Satisfiability Algorithms for Small Depth Circuits with Symmetric Gates

Suguru TAMAKI

Kyoto University & Simons Institute
This Talk

is about Algorithm Design & Complexity Theory because
this workshop is about “Connections Between Algorithm Design and Complexity Theory”
this program is about
“Fine-Grained Complexity and Algorithm Design”

Contribution (Algorithm Design)
Circuit SAT algorithms for “interesting” circuit classes

Implications (Complexity Theory)
Circuit size lower bounds (by known results)
Our Problem

Circuit Satisfiability (SAT)

Input:

Boolean circuit $C: \{0,1\}^n \rightarrow \{0,1\}$

Output:

$\exists x, C(x) = 1 \Rightarrow \text{Yes}$
$\forall x, C(x) = 0 \Rightarrow \text{No}$

- Canonical NPC problem
- Solved in time $\text{poly}(|C|)2^n$ ($n$: #variables)
- $C$-SAT: input only from circuit class $C$
  
  e.g. $C = (k-)\text{CNF}, \text{AC}^0, \text{AC}^0[p], \text{ACC}^0, \text{TC}^0, \text{NC}^1$ (Formula),...
General Research Goals

1. Design non-trivial algorithms for a stronger circuit class

   **Non-trivial:**
   - super-polynomially (exponentially) faster than $2^n$

   **Stronger circuit class:**
   - $(k-)$CNF $\subset AC^0 \subset AC^0[p] \subset ACC^0 \subset TC^0 \subset NC^1 \subset \ldots \subset CKT$

2. If non-trivial algorithms exist for $C$-SAT, then
   - improve the running time
   - prove the difficulty of improvement
Why Study Circuit SAT?

1. Useful

- **can encode** many combinatorial problems efficiently
- (sometimes) **inspires algorithms** for other problems
  e.g. All-Pairs Shortest Paths (APSP) [Williams’14,...]

2. Connection to circuit lower bounds

- [black box] non-trivial \( \mathcal{C} \)-SAT algorithm \( \Rightarrow \) \( \text{NEXP} \not\subseteq \mathcal{C} \)
  [Williams’10,11,...] (NEXP: nondeterministic exponential time)

- [white box] analysis of \( \mathcal{C} \)-SAT algorithm
  \( \Rightarrow \) **average-case lower bounds**
  [Santhanam’10,Seto-T’12,Chen-Kabanets-Kolokolova-Shaltiel-Zuckerman’14,...]
Circuit Classes

\((k-)CNF \subset AC^0 \subset AC^0[p] \subset ACC^0 \subset TC^0 \subset NC^1 \subset \ldots \subset CKT\)

- \((k-)CNF\): conjunction of disjunctions of (at most \(k\)) literals
- \(AC^0\): constant-depth, unbounded-fan-in, AND/OR/NOT
- \(AC^0[p]\): \(AC^0 + \text{mod } p\) gates (\(p\): prime power)
- \(ACC^0\): \(AC^0 + \text{mod } m\) gates (\(m\): integer \(\geq 2\))
- \(TC^0\): constant-depth, unbounded-fan-in, linear threshold (THR) gates: \(\text{sgn}(\sum_{i=1}^{n} w_i x_i - \theta)\)
- \(NC^1\): fan-in 2, fan-out 1, AND/OR/NOT(/XOR)
- \(CKT\): fan-in 2, AND/OR/NOT(/XOR)
- \(\mathcal{C}_1 \circ \mathcal{C}_2\): composition of \(\mathcal{C}_1 \circ \mathcal{C}_2\) e.g. \(CNF = \text{AND} \circ \text{OR}\)
  (Note: assume \#gates = \(\text{poly}(n)\) unless otherwise specified)
... ⊂ AC^0[p] ⊂ ACC^0 ⊆ ACC^0 \circ THR ⊆ TC^0 ⊆ NC^1 ⊆ ... ⊆ CKT

Non-trivial \(\mathcal{C}\)-SAT algorithm:
- ACC^0 \circ THR with a super-poly \# gates [Williams’14]
- THR \circ THR with a linear \# wires [Impagliazzo-Paturi-Schneider’13, ...]

Lower Bounds for \(\mathcal{C}\):
- majority, mod \(q\) ∉ AC^0[p] [Razborov’87, Smolensky’87]
- NEXP ∉ ACC^0 \circ THR [Williams’14]
- parity ∉ depth-\(d\) TC^0 with
  \[\# wires = n^{1+1/3^d} \quad \text{or} \quad \# gates = (n/2)^{1/(2d-1)}\]
  [Impagliazzo-Paturi-Saks’93]
New $C$-SAT algorithms

Attempts to handle $TC^0$ (probably $C \not\subseteq ACC^0 \circ THR$)
- $AC^0$ with a limited $\#$ symmetric gates: $g(\sum_{i=1}^{n} x_i)$
- THR$\circ$THR with a sub-quadratic $\#$ gates

Faster algorithms within $AC^0[p]$ ($C \subseteq ACC^0 \circ THR$)
- Systems of (degree-$k$) Polynomial Equations over GF(2)
- $XOR \circ AND \circ XOR \circ AND \circ XOR$
- $AC^0[p]$
$\text{AC}^0$ with a limited #symmetric gates
Motivation

Think about some interesting $\mathcal{C} \subset TC^0 \setminus ACC^0 \circ THR$
i.e. $\mathcal{C} = \text{``AC}^0 \text{ with } t(n) \text{ symmetric gates''}$
(Note: $\mathcal{C} \not\subset ACC^0 \circ THR$ is not known)

Definition:

- $f : \{0,1\}^n \rightarrow \{0,1\}$ is symmetric (SYM)
if $\exists g : \mathbb{Z} \rightarrow \{0,1\}$, $f = g(\sum_{i=1}^{n} x_i)$

- $f : \{0,1\}^n \rightarrow \{0,1\}$ is weighted symmetric
if $\exists g : \mathbb{Z} \rightarrow \{0,1\}$, $\exists w_i \in \mathbb{Z}$, $f = g(\sum_{i=1}^{n} w_i x_i)$

AND, OR, parity, mod $m$, majority are symmetric
THR $(\text{sgn}(\sum_{i=1}^{n} w_i x_i - \theta))$ is weighted symmetric
Motivation

\[ \mathcal{C} = \text{``AC}^0 \text{ with } t(n) \text{ symmetric gates''} \]

Interesting?

■ contains Max SAT when depth-2, \( t(n) = 1 \) (THR\( \circ \)OR)
  non-trivial algorithm for Max 3-SAT is open
  (cf. \( 2^{0.791n} \) time algorithm for Max 2-SAT [Williams’04])

■ Lower bounds:
  generalized inner product (GIP) \( \not\in \text{AC}^0 \) with
  \#symmetric gates = \( n^{1-o(1)} \) or \#THRs = \( n^{1/2-o(1)} \)
  […, Lovett-Srinivasan’11]
New $C$-SAT algorithms (1)

**Theorem** [Sakai-Seto-T-Teruyama]:
Let $C = \text{``AC}^0 \text{ with } t(n) \text{ weighted symmetric gates''}$
where $t(n) = n^{o(1)}$, maximum weight $2^{n^{0.99}}$
There is a non-trivial deterministic algorithm for $\#C$-SAT
(Note: we assume evaluation of symmetric gate is easy)

**Corollary:**
Max SAT can be solved in deterministic time $2^{n-n^{1/O(k)}}$
when $\#\text{clauses} = O(n^k)$
(Note: Max $k$-SAT $\Rightarrow \#\text{clauses} = O(n^k)$)
Implications

Corollary:
Let $\mathcal{C} = \text{``AC}^0\text{ with } t(n)\text{ weighted symmetric gates''}$
where $t(n) = n^{o(1)}$, maximum weight $2^{n^{0.99}}$
Then $\mathsf{E}^{\mathsf{NP}} \not\subset \mathcal{C}$

Questions:
New? Interesting?
Lemma:

Let $\mathcal{C}=(\text{weighted SYM}) \circ \text{AND}$
where $\#\text{ANDs} = m$, maximum weight $w$

There is a deterministic algorithm for $\#\mathcal{C}$-SAT
that runs in time $\text{poly}(n, m, \log w)2^{n-\mu(n,m,w)}$
where $\mu(n,m,w) = (n/\log(mw))^{\Omega(\log n/ \log m)}$

Based on "Concentrated Shrinkage" & DP

(Note: Theorem follows from Lemma and transformation
$\mathcal{AC}^0$ with symmetric gates $\Rightarrow$ SYM$\circ$ AND using
[Beigel-Reingold-Spielman'91,Beigel'92,Beame-Impagliazzo-Srinivasan'12])
THR • THR with a sub-quadratic #gates
Think about another interesting $\mathcal{C} \subset TC^0 \setminus ACC^0 \circ THR$
i.e. $\mathcal{C} = THR \circ THR$
(Note: $\mathcal{C} \not\subseteq ACC^0 \circ THR$ is not known)

$\mathcal{C}$-SAT can be solved in time $2^n(1-\mu(c))$
where $\mu(c) = 1/c^{O(c)}$, $\#\text{wires} = cn$
[Impagliazzo-Paturi-Schneider’13, Chen-Santhanam’15]
(non-trivial if $cn = o(n \log n / \loglog n)$

parity $\not\in$ depth-$d$ $TC^0$ with
$\#\text{wires} = n^{1+1/3d}$ or $\#\text{gates} = (n/2)^{1/(2d-1)}$
[Impagliazzo-Paturi-Saks’93]
New $C$-SAT algorithms (2)

Theorem [T]:
Let $C = \text{THR} \circ \text{THR}$, where $\#\text{gates} = m$
There is a randomized algorithm for $C$-SAT that runs in time $\text{poly}(n, m) \cdot 2^{n - \mu(n,m)}$,
where $\mu(n, m) = \Omega(n/m^{1/2+o(1)})^c$, $\exists c < 1/5$
(Note: $\#\text{gates} \leq \#\text{wires}$)

Questions:
Derandomization?
(coNP algorithm is enough for $E^{\text{NP}} \not\subseteq C$)
New lower bounds from analysis?
Proof Sketch

- based on the Polynomial Method in Circuit Complexity
- follow the framework for $\text{ACC}^0 \circ \text{THR}$ [Williams’14]
- use probabilistic polynomial for THR [Srinivasan’13]
- some transformation techniques due to [Maciel-Therien’98], [Beigel’92]
- use fast evaluation algorithm for $\text{SYM} \circ \text{SYM}$ [Williams’14]

Some details later
Faster algorithms within $\text{ACC}^0$
(k-)CNF $\subset AC^0 \subset AC^0[p] \subset ACC^0$

$C$: $C$-SAT in time $T$, condition

- **k-CNF:** $2^n(1-\mu(k)), \mu(k) = 1/O(k)$
  
  [Paturi-Pudlak-Zane’97,…]

- **CNF:** $2^n(1-\mu(c)), \mu(c) = 1/O(\log c), \#\text{clauses} = cn$
  
  [Schuler’05,Calabro-Impagliazzo-Paturi’06,…]

- **AC^0:** $2^n(1-\mu(c,d)), \mu(c,d) = 1/O(\log c + d \log d)^{d-1}$,
  
  depth-$d$, $\#\text{gates} = cn$  
  [Impagliazzo-Matthews-Paturi’12]

- **ACC^0:** $2^n-\mu(n,d), \mu(n,d) = n^{1/2\omega(d)}$,
  
  depth-$d$, $\#\text{gates} = 2^{n^{\omega(1)}}$  
  [Williams’11]
New $C$-SAT algorithms (3)

**Theorem [T-Williams]:**

$C$: $C$-SAT in time $T$, condition

- Systems of **degree-$k$** Polynomial Equations over $\text{GF}(2)$
  
  $\left(= \text{AND} \circ \text{XOR} \circ \text{AND}_k \supset k\text{-CNF} = \text{AND} \circ \text{OR}_k\right)$:
  
  $2^{n(1-\mu(k))}, \mu(k) = 1/O(k)$

- $\text{XOR} \circ \text{AND} \circ \text{XOR} \circ \text{AND} \circ \text{XOR}$ ($\supset \text{CNF} = \text{AND} \circ \text{OR}$):
  
  $2^{n(1-\mu(c))}, \mu(c) = 1/O(\log c), \#\text{ANDs} = cn$ at depth-4

- $\text{AC}^0[p]$ ($\supset \text{AC}^0$):
  
  $2^{n(1-\mu(d,m))}, \mu(d, m) = 1/O(\log m)^{d-1}$, depth-$d$, $\#\text{gates} = m$
Proof Sketch

- based on the Polynomial Method in Circuit Complexity
- use probabilistic polynomial for AND/OR [Razborov’87, Smolensky’87]
  \(\text{AC}^0[p]\) [Kopparty-Srinivasan’12]
- use fast evaluation algorithm for polynomial [Yates,…]
- first item is essentially due to [Lokshtanov-Paturi]
  (algorithm for \(k\)-CNF based on the polynomial method)
- second item is based on degree reduction for \(\text{AND} \circ \text{XOR} \circ \text{AND} \circ \text{XOR}\)
  extending Schuler’s width reduction for CNF

Some details later
Algorithms via Polynomial Method
Example [Razborov’87, Smolensky’87]:
1. $\text{AC}^0[p]$ can be well approximated by a low-degree $\text{GF}(p)$ polynomial
2. majority, mod $q$ cannot be well approximated by a low-degree $\text{GF}(p)$ polynomial

$1+2 \Rightarrow \text{majority, mod } q \notin \text{AC}^0[p]$

item 1 is useful in algorithm design
(``sparse“ suffices instead of ``low-degree“ in many cases)
Polynomial Method

Definition:
Let $f: \{0,1\}^n \rightarrow \{0,1\}$

A distribution $P$ over polynomials is an $\epsilon$-error probabilistic polynomial for $f$
if $\forall x$, $\Pr_{p \sim P}[p(x) \neq f(x)] \leq \epsilon$

$\deg(P) \leq d$ if $\Pr_{p \sim P}[\deg(p) \leq d] = 1$

$\epsilon$-error probabilistic $C$-circuit is defined analogously
Algorithm for $\mathcal{C}$-SAT

**Input:** $C: \{0,1\}^n \rightarrow \{0,1\}, C \in \mathcal{C}$

**Step 1.** Define $C': \{0,1\}^{n-n'} \rightarrow \{0,1\}, C' \in \text{OR} \circ C$ as

$$C'(y) := \bigvee_{a \in \{0,1\}^{n'}} C(y, a) \quad \text{(Note: } |C'| \approx 2^{n'}|C|)$$

**Step 2.** Construct (1/3)-error probabilistic polynomial $p$ for $C'$ in time $T(n, n', |C|)$

**Step 3.** Evaluate $p(y)$ for all $y \in \{0,1\}^{n-n'}$ in time $T'(n, n', |C|)$

**Step 4.** Repeat 2-3 $O(n)$ times to reduce error probability

**Output:** truth table $V$ of $C'$ such that

$$\forall y, \Pr[V(y) \neq C'(y)] \leq 2^{-2n}$$

**Running Time:** $O(n(T(n, n', |C|) + T'(n, n', |C|)))$
Lemma [Razborov’87, Smolensky’87]:
There exists $\epsilon$-error probabilistic polynomial for AND/OR of degree $\log(1/\epsilon)$ and it is efficiently samplable

Lemma [Srinivasan’13]:
There exists $\epsilon$-error probabilistic polynomial for THR of degree $\sqrt{n \log(n/\epsilon)}$ and it is efficiently samplable
Ingredients for THR\circ THR (2/3)

Lemma:

\[ \text{XOR}\circ\text{AND}\circ\text{XOR}\circ\text{AND} \subseteq \text{XOR}\circ\text{AND} \]

Lemma [Maciel-Therien’98]:

THR \subseteq AC^0[2] \circ \text{SYM}

Lemma [Beigel’92]:

\[ \text{AND}\circ\text{SYM} \subseteq \text{weighted SYM} \]
Lemma [Williams’14]:

Let $C : \{0,1\}^n \rightarrow \{0,1\}$, $C \in \text{SYM} \circ (\text{weighted SYM})$ where

- top gate has fan-in $u$
- bottom gates have maximum weight $w$

such that $uw \leq 2^{0.1n}$

Then, truth table of $C$ can be generated in time $\text{poly}(n)2^n$
Algorithm for \( \text{THR} \circ \text{THR-\text{SAT}} \)

**Input:** \( C : \{0,1\}^n \rightarrow \{0,1\}, C \in \text{THR} \circ \text{THR} \)

**Step 1.** Define \( C' : \{0,1\}^{n'} \rightarrow \{0,1\}, C \in \text{OR} \circ C \) as

\[
C'(y) := \bigvee_{a \in \{0,1\}^{n'}} C(y, a) \quad \text{(Note: } |C'| \approx 2^{n'} |C| \text{)}
\]

**Step 2.** Construct \((1/3)\)-error probabilistic circuit \( C'' \) for \( C' \)

\[
C'' \in (\text{XOR} \circ \text{AND}) \circ (\text{XOR} \circ \text{AND}) \circ \cdots \circ (\text{XOR} \circ \text{AND}) \circ \text{SYM}
\]

**Step 3.** Transform \( C'' \) into \( C''' \in \text{XOR} \circ (\text{weighted SYM}) \)

**Step 4.** Evaluate \( C'''(y) \) for all \( y \in \{0,1\}^{n-n'} \)

**Step 5.** Repeat 2-4 \( O(n) \) times to reduce error probability

**Output:** truth table of \( C' \)
Algorithm for THR$\circ$THR-SAT

Theorem [T]:
Let $\mathcal{C} = \text{THR} \circ \text{THR}$, where $\#\text{gates} = m$
There is a randomized algorithm for $\mathcal{C}$-SAT that runs in time $\text{poly}(n, m) \cdot 2^{n-\mu(n,m)}$,
where $\mu(n, m) = \Omega\left(n/m^{1/2+o(1)}\right)^c$, $\exists c < 1/5$

Questions:
Derandomization?
(coNP algorithm is enough for $E^{NP} \not\subseteq \mathcal{C}$)
New lower bounds from analysis?
Other Techniques
Degree Reduction

AND\circ XOR\circ AND\circ XOR with \#ANDs at depth-3 = m can be computed by a \textit{decision tree} such that

1. \textbf{internal node} queries a linear equation $Ax = b$?
   where $\text{rank}(A) \approx \log(m/n)$
2. \textbf{leaf} queries a system of degree-$d$ polynomial equations
   where $d \approx \log(m/n)$
3. if leaf is reached after $L$ times \textit{Yes},
   the system is defined over linear space of dimension $\approx n - L \log(m/n)$
4. \#leaves reached by $L$ times \textit{Yes}
   is at most $\binom{m + L}{L}$ (Note: $L \leq n/\log(m/n)$)
Degree Reduction

degree reduction for AND$\circ$XOR$\circ$AND$\circ$XOR is a generalization of Schuler’s width reduction for CNF

Question:

degree reduction is useful in proving average-case lower bounds for $\text{AC}^0[p]$?

(as Schuler’s width reduction is useful in proving average-case lower bounds for $\text{AC}^0$)
Bottom Fan-In Reduction

(weighted SYM)\(\circ\)AND with \#ANDs \(= m = O(n^k)\) can be computed by a decision tree such that

1. internal node queries a variable \(x_i\)
2. leaf queries a (weighted SYM)\(\circ\)AND circuit whose bottom fan-in \(= O(k)\)
3. \#leaves \(\leq 2^{n-\sqrt{n}}\)

Question:
useful in proving average-case lower bounds for (weighted SYM)\(\circ\)AND?
Conclusion
New $\mathcal{C}$-SAT algorithms

Attempts to handle $\text{TC}^0$ (probably $\mathcal{C} \not\subseteq \text{ACC}^0 \circ \text{THR}$)
- $\text{AC}^0$ with a limited \#weighted symmetric gates
- $\text{THR} \circ \text{THR}$ with a sub-quadratic \#gates

Faster algorithms within $\text{AC}^0[p]$ ($\mathcal{C} \subseteq \text{ACC}^0 \circ \text{THR}$)
- Systems of (degree-$k$) Polynomial Equations over $\text{GF}(2)$ ($\supset k$-\text{CNF})
- $\text{XOR} \circ \text{AND} \circ \text{XOR} \circ \text{AND} \circ \text{XOR}$ ($\supset$ \text{CNF})
- $\text{AC}^0[p]$ ($\supset$ $\text{AC}^0$)
Open Questions

- non-trivial algorithm for stronger \( \mathcal{C} \):
  \[
  \text{ACC}^0 \circ \text{THR} \subseteq \text{TC}^0 \subseteq \text{NC}^1 \subseteq ... \subseteq \text{CKT}
  \]
  e.g. \( \text{AC}^0 \) with more symmetric gates, \( \text{THR} \circ \text{THR} \) with more gates, \( \text{THR} \circ \text{THR} \circ \text{THR} \),... or improve:
  \( \text{NC}^1 \) with \( n^3 \ (n^2) \) gates [Komargodski-Raz-Tal'13,...]
  \( \text{CKT} \) with \( 3n \ (2.5n) \) gates [Chen-Kabanets'15]

- without polynomial method? (in polynomial space?)

- other lower bound techniques useful?
  e.g. communication complexity, proof complexity, mathematical programming,...

- lower bound for \( \mathcal{C} \Leftrightarrow \) non-trivial \( \mathcal{C} \)-SAT algorithm?

- fine-grained reduction between \( \mathcal{C} \)-SAT and \( \mathcal{C}' \)-SAT?