

The Iterated Mod Problem

Soham Chatterjee

Chennai Mathematical Institute

November 9, 2023

Contents

- 1 Iterated Integer Mod (IIM) Problem
 - Circuit Value Problem
 - $NANDCVP \leq_I IIM$
- 2 Super Increasing 0-1 Knapsack Problem
 - Introduction
 - Super Increasing Knapsack Problem is P -complete
- 3 Polynomial Iterated Mod Problem (PIM)
 - Introduction
 - PIM is in NC

Introduction

- This paper is about the Iterated Mod Problem by Karloff and Ruzzo [**iteratedmod**]
- 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

- 1 Iterated Integer Mod (IIM) Problem
 - Circuit Value Problem
 - $NANDCVP \leq_I IIM$
- 2 Super Increasing 0-1 Knapsack Problem
 - Introduction
 - Super Increasing Knapsack Problem is P -complete
- 3 Polynomial Iterated Mod Problem (PIM)
 - Introduction
 - PIM is in NC

Iterated Integer Mod Problem

Problem:

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

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

Theorem

Iterated Integer Mod $\in P$

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

Circuit Value Problem

Theorem

Circuit Value Problem is P-complete.

- Enough to take CVP for circuits with only $NAND$ gates, $NANDCVP$

$Gates \in [G]$

Input Variables: $y_i, i \in [r]$, Input Bits: $Y_i, i \in [r]$

$NANDCVP \leq_I IIM$

Log-Space Reduction

Let $n = 2G$.

- x is $n + 1$ -bit integer whose i th bit is Y_j if the i th edge is incident from the input y_j . Otherwise it is 1.
- $1 \leq g \leq G$

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

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

$NANDCVP \leq_I IIM$

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 j th edge is an outgoing edge from an input node or from a gate h such that $h \geq g$ then x_g 's j th bit is the value carried by j th edge otherwise 1

$NANDCVP \leq_I IIM$

Correctness

Prove by downward induction:

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

$NANDCVP \leq_I IIM$ III

Correctness

Part (a):

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

$NANDCVP \leq_I IIM IV$

Correctness

Part (b):

- The only bits differ between x_{k+1} and x_k are the bits corresponding to edges incident on k th vertex (in and out). In x_{k+1} the j th bits are 1 if j th 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:

$NANDCVP \leq_I IIM$

Correctness

Both $(2k)$ and $(2k + 1)$ th bits are 1:

$m_{2k} \leq x_{k+1} < 2m_{2k}$. So

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

So in x_{2k} at output bits position of m_{2k} the 1 is replaced by 0

At least one of the bits is 0:

$$x_{k+1} < m_{2k} \implies x_{k+1} \bmod m_{2k} = x_{k+1}$$

So in x_{2k} at output bits position of m_{2k} has 1.

IIM is P-complete

$x_1 < 2^1$ is the value carried by the 0th edge, value of the *CVP* instance.

Theorem

$NANDCVP \leq_I \text{Iterated Integer Mod}$

Theorem

Integer Iterated Mod Problem is P-complete

Contents

- 1 Iterated Integer Mod (IIM) Problem
 - Circuit Value Problem
 - $NANDCVP \leq_I IIM$
- 2 Super Increasing 0-1 Knapsack Problem
 - Introduction
 - Super Increasing Knapsack Problem is P -complete
- 3 Polynomial Iterated Mod Problem (PIM)
 - Introduction
 - PIM is in NC

Super Increasing Knapsack Problem (SIK)

Introduction

Definition (0-1 Knapsack Problem)

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

- 0-1 Knapsack Problem is known to be NP -complete.
 [guidetontpc]
- 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 $w_i > \sum_{j=1}^{i-1} w_j$

Super Increasing Knapsack Problem (SIK)

Introduction

Theorem

Super Increasing Knapsack 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

We will show $NANDCVP \leq SIK$. For that we will reduce $NANDCVP$ to a special instance of IIM which is reducible to SIK .

- Let x is $n + 1$ -length base 4 number whose i th digit is Y_j if the i th edge is incident from the input y_j . Otherwise it is 1.
- $1 \leq g \leq G$

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

$$m_{2g-0.5} = 4^{2g} - 4^{2g-1}, \quad m_{2g-1} = 4^{2g-1}$$

SIK is P -complete II

Define for all $1 \leq g \leq G$,

$$x_g = (((\cdots ((x \bmod m_{2G}) \bmod m_{2G-0.5}) \bmod m_{2G-1}) \cdots \bmod m_{2g}) \bmod m_{2g-0.5}) \bmod m_{2g-1}) = 0 \text{ and } x_{G+1} = x.$$

- $x_g \leq 4^{2^{g-1}}$ for all $1 \leq g \leq G+1$

SIK is P -complete III

Theorem

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

SIK is P -complete IV

- 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 k th 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 V

If both of them 1:

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

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

In x_k the positions where m_{2k} has 1 will have 0.

SIK is P -complete VI

If at least one of them 0:

$x_{k+1} \bmod m_{2k} = x_{k+1}$. In x_k positions where m_{2k} has 1 will have 1.

$$x_{k+1} = a \times 4^{2k} + b \times 4^{2k-1} + c \text{ where } a, b \in \{0, 1\}$$

- $a = 1, b = 0$:

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

- $b = 0, 1$:

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

SIK is P -complete VII

After m_1 , $x_1 < 2^1$ is the value carried by the 0th edge, the value of the CVP.

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

Since

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

SIK is P -complete VIII

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

SIK is P -complete IX

Theorem

If w_1, \dots, 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, \dots, x_n such that $\sum_{i=1}^n x_i w_i = w$ iff

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

SIK is P -complete X

Theorem

$NANDCVP \leq_1 \text{Super Increasing Knapsack}$

Theorem

Super Increasing Knapsack Problem is P -complete.

Contents

- 1 Iterated Integer Mod (*IIM*) Problem
 - Circuit Value Problem
 - $NANDCVP \leq_l IIM$
- 2 Super Increasing 0-1 Knapsack Problem
 - Introduction
 - Super Increasing Knapsack Problem is *P*-complete
- 3 Polynomial Iterated Mod Problem (*PIM*)
 - Introduction
 - *PIM* is in *NC*

Polynomial Iterated Mod Problem

Introduction

Definition (Polynomial Iterated Mod Problem)

Given univariate polynomials $a(x), b_1(x), \dots, b_n(x)$ 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