COUNTING COMPLEXITY BY USING PARTIAL CIRCUIT INDEPENDENCY

KOJI KOBAYASHI

Abstract. This paper describes about complexity of NP problems by using "Effective circuit" independency, and apply SAT problem.

Inputs of circuit family that compute P problem have some explicit symmetry that indicated circuit structure. To clarify this explict 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"which index i correspond to selection of nondeterministic transition functions. That is, NTM split many different asymmetry DTM and compute all DTM in same time.

Consider concrete DTM and effective circuit set, circuit family [SAT] that solve SAT problem have to include all effective circuit set [CVPi] that correspond to concrete DTM as Circuit Value Problem. [CVPi] have unique gate and [SAT] must include all [CVPi]. Number of [CVPi] is over polynomial size of input. Therefore, [SAT] is over polynomial size.

1. Effective circuit set

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

Definition 1.1.

Date: 2017-10-01.

We use term as following;

$|x|$: Size of Input x

$F(x)$: Circuit or TM value when input is x.

SAT : boolean SATisfiability problem.

CVP : Circuit Value Problem.

TM : Set of Turing Machine.

DTM : Set of Deterministic TM.

NTM : Set of Nondeterministic TM.

$\mathbb{N}$: Natural Number.

$O(n^c)$: Big O notation of polynomial size.

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 with input x" or "$c = [C(x)]$" as one of possible partial circuit of unform circuit family which remove all ineffective gate one by one. "Ineffective gate" is gate that circuit keep value even if the gate invert output value. Unlike circuit family, effective circuit probably become $(p \neq q) \wedge (|p| = |q|) \rightarrow [C(p)] \neq [C(q)]$.

We also use the term "Effective circuit set" or $[C] = \{[C(x)] \mid C(x) = 1\}$ as set of effective circuit $[C(x)]$ that correspond to $C(x) = 1$.

For simplicity, we suppose all circuit family as PTIME DTM emulater like [Sipser] theorem 9.30. That is; a) Each gates simulate each tape cell and state of TM at each step. b) Each gate connecte that simurate TM transition functions with monotone circuit. c) NOT gate only connect input gate, and split each input $\{0, 1\}$ to $\{01, 10\}$.

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 $D_I = \bigvee_{i \in I} D_i$ that $I \subset \mathbb{N}, |I| < k \in \mathbb{N}$ as disjunction of Concrete DTM.

For simplicity, i is Binary number $\mathbb{N} \ni i = \{0,1\}^{|i|}$. If D_i does not use all of i to compute x, or i is not enough to compute x, then $D_i(x) = 0$.

3. Computing NP Problem with Circuit Family

Consider to solve SAT with circuit family. SAT have extra implicit symmetry CVP_i (that mention following). Because this extra implicit symmetry decide SAT result, circuit family necesary to compute this symmetry to solve SAT. Especially, CVP_i have some input x that $\mathrm{CVP}_p(x) = 1$ and $\mathrm{CVP}_{q \neq p}(x) = 0$, and some input y that $\mathrm{CVP}_p(y) = \mathrm{CVP}_q(y) = 0$. This means that all CVP_i are independ each other.

Definition 3.1.

We will use the term following;

CVP_i : Concrete DTM of SAT that value assignment is $\mathbb{N} \ni i = \{0,1\}^{|i|}$. If input x arity is not equal $|i|$, then $\mathrm{CVP}_i(x) = 0$.

CVP_I : Disjunction of $\mathrm{CVP}_i \bigvee_{i \in I} \mathrm{CVP}_i$.

[SAT] : Circuit family that compute SAT.

$[\mathrm{CVP}_i]$: Effective circuit set of [SAT] that $\mathrm{CVP}_i(x) = 1 \to [\mathrm{CVP}_i](x) = 1$.

$[\mathrm{CVP}_I]$: Effective circuit set that all of $[\mathrm{CVP}_i] \mid i \in I$ included.

Theorem 3.2.

$$\forall I, i\ \exists x\left(\left(|x| < O\left(|i|^{c}\right)\right) \wedge \left(\left(I \not\ni i\right) \rightarrow \left(CVP_I\left(x\right) = 0\right) \wedge \left(CVP_i\left(x\right) = 1\right)\right)\right)$$

Proof. It is trivial because some formula x become $x\left(i\right) = 1, x\left(j\right) = 0 \mid j \in I$ and $|x| < O\left(|i|^{c}\right)$ (like $x\left(t\right) \equiv \left(t = i\right)$). □

Theorem 3.3.

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

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

Proof. It is trivial from definition 3.1. □

Theorem 3.4.

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

Proof. It is trivial from definition 3.1.

$\left[\mathrm{CVP}_i\right]$ have all gates which decide $\left[\mathrm{CVP}_i\left(x\right)\right]\left(x\right) = \left[\mathrm{CVP}_i\right]\left(x\right) = 1$ and any $\left[\mathrm{CVP}_I\right] \backslash \left[\mathrm{CVP}_i\right]$ gates cannot change $\left[\mathrm{CVP}_i\right]\left(x\right)$ output values. Therefore $\left[\mathrm{CVP}_i\right]\left(x\right) = 1$ imply $\left[\mathrm{CVP}_I\right]\left(x\right) = 1$ if $\left[\mathrm{CVP}_I\right] \supseteq \left[\mathrm{CVP}_i\left(x\right)\right]$. □

Corollary 3.5.

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

Theorem 3.6.

$$\forall I, i, x\left(\left(CVP_I\left(x\right) = 0\right) \wedge \left(CVP_i\left(x\right) = 1\right) \rightarrow \left[CVP_I\right] \not\supseteq \left[CVP_i\left(x\right)\right]\right)$$

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

$$\exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right) = 0\right) \wedge \left(\mathrm{CVP}_i\left(x\right) = 1\right) \wedge \left(\left[\mathrm{CVP}_I\right] \supseteq \left[\mathrm{CVP}_i\left(x\right)\right]\right)\right)$$

Mentioned above 3.5

$$\forall I, i, x\left(\left[\mathrm{CVP}_I\right] \supseteq \left[\mathrm{CVP}_i\left(x\right)\right] \rightarrow \left(\left[\mathrm{CVP}_I\right]\left(x\right) = 0 \rightarrow \left[\mathrm{CVP}_i\right]\left(x\right) = 0\right)\right)$$

Therefore

$$\exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right) = 0\right) \wedge \left(\mathrm{CVP}_i\left(x\right) = 1\right) \wedge \left(\left[\mathrm{CVP}_I\right] \supseteq \left[\mathrm{CVP}_i\left(x\right)\right]\right)\right)$$

$$\rightarrow \exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right) = 0\right) \wedge \left(\mathrm{CVP}_i\left(x\right) = 1\right) \wedge \left(\left[\mathrm{CVP}_I\right]\left(x\right) = 0 \rightarrow \left[\mathrm{CVP}_i\right]\left(x\right) = 0\right)\right)$$

However mentioned above 3.3

$\forall i, x\left(\mathrm{CVP}_i\left(x\right)=1 \rightarrow \left[\mathrm{CVP}_i\right]\left(x\right)=1\right)$

$\forall I, x\left(\left[\mathrm{CVP}_I\right]\left(x\right)=0 \rightarrow \mathrm{CVP}_I\left(x\right)=0\right)$

Therefore

$\exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right)=0\right) \wedge \left(\mathrm{CVP}_i\left(x\right)=1\right) \wedge \left(\left[\mathrm{CVP}_I\right]\left(x\right)=0 \rightarrow \left[\mathrm{CVP}_i\right]\left(x\right)=0\right)\right)$

$\rightarrow \exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right)=0\right) \wedge \left(\left[\mathrm{CVP}_i\right]\left(x\right)=1\right) \wedge \left(\mathrm{CVP}_I\left(x\right)=0 \rightarrow \left[\mathrm{CVP}_i\right]\left(x\right)=0\right)\right)$

$\rightarrow \exists I, i, x\left(\left(\mathrm{CVP}_I\left(x\right)=0\right) \wedge \left(\left[\mathrm{CVP}_i\right]\left(x\right)=1\right) \wedge \left(\left[\mathrm{CVP}_i\right]\left(x\right)=0\right)\right)$

and contradict assumption. □

Theorem 3.7.

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

Proof. It is trivial from definition 1.2. □

Theorem 3.8.

$\left|\left[\overline{SAT}\right]\right| \notin O\left(n^c\right)$

Proof. Mentioned above 3.6 3.7 ,

$\forall I, j, x\left(\left(\mathrm{CVP}_I\left(x\right)=0\right) \wedge \left(\mathrm{CVP}_j\left(x\right)=1\right) \rightarrow \left[\mathrm{CVP}_I\right] \not\supseteq \left[\mathrm{CVP}_j\left(x\right)\right]\right)$

$\forall I, i, x\left(I \ni i \rightarrow \left[\mathrm{CVP}_I\right] \supseteq \left[\mathrm{CVP}_i\left(x\right)\right]\right)$

That is, each $\left[\mathrm{CVP}_j\right]$ have unique gate in $\left[\mathrm{CVP}_j\left(x\right)\right]$, x is some input that $\mathrm{CVP}_j\left(x\right)=1$ and $\mathrm{CVP}_{i\neq j}\left(x\right)=0$.

Mentioned above 3.2,

$\forall I, i\ \exists x\left(\left(\left|x\right|<O\left(\left|i\right|^c\right)\right) \wedge \left(\left(I \not\ni i\right) \rightarrow \left(\mathrm{CVP}_I\left(x\right)=0\right) \wedge \left(\mathrm{CVP}_i\left(x\right)=1\right)\right)\right)$

such x exist atmost $\left|x\right|<O\left(\left|i\right|^c\right)$ size.

So number of unique gates that correspond to $\left[\mathrm{CVP}_j\left(x\right)\right]$ is over polynomial size of $\left|x\right|$, because number of $\left[\mathrm{CVP}_j\right]$ is exponential size of $\left|i\right|$.

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

□

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