The Iterated Mod Problem

Soham Chatterjee

Chennai Mathematical Institute

November 4, 2023

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.

First we have

Theorem

Iterated Iinteger Mod $\in P$

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 $IIM \in P$.

Circuit Value Problem

To show IIM is P-complete. We will use this theorem.

Theorem

Circuit Value Problem is P-complete.

Since we can replace every $\wedge$, $\vee$, $\neg$ in a circuit with $NAND$ gates and the size of the circuit still remains polynomial we only consider the circuits with $NAND$ and NOT gates.We call this $NANDCVP$.

- A $NANDCVP$ circuit the r nodes $y_1, \ldots, y_r$ of indegree 0 are the inputs
- The G many 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 $2g - 1$.

$NANDCVP \leq_l IIM$

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*

$NANDCVP \leq_l IIM$ II

Correctness

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 $g > k$.

Part (a):

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

Part (b):

- 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:

$NANDCVP \leq_l IIM$ III

Correctness

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=$NAND(1,0) = NAND(0,1) = NAND(0,0)$ 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

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 $NANDCVP \leq IIM$

Theorem

Integer Iterated Mod Problem is P-complete

Contents

Super Increasing Knaspsack Problem (SIK)

Introduction

Definition (0-1 Knapsack Problem)

Given an integer w and a sequence of integers $w_1, w_2, \ldots, w_n$ is there a sequence of $0-1$ valued variables $x_1, \ldots x_n$ such that $w = \sum_{i=1}^{n} x_i w_i$.

- 0-1 Knapsack Problem is known to be NP-complete. [GJ90]
- A knapsack instance is called super increasing (SIK) if each weight w_i is larger than the sum of the previous weights i.e. for all $2 \leq i \leq n$ we have $w_i > \sum_{j=1}^{i-1} w_j$

Theorem

Super Increasing Knaspsack Problem $\in P$

Greedy strategy considering the w_i' in decreasing order gives a linear time algorithm for solving super increasing knapsack problem.

SIK is P-complete I

Theorem

Super Increasing Knapsack Problem is P-complete

We will show $NANDCVP \leq SIK$ and the proof is very much like $NANDCVP \leq IIM$. Here we will consturct base 4 numbers instead of binary. The reduction goes like this:

- Let x is $n+1 = E$-length base 4 number whose ith digit 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

$$m_{2g} = 4^{2g} + 4^{2g-1} + \sum_{\substack{j\text{th edge} \\ \text{out-edge from } g}} 4^j, \;\; m_{2g-0.5} = 4^{2g} - 4^{2g-1}, \;\; m_{2g-1} = 4^{2g-1}$$

Define for all $1 \leq G$,
$x_g = ((\cdots((x \bmod m_{2G}) \bmod m_{2g-1}) \cdots \bmod m_{2g}) \bmod m_{2g-1}) = 0$ and $x_{G+1} = x$.

- $x_k \leq 4^{2k-1}$ for all $1 \leq g \leq G+1$, $x_k < 4^{2g-1}$

SIK is P-complete II

Theorem

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 $g = G + 1$ is true.
- x_{k+1} and x_k differs at the positions corresponding to the edges incident on kth vertex.
- $2k$ and $2k - 1$th edges are in-edges of vertex k so they are the values carried by $2k$ and $2k - 1$th edges

SIK is P-complete III

If both of them 1:
Then

$$4m_{2k} > x_{k+1} \geq m_{2k} \implies x_{k+1} \bmod m_{2k} = x_{k+1} - m_{2k} < 4^{2k-1}$$

So

$$(x_{k+1} - m_{2k} \bmod m_{2k-0.5}) \bmod m_{2k-1} = x_{k+1} - m_{2k}$$

In x_k the positions where m_{2k} has 1 will have 0=$NAND(1,1)$
If at least one of them 0:
Then $x_{k+1} \bmod m_{2k} = x_{k+1}$. So after that the positions in x_k where m_{2k} has 1 will have 1=$NAND(1,0) = NAND(0,1) = NAND(0,0)$. Now

$$x_{k+1} = a \times 4^{2k} + b \times 4^{2k-1} + c$$

where $a, b \in \{0,1\}$.

- $a = 1, b = 0$:

$$(x_{k+1} \bmod m_{2k-0.5}) \bmod m_{2k-1} = 1 \times 4^{2k-1} + c \bmod m_{2k-1} = c$$

- $b = 0/1$:

$$(x_{k+1} \bmod m_{2k-0.5}) \bmod m_{2k-1} = b \times 4^{2k-1} + c \bmod m_{2k-1} = c$$

SIK is P-complete IV

Using this theorem like in the Iterated Integer Mod 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.

- **Notice**: The modulos satisfies the super increasing knapsack problem.

Since

$$\sum_{g=1}^{k} m_{2g} + m_{2g-0.5} + m_{2g-1} = \sum_{g=1}^{k} m_{2g} + 4^{2g} < 4^{2k+1} = m_{2(k+1)-1}$$

So:

1. Sum of weights till m_{2k} is strictly $< m_{2(k+1)-1}$
2. $$\begin{aligned}\text{Sum of weights till } m_{2k-1} &= (\text{sum of weights till } m_{2k}) + m_{2(k+1)-1}\\ &< 2\times 4^{2(k+1)-1} < 3\times 4^{2(k+1)-1} = m_{2(k+1)-0.5}\end{aligned}$$
3. $$\begin{aligned}\text{Sum of weights till } m_{2k-0.5} &= (\text{sum of weights till } m_{2k}) + m_{2(k+1)-1} + m_{2(k+1)-0.5}\\ &< 2\times 4^{2(k+1)-1} + 3\times 4^{2(k+1)+1}\\ &= 4^{2(k+1)} + 4^{2(k+1)-1} < m_{2(k+1)}\end{aligned}$$

SIK is P-complete V

Theorem

If $w_1, \ldots, w_n$ are such that $\forall\, i \in [n-1]\ \sum_{k=1}^{i} w_k < w_{i+1}$ then there is a 0-1 sequence of variables $x_1, \ldots, x_n$ such that $\sum_{i=1}^{n} x_i w_i = w$ iff

$$((\cdots((w \bmod w_n) \bmod w_{n-1})\cdots) \bmod w_2) \bmod w_1 = 1$$

So now we have an reduction of $NANDCVP$ to SIK.

Contents

Polynomial Iterated Mod Problem

Introduction

Definition (Polynomial Iterated Mod Problem)

Given univariate polynomials $a(x), b_1(x), \ldots, b_n(x)$ over a field $\mathbb{F}$ compute the residue $((\cdots((a(x) \bmod b_1(x)) \bmod b_2(x)) \cdots \bmod b_{n-1}(x)) \bmod b_n(x))$

PIM is in NC

Beamer Introduction

Beamer is a LaTeX class.

References

[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.

[GJ90] Michael R. Garey **and** David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. USA: W. H. Freeman & Co., 1990. ISBN: 0716710455.