The Iterated Mod Problem

Soham Chatterjee

Chennai Mathematical Institute

October 29, 2023

Contents

Contents

Introduction

- This paper is about the Iterated Mod Problem by Karloff and Ruzzo [KR89]
- Diferente de programas $WYSWYG$;
- Uma apresentação *Beamer* é como qualquer outro documento LaTeX, contém:
  - Preâmbulo e um corpo;
  - O preâmbulo pode-se dizer que é o “índice”, tipo do documento e pacotes;
  - O corpo contém *sections* e *subsections*;
  - Os dispositivos deverão ser estruturados utilizando ambientes de *item* e *enumerate*, ou texto simples (curto).

Contents

Iterated Integer Mod Problem

- Given positive integers $x, m_n, m_{n-1}, \ldots, m_1$ find if

$$((x \bmod m_n) \bmod m_{n-1}) \cdots) \bmod m_1) = 0$$

- We will show this problem is P-complete.
- Since we can replace every $\wedge$ and $\vee$ in a circuit with $NAND$ gate and the size of the circuit still remains polynomial we only consider the circuits with $NAND$ and NOT gates.
- We will show that $NANDCVP$ is log space reducible to IIM.
- An $NANDCVP$ circuit the r nodes $y_1, \ldots, y_r$ of indegree 0 are th inputs and the G nodes with indegree 2 are the gates. The gates are numbers $1, \ldots, G$. The gates are numbered in reverse topological order i.e. every edge is directed from a higher numbered gate to a lower numbered gate and the last gate with gate number 1 is the output with the edge going out of it is 0th edge. The edges $E = 2G + 1$ are numbered so that the two gates into gate g are numbered $2g$ and $2g - 1$.

CVP is P-complete

$NANDCVP \leq_l IIM$

Log-Space Reduction

Let $n = 2G$. The reduction from $NANDCVP$ to the integer iterated mod problem is as follows:

- Let x is $n + 1 = E$-bit integer whose ith bit is Y_j if the ith edge is incident from the input y_j. Otherwise it is 1.
- For $1 \leq g \leq G$ let

$$m_{2g} = 2^{2g} + 2^{2g-1} + \sum_{\substack{j\text{th edge} \\ \text{out-edge from } g}} 2^j \text{ and } m_{2g-1} = 2^{2g-1}$$

This reduction is a log-space reduction from $NANDCVP$ to Integer Iterated Mod problem.

- Here m_{2g} and m_{2g-1} simulate the gate g

The next theorem proves that the output gate of the CVP instance is 0 iff

$$((\cdots((x \bmod m_{2G}) \bmod m_{2g-1})\cdots)) = 0$$

$NANDCVP \leq_l IIM$ I

Correctness

Theorem

Let $x_{G+1} = x$. And for all $1 \leq g \leq G$
$x_g = ((\cdots((x \bmod m_{2G}) \bmod m_{2g-1}) \cdots \bmod m_{2g}) \bmod m_{2g-1}) = 0$. *Then:*

1. *For all $1 \leq g \leq G+1$, $x_g \leq 2^{2g-1}$*
2. *For all $1 \leq g \leq G+1$, $0 \leq j \leq 2g-1$ if the jth edge is an outgoing edge from an input node or from a gate h such that $h \geq g$ then x_g's jth bit is the value carried by jth edge otherwise 1*

Prove by downward induction.

Base Case ($g = G+1$): We have $x < 2^{2(G+1)-1} = 2^{2G+1} = 2^n$. True as x is n-bit number. And second condition follows by constuction. Let the theorem holds for all $g > k$.

$x_k = (x_{k+1} \bmod m_{2k}) \bmod m_{2g-1}$. $m_{2k-1} = 2^{2k-1}$. So x_k has $2k-1$ bits so $x_k < 2^{2k-1}$. So Part (a) is proved.

$NANDCVP \leq_l IIM$ II

Correctness

- The only bits differ between x_{k+1} and x_k are the bits corresponding to edges incident on kth vertex (in and out). In x_{k+1} the jth bits are 1 if jth edge going out from gate k.
- The $2k$ and $2k-1$th edges are in edges of gate k. So in x_{k+1} the $(2k)$th and $(2k-1)$th bits are the value carried by the $(2k)$ and $(2k-1)$th edges. Two cases to consider:
- Both $(2k)$ and $(2k+1)$th bits are 1. $x_{k+1} \geq m_{2k}$ and $x_{k+1} < 2m_{2k}$. So $x_{k+1} \bmod m_{m_{2k}} = x_{k+1} - m_{2k} < 2^{2k-1} \implies x_{k+1} - m_{2k} \bmod m_{2k-1} = x_{k+1} - m_{2k}$. So x_k obtained is deleting the leading two 1's and replacing the 1 in position j by a 0 where jth bit of m_{2k} is 1. So at every edge leaving k has value 0=$NAND(1,1)$
- At least one of the bits $2k, 2k-1$ is 0. Then $x_{k+1} < m_{2k} \implies x_{k+1} \bmod m_{2k} = x_{k+1}$. So x_k has the rightmost $2k-1$ bits of x_{k+1}. So the jth bit of x_k has 1 where jth bit of m_{2k} is 1. So every edge leaving k has value 1=$NAND(1,0) = NAND(0,1) = NAND(0,0)$
- Part (b) is proved

So with previous theorem true after m_1 we have $x_1 < 2^1$ which is the value carried by the 0th edge which is the value of the CVP instance. Hence $NANDCVP \leq IIM$

IIM is P-complete

Theorem

$IIM \in P$

For any 2 numbers a and b, a mod b is in P. Here we are doing n iterated mods. So it still takes polynomial time. So $IIM \in P$.

Theorem

Integer Iterated Mod Problem is P-complete

Contents

Duas *colums*

Exemplo de duas *colums*

\begin{columns}
\column{.4\textwidth}
Left column
\column{.4\textwidth}
Right column
\end{columns}

Left column

Right column

Block

Beamer Introduction

Beamer is a LaTeX class.

itemize

```
\begin{itemize}
\item The first one.
\item The second one.
\begin{itemize}
\item The larger one.
\item The smaller one.
\end{itemize}
\item The third one.
\end{itemize}
```

- The first one.
- The second one.
  - The larger one.
  - The smaller one.
- The third one.

Clique aqui para mais informações.

enumerate

```
\begin{enumerate}
\item The first one.
\item The second one.
\begin{enumerate}
\item The large one.
\item The small one.
\end{enumerate}
\item The third one.
\end{enumerate}
```

1. The first one.
2. The second one.
   1. The large one.
   2. The small one.
3. The third one.

Clique aqui para mais informações.

References I

[KR89] Howard J. Karloff **and** Walter L. Ruzzo. "The iterated mod problem". **in***Information and Computation*: 80.3 (1989), **pages** 193–204. ISSN: 0890-5401. DOI: https://doi.org/10.1016/0890-5401(89)90008-4. URL: https://www.sciencedirect.com/science/article/pii/0890540189900084.