# MINIMAL CIRCUIT IN P VS NP PROBLEM

KOJI KOBAYASHI

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

Inputs of uniform circuit family that compute P problem have some symmetry that indicated curcit structure. To clarify this symmetry, we define "Minimal circuit" as subgraph of circuit which are necessary to compute subset of inputs. Minimal circuit 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 minimal circuit family, uniform circuit family N that solve NP problem have to include minimal circuit family that correspond to Di. These minimal circuit family have unique circuit gate and N must include these minimal circuit family and gates. Number of such minimal circuit is over polynomial size of input. Therefore, N is over polynomial size, and P is not NP.

## 1. Circuit family symmetry

Inputs of uniform circuit family have some symmetry that indicated each gate output value in curcit family. To clarify this symmetry, we define "Minimal circuit family" as subgraph of circuit which correspond to subset of inputs.

**Definition 1.1.** We use term as following;
$|x|$ : Size of Input $x$.
$c_k$: Boolean circuit which input length is $k$.
$\{c_k\} = C$ : Uniform circuit family
$C(x)$ : Circuit value when input is $x$.
$SAT$ : Boolean satisfiability problems.
$CVP$ : Circuit Value Problems
$TM$ : Set of Turing Machine.
$NTM$ : Set of Nondeterministic TM.
$DTM$ : Set of Deterministic TM.

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

**Definition 1.2.** We will use the term "Minimal circuit $c$ of circuit $C$ at input(s) $x$" or "$c = [C(x)]$" as one of possible circuits which generated uniformly, and remove ineffective gate one by one. Ineffective gate is that circuit keep value even if gate output invert value. (Minimal circuit have all wire between gates which minimal circuit have)

We also use the term "(Minimal) circuit path" as directed graph path from one of input gates to output gate.

Mininal circuit of each input are different each other, but these circuits can overlay partially each other. That is, inputs have some symmetry that indicated minimal circuit. So if inputs have extra assymetry, circuit have to use extra gate.

**Theorem 1.3.** *If all circuit path $u$ of minimal circuit $[C_p(x)]$ is included $C_q$, minimal circuit $[C_q(x)]$ equal $[C_p(x)]$.*

$\forall u \subset [C_p(x)] \, (u \subset C_q) \rightarrow [C_p(x)] = [C_q(x)]$

*Proof.* From minimal circuit and circuit path difinition 1.2, whole of circuit path in $[C_p(x)] \subset C_p$ cover whole of $[C_p(x)]$ gate, and whole of circuit path in $[C_q(x)]$ also cover whole of all $[C_q(x)]$ gate. If $[C_p(x)], [C_q(x)]$ have same gate then $[C_p(x)], [C_q(x)]$ have same wire. Therefore

$\forall u \subset [C_p(x)] \, (u \subset [C_p(x)] \subset C_p) \rightarrow [C_p(x)] = [C_q(x)]$ □

## 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.

For simplicity, $i$ have 0 filler $i = \{0,1\}^{|i|} + 0^*$, and if $D_i$ does not use some of $i$ to compute $x$, then $D_i(x) = 0$

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

*Proof.* It is trivial from Concrete DTM difinition 2.1. □

## 3. Computing NP Problem with Circuit Family

Consider to solve $N \in NP$ with circuit family $\{c_k\} \in P$. $N$ 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 "$CVP_i \in P-Complete$" as the Concrete DTM of $SAT \in NP - Complete$.

"$fix(p)$" as one of special input that $CVP_p(fix(p)) = 1$ and $CVP_{q \neq p}(fix(p)) = 0$. "$fix(0)$"as one of special input that $SAT(fix(0)) = 0$.

**Theorem 3.2.** *Each $CVP_i$ have different $fix(i)$.*

$\forall p \exists fix(p) \, (CVP_p(fix(p)) = 1, CVP_{q \neq p}(fix(p)) = 0)$

*Proof.* It is trivial because $CVP_p$ have some input fomuras $x$ that

$x(p) = 1, x(q \neq p) = 0$ such as $x = fix(0) \vee p$. □

**Theorem 3.3.** *Circuit family* $[SAT]$ *that compute SAT problem include all* $[CVP_p(fix(p))]$.

*Proof.* It is trivial because if $[SAT]$ do not include $[CVP_p(fix(p))] = 1$ then $[SAT](fix(p)) = 0$ and cannot compute correctly.

The other hand, if some partial circuit $c \subset [SAT](x)$ become $c(fix(p)) = 1$ and lead $[SAT](fix(p)) = 1$ , then $[CVP_p(fix(p))] = [c]$. □

**Theorem 3.4.** *All* $[CVP_p(fix(p))]$ *have unique circuit path and gate.*
$\forall [CVP_p(fix(p))], [CVP_{q\neq p}(fix(q))]\ \exists u \subset [CVP_p(fix(p))](u \not\subset [CVP_q(fix(q))])$

*Proof.* (Proof by contradiction.) Assume to the contrary that
$\exists [CVP_p(fix(p))], [CVP_{q\neq p}(fix(q))]\ \forall u \subset [CVP_p(fix(p))](u \subset [CVP_q(fix(q))])$
Mentioned above 1.3,
$\forall u \subset [CVP_p(fix(p))](u \subset [CVP_q(fix(q))]) \rightarrow [CVP_p(fix(p))] = [CVP_q(fix(q))]$
Therefore
$\exists [CVP_p(fix(p))], [CVP_{q\neq p}(fix(q))]\ \forall u \subset [CVP_p(fix(p))](u \subset [CVP_q(fix(q))])$
$\rightarrow \exists [CVP_p(fix(p))], [CVP_{q\neq p}(fix(q))]([CVP_p(fix(p))] = [CVP_q(fix(q))])$
However, from $fix(p), fix(q)$ definition 3.1,
$[CVP_p(fix(p))](p) = 1$, $[CVP_q(fix(q))](p) = 0$
and contradict assumption. □

**Theorem 3.5.** *Circuit family* $[SAT]$ *have over polynomial size.*

*Proof.* Mentioned above 3.4, each minimal circuit $[CVP_p(fix(p))]$ have unique circuit path and gate. Number of $[CVP_p(fix(p))]$ is over polynomial of input size $|x|$ because one of input $fix(p)$ (which is one of input) is over logarithm size of $p$.

Therefore, $[SAT]$ that include all unique gate of $[CVP_p(fix(p))]$ is also over polynomial size. □

**Corollary 3.6.** $P \neq NP$

## 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