INDEPENDENT PARTIAL CIRCUIT IN P VS NP PROBLEM

KOJI KOBAYASHI

Abstract. This paper describes about complexity of NP problems by using "Effective circuit", and divide class P and NP.

Inputs of circuit family that compute P problem have some symmetry that indicated circuit structure. To clarify this symmetry, we define "Effective circuit" as partial circuit which are necessary to compute target inputs. Effective circuit set divide problem to some symmetric partial problems.

The other hand, inputs of NTM that compute NP problem have extra implicit symmetry that indicated nondeterministic transition functions. To clarify this implicit symmetry, we define special DTM "Concrete DTM : Di"which index i correspond to selection of nondeterministic transition functions. That is, NTM split many different asymmetry DTM Di and compute all Di in same time.

Consider Di and effective circuit set, circuit family [SAT] that solve SAT problem have to include all effective circuit set [Di] that correspond to Di. [Di] have unique gate and [SAT] must include all [Di]. Number of [Di] is over polynomial size of input. Therefore, [SAT] is over polynomial size, and P is not NP.

1. Effective circuit set

Inputs of DTM circuit family that emulate DTM have some symmetry that indicated circuit structure. To clarify this symmetry, we define "Effective circuit" as partial circuit which are necessary to compute some inputs. Effective circuit set divide problem to some symmetric partial problems.

Definition 1.1. We use term as following;

$|x|$: Size of Input x

$C(x)$: Circuit C value when input is x.

SAT : Boolean satisfiability problems.

CVP : Circuit Value Problems

TM : Set of Turing Machine.

DTM : Set of Deterministic TM.

NTM : Set of Nondeterministic TM.

$\mathbb{N}$: Natural Number.

In this paper, we will use words and theorems of References [Sipser].

Definition 1.2. We will use the term "Effective circuit c in circuit C at input x" or "$c = [C(x)]$" as one of possible partial circuits which remove all ineffective gate one by one. "Ineffective gate" is gate that circuit keep value even if the gate invert output value.

We also use the term "Effective circuit set" or $[C(X)] = \{[C(x)] \mid x \in X\}$ as set of effective circuit $[C(x)]$ that correspond to input set X. Each circuit in effective circuit set accepts particular input x.

2. NP extra symmetry

The other hand, inputs of NTM which compute NP problem have extra implicit symmetry that indicated nondeterministic transition functions. NTM compute many configuration nondeterministicly. Each configuration means different DTM because these transition functions set are different and compute different results. That is, NTM split many different asymmetry indexed DTM and compute all DTM in same time.

To clarify this implicit symmetry, we define special DTM "Concrete DTM"which correspond to actual DTM in NTM.

Definition 2.1. We will use the term "Concrete DTM" or $D_i \in DTM$ of $N \in NTM$ as the DTM that fixed NTM nondeterministic transition functions selection to i. That is, i is list of nondeterministic transition functions, and D_i compute N

that nondeterministic transition functions select i order. "Concrete DTM set" or $D_I = \bigcup_{i \in I} D_i$ that $I \subset \mathbb{N}, |I| < k \in \mathbb{N}$ as disjunction of Concrete DTM.

For simplicity, i is Binary number that have 0 implicit filler $\mathbb{N} \ni i = \{0,1\}^{|i|} (+0^*)$, and if D_i does not use some of i to compute x, then $D_i(x) = 0$.

Theorem 2.2. $\forall N \in NP \left(N = \bigcup_i D_i \mid D_i \in P \right)$

Proof. It is trivial from Concrete DTM definition 2.1. □

3. Computing NP Problem with Circuit Family

Consider to solve $N \in NP$ with circuit family $\{C_i\} \in P$. N have extra implicit symmetry D_i, and $\{c_k\}$ is necessary to treat this symmetry to solve N because this extra implicit symmetry decide N result. Especially, D_i have some input x that $D_p(x) = 1$ and $D_{q \neq p}(x) = 0$, and some input y that $D_p(y) = D_q(y) = 0$. This means that each D_p is not include D_q.

Definition 3.1. We will use the term "Concrete CVP" or "CVP_i" as the Concrete DTM of SAT,

"CVP_I" that $I \subset \mathbb{N}, 0 < |I| < k \in \mathbb{N}$ as $\bigvee_{i \in I} CVP_i$,

"$[SAT]$" as circuit family that compute SAT,

"$[CVP_i]$" as effective circuit set of $[SAT]$ that compute $[CVP_i](x) = 1$ if $CVP_i(x) = 1$,

"$[CVP_I]$" that $I \subset \mathbb{N}, 0 < |I| < k \in \mathbb{N}$ as effective circuit set of $[SAT]$ that compute $[CVP_I](x) = 1$ if $CVP_I(x) = 1$.

Theorem 3.2. $\forall I, i \left(I \not\ni i \rightarrow \exists x \left((|x| < O(|i|)) \wedge (CVP_I(x) = 0) \wedge (CVP_i(x) = 1) \right) \right)$

Proof. It is trivial because some formula x with i and $q \in I$ become $x(i) = 1, x(q) = 0$ like $x(t) \equiv (t = i)$ and $|x| < O(|i|)$. □

Theorem 3.3. $\forall I, x \left(CVP_I(x) = 1 \rightarrow [CVP_I](x) = 1 \right)$

$\forall I, x \left([CVP_I](x) = 0 \rightarrow CVP_I(x) = 0 \right)$

Proof. It is trivial from definition 3.1. □

Theorem 3.4. $\forall I, i, x \left([CVP_I] \supseteq [CVP_i] \rightarrow [CVP_i](x) = 1 \rightarrow [CVP_I](x) = 1 \right)$

Proof. It is trivial because mentioned above 3.1, $[CVP_i]$ have all gates which decide $[CVP_i](x) = 1$ and any $[CVP_I] \setminus [CVP_i]$ gates cannot change $[CVP_i](x)$ values. Therefore $[CVP_I](x) = 1$ if $[CVP_i](x) = 1$. □

Theorem 3.5. $\forall I, i, x \left([CVP_I] \supseteq [[CVP_i](x)] \rightarrow [CVP_I](x) = 0 \rightarrow [CVP_i](x) = 0 \right)$

Proof. (Proof by contradiction.) Assume to the contrary that

$\exists I, i, x \left(([CVP_I] \supseteq [[CVP_i](x)]) \wedge ([CVP_I](x) = 0) \wedge ([CVP_i](x) = 1) \right)$

Mentioned above 3.4,

$\forall I, i, x \left([CVP_I] \supseteq [[CVP_i](x)] \rightarrow [[CVP_i](x)](x) = 1 \rightarrow [CVP_I](x) = 1 \right)$

$\rightarrow \forall I, i, x \left([CVP_I] \supseteq [[CVP_i](x)] \rightarrow [CVP_i](x) = 1 \rightarrow [CVP_I](x) = 1 \right)$

Then

$\exists I, i, x \left(([CVP_I] \supseteq [[CVP_i](x)]) \wedge ([CVP_I](x) = 0) \wedge ([CVP_i](x) = 1) \right)$

$\rightarrow \exists I, i, x \left(([CVP_i](x) = 1 \rightarrow [CVP_I](x) = 1) \wedge ([CVP_I](x) = 0) \wedge ([CVP_i](x) = 1) \right)$

$\rightarrow \exists I, i, x \left(([CVP_I](x) = 1) \wedge ([CVP_I](x) = 0) \wedge ([CVP_i](x) = 1) \right)$

and contradict assumption. □

Theorem 3.6. $\forall I, i \left(I \not\ni i \rightarrow \exists x \left((|x| < O(|i|)) \wedge ([CVP_I] \not\supseteq [[CVP_i](x)]) \right) \right)$

Proof. (Proof by contradiction.) Assume to the contrary that

$\exists I, i \left((I \not\ni i) \wedge \forall x \left(|x| < O(|i|) \rightarrow ([CVP_I] \supseteq [[CVP_i](x)]) \right) \right)$

Mentioned above 3.2

$\forall I, i \left(I \not\ni i \rightarrow \exists y \left((|y| < O(|i|)) \wedge (CVP_I(y) = 0) \wedge (CVP_i(y) = 1) \right) \right)$

Then

$\exists I, i \left((I \not\ni i) \wedge \forall x \left((|x| < O(|i|)) \rightarrow ([CVP_I] \supseteq [[CVP_i](x)]) \right) \right)$

$\rightarrow \exists I, i \left(\exists y \left((|i| < O(|y|)) \wedge (CVP_I(y) = 0) \wedge (CVP_i(y) = 1) \right) \wedge \forall x \left((|x| < O(|i|)) \rightarrow ([CVP_I] \supseteq [[CVP_i](x)] \right.\right.$

$\rightarrow \exists I, i, x \left((|i| < O(|x|)) \wedge (CVP_I(x) = 0) \wedge (CVP_i(x) = 1) \wedge ([CVP_I] \supseteq [[CVP_i](x)]) \right)$

Mentioned above 3.5

$\forall I, i, y \left([CVP_I] \supseteq [[CVP_i](y)] \rightarrow [CVP_I](y) = 0 \rightarrow [CVP_i](y) = 0 \right)$

Then

$\exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(\left[CVP_I \right] \supseteq \left[\left[CVP_i \right] (x) \right] \right) \right)$

$\rightarrow \exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \forall y \left(\left[CVP_I \right] (y) = 0 \rightarrow \left[CVP_i \right] (y) = 0 \right) \right)$

$\rightarrow \exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(\left[CVP_I \right] (x) = 0 \rightarrow \left[CVP_i \right] (x) = 0 \right) \right)$

Mentioned above 3.3

$\forall I, x \left(\left[CVP_I \right] (x) = 0 \rightarrow CVP_I\left(x \right) = 0 \right)$

Then

$\exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(\left[CVP_I \right] (x) = 0 \rightarrow \left[CVP_i \right] (x) = 0 \right) \right)$

$\rightarrow \exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(CVP_I\left(x \right) = 0 \rightarrow \left[CVP_i \right] (x) = 0 \right) \right)$

$\rightarrow \exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(\left[CVP_i \right] (x) = 0 \right) \right)$

However mentioned above 3.3

$\forall i, x \left(CVP_i\left(x \right) = 1 \rightarrow \left[CVP_i \right] (x) = 1 \right)$

Then

$\exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(CVP_i\left(x \right) = 1 \right) \wedge \left(\left[CVP_i \right] (x) = 0 \right) \right)$

$\rightarrow \exists I, i, x \left(\left(|i| < O\left(|x| \right) \right) \wedge \left(CVP_I\left(x \right) = 0 \right) \wedge \left(\left[CVP_i \right] (x) = 1 \right) \wedge \left(\left[CVP_i \right] (x) = 0 \right) \right)$

and contradict assumption. □

Theorem 3.7. $|[SAT]| \notin O\left(n^c \right)$

Proof. Mentioned above 3.6, each effective circuit set $[CVP_i]$ have unique gate, and these unique gates are necessary to compute input $x \mid |x| < O\left(|i| \right)$. Therefore number of unique gates that correspond to $[CVP_i]$ is over polynomial size of $|x|$ because number of $[CVP_i]$ is exponential size of $|i|$.

Therefore, $[SAT]$ have gates that is over polynomial size, and $|[SAT]| \notin O\left(n^c \right)$.

□

Corollary 3.8. $P \neq NP$

References

[Sipser] Michael Sipser, (translation) OHTA Kazuo, TANAKA Keisuke, ABE Masayuki, UEDA Hiroki, FUJIOKA Atsushi, WATANABE Osamu, Introduction to the Theory of COMPUTATION Second Edition, 2008