively. We analyze the real world by this: a
definition that is derived from our concept of memory. (Our final goal should
be to explain the real world.) The concept is based on the following observation:
Intuitively it is suggested that the time when a person memorizes/does not
memorize a thing is with an interior point is sufficiently acceptable. By
Theorem 38 a person should memorize a thing any time. Further, intuitively
it is suggested that the set of particles is finite and this is sufficiently accept-
able, so a person should be replaced with a system, or all particles. We define
memorize a thing to be a happening of almost the same phenomena. It is sug-
gested that this will be sufficiently acceptable. By the reproducibility, thus, we
obtain that a person memorizes a thing by preserving the state of the brain.
That is, if the brain of a person remains almost the same or returns to almost
the same state, and if things surrounding it return to almost the same state,
or if the system returns to almost the same state, almost the same phenomena
happen (principle of memory).
Brain structure is the structure of a system with brain and a brain part is
an intuitive/classical part of an intuitive/classical brain (the former is a good
definition in physics and the latter is a set of values of physical quantities).

**Term 40. (CA-pseudocontrol)**
Consider the fundamental equation of general physics. A CA-pseudocontrol is a
trying to realize a solution in the target range giving conditions.

**Term 41.** Let $D$ be a region in the space of states where the substances $1, 2, \ldots, N'$
are in the desired states. The substances $1, 2, \ldots, N'$ has a high problem solving
ability for the input set $S$ if each element of $S$ is staying in $D$ for $T_0 \leq t \leq T_1$
($T_0 < T_1$). A solution $\Psi(t)$ is staying in $D$ for $T_0 \leq t \leq T_1$ if $\Psi(t) \in D$
($T_0 \leq t \leq T_1$).

Intuitively, it is suggested that if a person is stable with any trouble, then,
he/she has good problem solving ability.

**Discussion 42. (Learning Principle)** It is suggested that the possible states
of the brain structure are limited if the input (or environment) is determined. It
is thus suggested that the brain structure changes as long as it conflicts with the
input. If the inputs have patterns (or common physical quantities), it is then
suggested that the corresponding patterns are constructed in the brain structure.

Note that, intuitively, it is suggested that a person learns things so that she/he maximizes the problem solving ability for natural desired states (with
respect to realistic input sets).

There exist evidences for our learning theory. See e.g. [5] p16, [6]. The ex-
periments in [5], [6] are explained by the reproducibility easily. Here we use
the concepts of degree, so that it is sufficient that the experiment suggests the
tendency.
Remark 43. Throughout this paper we used intuitively, will etc. and assumed many things. With all we conclude that CA-concept is sufficiently acceptable and it then establishes our learning theory. Thus the above evidences are at the same time ones of the assumptions in this paper.

Remark 44. The above arguments are independent of CA-model theory.

6 Hilbert program

The following is stated intuitively. Even if we can construct the (super-)axiomatic set theory completely, our (super-)science predicts the incompleteness of the science (limit of measurement). It suggests that we should establish the (super-)axiomatic set theory and the (super-)science (or some (super-)theory) and modify them continuously so that the assumptions produce no troubles (by the above). By principle of memory, it is suggested that we classify things using the existing brain parts. Hence it is suggested that we should assume some assumptions to establish the (super-)axiomatic set theory (or the (super-)theory). Hilbert program is as follows (cf. [8]): We treat the mathematics as a formal system. Basically this program is thought up to establish the foundation of mathematics. The consistency will not be assessed but this formal method will be suggested to be carried out almost completely and will be suggested to have sufficient acceptability, that is, assuming least restrictive assumptions with no troubles with experiments is necessary and from many well-known experimental/statistical evidences it is shown that ZFC will be one of such.

For general physics, once we have obtained a (natural) theory of physics, Hilbert program is independent of CA-model theory.

7 Proof of Theorem

We prove the main theorem. Turing Machine is defined in [7], Chapter 3, Section 3.1, definition 3.3. We quote the definitions of the class P and NP (see [2], Chapter 2, Section 2.3.1, definition 2.4 and Section 2.6, definition 2.7).

Definition 45. We denote by P the class of decision problems that are efficiently solvable and by NP the class of sets that are each accepted by some nondeterministic polynomial time Turing Machine.

A P-(resp. NP-)problem is a computational problem in the class P (resp. NP).

Plan. First we shall construct a sequence of configurations of a nondeterministic Turing Machine solving an NP-problem that is not a sequence of configurations of a deterministic Turing Machine solving a P-problem.
Let $\xi$ be not in the input alphabet. Take a deterministic algorithm $A$ solving a P-problem with all inputs being solutions. Assume $\xi$ does not appear in any configurations in the algorithm $A$.

**Lemma 46.** There exists an algorithm $P_A$ from $A$ in which we obtain $x^\xi x$ from the input $x$ and then perform $A$ to the latter $x$ to obtain $x_{\xi 1}$.

*Proof.* Copy the input $x$, move the head to the right of $x$ and write $\xi$ and moving right write $x$. Move the head to the right of $\xi$ and perform $A$ to the latter $x$. Observe that such an algorithm exists for each one solving a P-problem. The assertion follows. □

**Lemma 47.** There exists a nondeterministic algorithm $NP_A$ in which we perform $P_A$ to the input $x$ and then obtain $x$ or $1$ (or possibly both) from $x_{\xi 1}$.

*Proof.* For the input $x$ perform the algorithm $P_A$ to obtain $x_{\xi 1}$. Delete $\xi 1$ or $x_{\xi}$ to obtain $x$ or $1$ (or possibly both). The resulting algorithm is a nondeterministic algorithm (distinct difference (see Remark 52)). The assertion follows. □

**Plan.** We shall prove that there exists an NP-problem that is not solved by a deterministic algorithm of finite description in polynomial time.

Two sets are not separated by deterministic Turing Machines solving P-problems if they are not separated by any deterministic Turing Machines solving P-problems.

If a nondeterministic transition function solving an NP-problem has sets of outputs not separated by deterministic Turing Machines solving P-problems there exists an NP-problem solved by a branch of the nondeterministic algorithm which is not solved by any deterministic transition function and we are done. We note that a deterministic algorithm solving one P-problem constructed from a branch of the NP-problem, if it exists, solves the others and that the conclusions of the P-problems corresponding to any branches of the nondeterministic algorithm are the same because they are not separated by deterministic Turing Machines solving P-problems.

Two sets are indistinguishable if they are not separated by a formula of ZFC.

**Lemma 48.** There exist at least two indistinguishable sets of outputs of $NP_A$.

*Proof.* Select at least in two ways $x$ or $1$ (or possibly both) at the branches so that the resulting sets are indistinguishable. This is possible because the (super) set of formulas of ZFC is countable and (super) $\mathbb{R}$ is uncountable. The assertion follows. □

The indistinguishable branches are contained in a set of those solving the same NP-problem not separated by deterministic Turing Machines solving P-problems. We note that defining such a set is carried out in ZFC and the
existence of a formula defining such is proved outside of ZFC. That is, if such
a set does not exist any branch is separated from the others by some determin-
istic Turing Machines solving P-problems, thus there exist no indistinguishable
branches (separated sets result in separated super sets). This is a contradiction.
The NP-problem solved by the corresponding nondeterministic transition func-
tion is a desired one.

Remark. The above argument does not work if we replace P and NP with
EXP and NP. (It is shown that trying to choose a deterministic algorithm
which solves such a branch results in a nondeterministic algorithm of the same
computational complexity.)

Remark 49. Here we used the distinct difference (see Remark 52).

Remark 50. Indistinguishable sets cannot be separated by a formula of ZFC.
This, however, is not saying that an indistinguishable set is not nonunique at
all in ZFC.

Remark 51. Here we used the sets outside ZFC.

Proof of Theorem 1. From above there exists an NP-problem that is not solved
by a deterministic Turing Machine in polynomial time. Hence we conclude that
the class NP is not equal to the class P. This shows the assertion. □

Remark 52. In the proof we used the distinct difference: the difference between
the class P and the class NP is that it is defined by deterministic algorithms or
by nondeterministic algorithms.

Remark 53. The proof used the sets outside ZFC and thus it is not complete
in ZFC (in particular in computer science or ordinary mathematics). Also it is
not related with the assertion that Theorem 1 is independent of ZFC. Further-
the distinct difference implies that generally without given additional condi-
tions we cannot specify a branch of a nondeterministic algorithm by any deter-
rministic algorithms.

Remark 54. The proof used Hilbert program in the following sense. Hilbert
program (see Section 6) asserts that it is virtually perfect to assume least re-
strictive assumptions with no troubles with experiments. It is well-known that
ZFC will be one of such. Furthermore assuming the sets outside ZFC is less re-
strictive than assuming ZFC only and it is well-known that it is with no troubles
with experiments.

Remark 55. The above solution and proof of P v.s. NP problem implies that
adding some necessary conditions may drastically ease the proof of a proposition.
Hence a hard problem may become an undergraduate level problem as time goes
by, especially just after it has been solved.
References

claymath.org/sites/default/files/pvsm.pdf [Accessed: 19th July 2016]


[5] Ochanomizu University, Heisei 25 nendo zenkoku gakuryoku chousa (kimekonakai chousa) no kekka wo katsuyou shita gakuryoku ni eikyou wo atau youin bunseki ni kansuru chousa kenkyuui (A study of analysis of factors for academic performance with the use of National academic ability survey 2013 (fine survey)), 2014

