Fine-grained complexity of NFA universality.

Petr Osička

KATEDRA INFORMATIKY
UNIVERZITA PALACKÉHO V OLOMOUCI

Jiří Balun, Tomáš Masopust, Petr Osička

Speed Me up If You Can: Conditional Lower Bounds on Opacity Verification.

MFCS 2023: 16:1-16:15

NFA Universality

- For NFA A, is $L(A) = \Sigma^*$?
- PSPACE-complete (Meyer, Stockmeyer, 1972)
- reducible to equivalence, inclusion
- PTIME for DFAs

Theorem

SETH implies that for any $\epsilon > 0$ universality of n-state NFA can't be decided in time $O^*(2^{n/(2+\epsilon)})$.

What was known (Fernau, Krebs 2017):

Theorem

ETH implies that universality of n-state NFA can't be decided in time $O^*(2^{o(n)})$.

Exponential time hypothesis

There is some $\epsilon > 0$ such that 3-SAT cannot be solved in time $O^*(2^{\epsilon n})$.

Strong exponential time hypothesis

For every $\epsilon > 0$, there is some $k \geqslant 3$ such that k-SAT cannot be solved in time $O^*(2^{(1-\epsilon)n})$, where n is the number of variables.

Proof

Given a k-CNF formula φ with n variable and m clauses we construct in poly(n) time an NFA A_φ with $N = 2n + 2$ states such that

$$\varphi \text{ is satisfiable} \qquad \text{iff} \qquad A_\varphi \text{ is universal.}$$

Solving universality in time $O^*(2^{N/(2+\epsilon)})$ then implies solving k-SAT in time $O^*(2^{(1-\epsilon')n})$ for $\epsilon' = \epsilon/(2+\epsilon)$. This contradicts SETH.

Construction idea:

- given a *special* input word, $\mathcal{A}_\varphi$ tries all variable assignments. If no satisfying assignment is found, $\mathcal{A}_\varphi$ switches to configuration consisting of one nonaccepting state.
- otherwise, $\mathcal{A}_\varphi$ keeps an accepting state in its configuration at all times.

Our special words are derived from Zimin words:

- Zimin word over alphabet $\{a_1, a_2, \ldots, a_n\}$ is

$$Z_1 = a_1,$$
$$Z_i = Z_{i-1} a_i Z_{i-1} \text{ (for } i > 1)$$

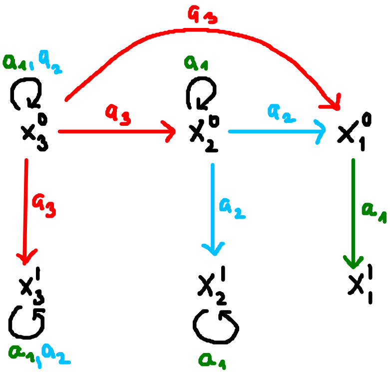
- $|Z_i| = 2^i - 1$
- *Key property*
  index of j-th symbol gives the position (counted from the end) of the rightmost 0 in a binary expansion of $j - 1$

……	4	3	2	1	
	0	0	0	0	a_1
	0	0	0	1	a_2
	0	0	1	0	a_1
	0	0	1	1	a_3
	0	1	0	0	a_1
	0	1	0	1	a_2
	0	1	1	0	a_1
	0	1	1	1	

Symbolic incrementation algorithm

1. Find rightmost 0
2. switch it to 1
3. All 1 to the right switch to 0

Zimin word gives us this



$$\{x_3^0, x_2^0, x_1^0\} \longrightarrow \{x_3^0, x_2^0, x_1^1\}$$

$$\longrightarrow \{x_3^0, x_2^1, x_1^0\}$$

$$\longrightarrow \{x_3^0, x_2^1, x_1^1\}$$

$$\longrightarrow \{x_3^1, x_2^0, x_1^1\}$$

$$\vdots$$

Let clauses of φ be $\mathcal{C} = \{C_1, C_2, \ldots, C_m\}$.
For a literal l let $\mathsf{cl}(l) = \{C \mid C \text{ is a clause containing } l\}$.

The alphabet Σ of A_φ is $\{a_1, a_2, \ldots, a_n, a_{n+1}\} \times \mathcal{C}$.

In the automata constructed so far, we replace $\xrightarrow{a_i}$ with $\xrightarrow{a_i \times \mathcal{C}}$.

We add states q_a, q_r and transitions $q_a \xrightarrow{\Sigma} q_a$, $q_r \xrightarrow{\Sigma} q_r$.
Initial states: $I = \{x_1^0, \ldots, x_n^0, q_r\}$, the only nonaccepting state is q_r.
(*Once we have q_a in a configuration, it stays there for the rest of the run, so the run is accepting.*)

We add transitions to q_a from valid literals under clauses they satisfy

$$x_i^0 \xrightarrow{\{a_1,\ldots,a_{n+1}\}\times \mathsf{cl}(\neg x_i)} q_a,$$
$$x_i^1 \xrightarrow{\{a_1,\ldots,a_{n+1}\}\times \mathsf{cl}(x_i)} q_a.$$

Zimin word Z_n

$$I \xrightarrow{(a_1,\ \ )} Y_1 \xrightarrow{(a_2,\ \ )} Y_2 \xrightarrow{(a_1,\ \ )} \qquad \xrightarrow{(a_1,\ \ )} Y_{2^n-1} \xrightarrow{(a_{n+1},\ \ )} Y_{2^n}$$

$$Y \xrightarrow{(a_i,\, C)} Y'$$

if Y satisfies C then $q_a \in Y'$

if Y does not satisfy C and $q_a \notin Y$, then $q_a \notin Y'$

→ if Y satisfies φ, then any choice of C ensures that $q_a \in Y'$

→ if Y does not satisfy φ and $q_a \in Y$, then there is a clause C st $q_a \notin Y'$.

Among „zimin words":
there is a run st. $Y_{2^n} = \{q_r\}$
iff
φ is not satisfiable

Assume φ is satisfiable and $w \in \Sigma^+$ is an arbitrary word ($\epsilon \in L(A_\varphi)$).

Let $u = u_1 \ldots$ be the longest prefix of w that is a "zimin word".

Let l be the minimal number whose binary representation corresponds to an assignment that satisfies φ.

If $|u| \geqslant l$ then $I \xrightarrow{u_1,\ldots,u_l} Y$, the set Y contains an accepting state ($x_i^{b_i}$ for all i). Moreover, by the previous slide, for any symbol $z \in \Sigma$ we have $Y \xrightarrow{z} Y'$ and Y' contains q_a.

If $|u| < l$ then $w = u\ (a_s, C)\ v$ for some word $v \in \Sigma^*$.

This entails $|u| < 2^n - 1$ and the configuration after reading u represents $|u|$ in binary.

Let $a_t \neq a_s$ be the correct first component in a "zimin word"after u.

$I \xrightarrow{u} \{x_n^{b_n}, \dots, x_1^{b_1}\} \cup \{q_r\}$; $(b_n, \dots, b_1)_2 = |u|$

key property of zimin words $\Rightarrow \left(\dots \begin{array}{cccc} b_t & b_{t-1} & \dots & b_1 \\ 0 & 1 & 1 \dots & 1 \end{array} \right)$

the config is $\{\dots, x_t^0, x_{t-1}^1, \dots, x_1^1\} \cup \{q_r\}$

<u>If $s < t$</u>

$$x_s^1 \xrightarrow{\{a_s\} \times \mathcal{C}} q_a$$

<u>if $s > t$</u>

$$x_t^0 \xrightarrow{\{a_s\} \times \mathcal{C}} q_a$$

This can be added to A_P without disrupting the "zimin" runs.