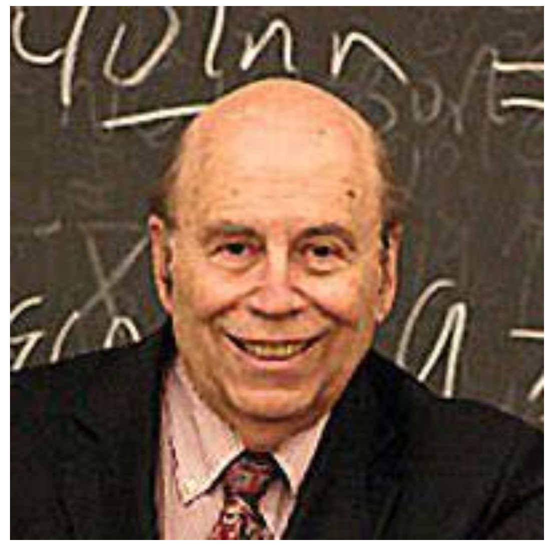
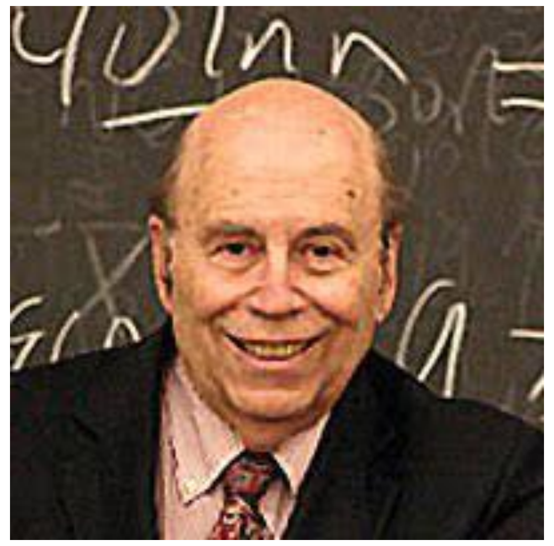
Presburger Arithmetic

a non polynomial lower bound

results of this chapter from: M.J. Fisher and M. Rabin 1973



results of this chapter from: M.J. Fisher and M. Rabin 1973



my role model for teaching

1 Background

1.1 Undecidabitlity of elementary arithmetic Z_E

review: Z_E**:**

- dealing with elements in $\mathbb{N}_0$
- Peano axioms
- predicates involving $=, +, \cdot$
- truth of predicates/statements undecidable

1 Background

1.1 Undecidabitlity of elementary arithmetic Z_E

review: Z_E:

- dealing with elements in $\mathbb{N}_0$
- Peano axioms
- predicates involving $=, +, \cdot$
- truth of predicates/statements undecidable

the crucial predicate: Consider 1-tape TM

$$M_u = (Z, A, \delta, z_0, E)$$

and $v \in \mathbb{B}^*$. M_u started with v halts iff

$$\exists w.\ w = \$k_0\$ \ldots \$k_t\$ \quad , \quad w \in (A \cup Z \cup \{\$\})^+$$

with

1. $k_0 = B \ldots B z_0 v B \ldots B$
2. $k_i \vdash k_{i+1}$ for $i < t$
3. $|k_i| = |k_j|$ for all i, j
4. in no k_i if a $z \in Z$ first or last element
5. k_t is endconfiguraion

$$H(u\#v) :\equiv \exists w\ (1) \wedge (2) \wedge (3) \wedge (4) \wedge (5)$$

1.1 Undecidabitlity of elementary arithmetic Z_E

review: Z_E:

- dealing with elements in $\mathbb{N}_0$
- Peano axioms
- predicates involving $=, +, \cdot$
- truth of predicates/statements undecidable

the crucial predicate: Consider 1-tape TM

$$M_u = (Z, A, \delta, z_0, E)$$

and $v \in \mathbb{B}^*$. M_u started with v halts iff

$$\exists w.\ w = \$k_0\$\ldots\$k_t\$ \quad , \quad w \in (A \cup Z \cup \{\$\})^+$$

with

1. $k_0 = B \ldots B z_0 v B \ldots B$
2. $k_i \vdash k_{i+1}$ for $i < t$
3. $|k_i| = |k_j|$ for all i, j
4. in no k_i if a $z \in Z$ first or last element
5. k_t is endconfiguraion

$$H(u\#v) :\equiv \exists w\ (1) \wedge (2) \wedge (3) \wedge (4) \wedge (5)$$

1.2 Bounding the length of strings involved

parameters:

- for fixed machine $M = (Z, A, \delta, z_0, Z_A)$
- input size $|v| = n$
- step number $t \geq n$.

length of strings involved

- configurations with state and surrounding blanks:

$$|k_i| \leq t + 3$$

- word w with $t+1$ configurations and $t+1$ separation signs \$:

$$|w| \leq (t+4) \cdot (t+1) + 1$$

1.2 Bounding the length of strings involved

parameters:

- for fixed machine $M = (Z, A, \delta, z_0, Z_A)$
- input size $|v| = n$
- step number $t \geq n$.

length of strings involved

- configurations with state and surrounding blanks:

$$|k_i| \leq t + 3$$

- word w with $t+1$ configurations and $t+1$ separation signs \$:

$$|w| \leq (t+4) \cdot (t+1) + 1$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
  $$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to

$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$

$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

1.2 Bounding the length of strings involved

parameters:

- for fixed machine $M = (Z, A, \delta, z_0, Z_A)$
- input size $|v| = n$
- step number $t \geq n$.

length of strings involved

- configurations with state and surrounding blanks:

$$|k_i| \leq t + 3$$

- word w with $t+1$ configurations and $t+1$ separation signs \$:

$$|w| \leq (t+4) \cdot (t+1) + 1$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

-
$$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
$$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

-
$$\psi(\varepsilon) = 0$$

- extend to
$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))}$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
$$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))}$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
  $$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
  $$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
  $$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\le p^{|w|} \\ &\le 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \end{aligned}$$

Lemma 1. *For computations with $t \ge |v| = n$ steps*

$$\psi(w) \le 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

1.4 estimating the length of predicate $H(u\#v)$:

(1): with coding the input

- $$\begin{aligned} & \exists k \ \exists m \exists a \ \exists b \exists c \\ (w \quad = \quad & [\hat{\$}, k, \hat{\$}, m] \\ & \wedge\, k = [a, b, c] \\ & \wedge\, a = \psi(B \ldots B) \\ & \wedge\, c = \psi(B \ldots B) \\ & b = \psi(z_0 v_{n-1} \ldots v_0)) \end{aligned}$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
  $$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
  $$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
  $$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

1.4 estimating the length of predicate $H(u\#v)$:

(1): with coding the input

- $$\begin{aligned} & && \exists k\ \exists m \exists a\ \exists b \exists c \\ (w &= && [\hat{\$}, k, \hat{\$}, m] \\ & && \wedge k = [a,b,c] \\ & && \wedge a = \psi(B \ldots B) \\ & && \wedge c = \psi(B \ldots B) \\ & && b = \psi(z_0 v_{n-1} \ldots v_0)) \end{aligned}$$

- $\sigma(d,a)$: d codes a single symbol in $\psi^{-1}(a)$

$$\sigma(d,a) :\equiv \exists e\ \exists f\ (a = [e,d,f]\ \wedge d < \overline{p} \wedge\ \sim d = 0)$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
$$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \; (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned}\psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}\end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

1.4 estimating the length of predicate $H(u\#v)$:

(1): with coding the input

- $$\begin{aligned} & && \exists k\ \exists m \exists a\ \exists b \exists c \\ (w &= && [\hat{\$}, k, \hat{\$}, m] \\ & && \wedge\, k = [a,b,c] \\ & && \wedge\, a = \psi(B \ldots B) \\ & && \wedge\, c = \psi(B \ldots B) \\ & && b = \psi(z_0 v_{n-1} \ldots v_0))\end{aligned}$$

- $\sigma(d,a)$: d codes a single symbol in $\psi^{-1}(a)$
$$\sigma(d,a) :\equiv \exists e\ \exists f\ (a = [e,d,f]\ \wedge d < \overline{p} \wedge\ \sim d = 0)$$

- $$a = \psi(B \ldots B) \quad :\equiv \forall d\ (\sigma(d,a) \to d = \hat{B})$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

-
$$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
$$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

-
$$\psi(\varepsilon) = 0$$

- extend to
$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

1.4 estimating the length of predicate $H(u\#v)$:

(1): with coding the input

-
$$\begin{aligned} & && \exists k\ \exists m \exists a\ \exists b \exists c \\ (w &= && [\hat{\$}, k, \hat{\$}, m] \\ & && \wedge\ k = [a, b, c] \\ & && \wedge\ a = \psi(B \ldots B) \\ & && \wedge\ c = \psi(B \ldots B) \\ & && b = \psi(z_0 v_{n-1} \ldots v_0)) \end{aligned}$$

- $\sigma(d,a)$: d codes a single symbol in $\psi^{-1}(a)$

$$\sigma(d,a) :\equiv \exists e\ \exists f\ (a = [e,d,f]\ \wedge d < \overline{p} \wedge\ \sim d = 0)$$

-
$$a = \psi(B \ldots B) \quad :\equiv \forall d\ (\sigma(d,a) \to d = \hat{B})$$

- Horner scheme for $\psi(z_0 v)$

$$\begin{aligned} b = \psi(z_0 v) \quad &:\equiv && \exists y_0 \ldots \exists y_s \\ (y_s &= && \hat{z}_0\ \wedge \\ y_{s-1} &= && \overline{p} \cdot y_s + \widehat{v_{s-1}} \\ & \ldots && \\ y_0 &= && \overline{p} \cdot y_1 + \hat{v}_0) \end{aligned}$$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

-
$$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
$$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

-
$$\psi(\varepsilon) = 0$$

- extend to
$$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
$$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p) \cdot ((t+4) \cdot (t+1) + 1))}$$

1.4 estimating the length of predicate $H(u\#v)$:

(1): with coding the input

-
$$\begin{aligned} & && \exists k \ \exists m \exists a \ \exists b \exists c \\ (w &= && [\hat{\$}, k, \hat{\$}, m] \\ & && \wedge k = [a, b, c] \\ & && \wedge a = \psi(B \ldots B) \\ & && \wedge c = \psi(B \ldots B) \\ & && b = \psi(z_0 v_{n-1} \ldots v_0)) \end{aligned}$$

- $\sigma(d, a)$: d codes a single symbol in $\psi^{-1}(a)$

$$\sigma(d,a) :\equiv \exists e \ \exists f \ (a = [e, d, f] \ \wedge d < \overline{p} \wedge \ \sim d = 0)$$

-
$$a = \psi(B \ldots B) \quad :\equiv \forall d \ (\sigma(d,a) \to d = \hat{B})$$

- Horner scheme for $\psi(z_0 v)$

$$\begin{aligned} b = \psi(z_0 v) \quad :\equiv & \quad \exists y_0 \ldots \exists y_s \\ (y_s &= \hat{z_0} \ \wedge \\ y_{s-1} &= \overline{p} \cdot y_s + \widehat{v_{s-1}} \\ & \ldots \\ y_0 &= \overline{p} \cdot y_1 + \hat{v_0}) \end{aligned}$$

- coding input by predicate of length $O(n)$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
  $$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
  $$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
  $$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

- coding input by predicate of length $O(n)$

1.3 Bounding the size of numbers involved

coding strings in numbers Let

$$p > \#A + \#Z + 2 \quad \text{prime number}$$

Interpret $w \in (A \cup Z \cup \{\$\})^*$ as number representation to base p.

- $$\psi : A \cup Z \cup \{\$\} \to [1 : p-1]$$
  $$\hat{a} = \overline{\psi(a)} = 1 + \ldots + 1 \ (\psi(a) \text{ times})$$

- $$\psi(\varepsilon) = 0$$

- extend to
  $$\psi : (A \cup Z \cup \{\$\})^* \to [1 : p-1]$$
  $$\psi(w[s-1:0]) = \sum_{i=1}^{s-1} \psi(w_i) \cdot p^i$$

$$\begin{aligned} \psi(w) &\leq p^{|w|} \\ &\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \end{aligned}$$

Lemma 1. *For computations with $t \geq |v| = n$ steps*

$$\psi(w) \leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))}$$

- coding input by predicate of length $O(n)$

- for fixed machine M (and variable v) all other parts of $H(u\#v)$ have length $O(1)$

Lemma 2. *For fixed machines $M = M_u$*

$$|H(u\#v)| = O(n)$$

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)
- intermediate result: omit multiplication

def: Presburger arithmetic

- Presburger arithmetic Z_P is Z_E without multiplication.
- decidable (around 1929)
- in time $2^{2^{2^{O(n \log n)}}}$ (D.C. Oppen, ACM STOC 1973)

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)
- intermediate result: omit multiplication

def: Presburger arithmetic

- Presburger arithmetic Z_P is Z_E without multiplication.
- decidable (around 1929)
- in time $2^{2^{2^{O(n\log n)}}}$ (D.C. Oppen, ACM STOC 1973)

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \text{ is true}\}$$

is EXPTIME-hard

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)
- intermediate result: omit multiplication

def: Presburger arithmetic

- Presburger arithmetic Z_P is Z_E without multiplication.
- decidable (around 1929)
- in time $2^{2^{2^{O(n\log n)}}}$ (D.C. Oppen, ACM STOC 1973)

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \text{ is true}\}$$

is EXPTIME-hard

- Let

$$L \in TIME(2^{Cn})$$

- Let $M = M_u$ be 2^{Cn}-time bounded 1-tape TM accepting L
- we show

$$L \leq_p Z_P$$

by constructing for input v with $|v| = n$ a predicate

$$H_n(u\#v) \in L_P$$

which is true iff $M = M_u$ started with v halts in an accepting state.

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)
- intermediate result: omit multiplication

def: Presburger arithmetic

- Presburger arithmetic Z_P is Z_E without multiplication.
- decidable (around 1929)
- in time $2^{2^{2^{O(n\log n)}}}$ (D.C. Oppen, ACM STOC 1973)

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \text{ is true}\}$$

is EXPTIME-hard

- Let

$$L \in TIME(2^{Cn})$$

- Let $M = M_u$ be 2^{Cn}-time bounded 1-tape TM accepting L
- we show

$$L \leq_p Z_P$$

by constructing for input v with $|v| = n$ a predicate

$$H_n(u\#v) \in L_P$$

which is true iff $M = M_u$ started with v halts in an accepting state.

- length of the computation:

$$t = 2^{Cn}$$

2 Presburger Arithmetic

- Recall Hilbert's program:
- show that Z_E is decidable
- possibly with very complex algorithms (which couldn't work)
- intermediate result: omit multiplication

def: Presburger arithmetic

- Presburger arithmetic Z_P is Z_E without multiplication.
- decidable (around 1929)
- in time $2^{2^{2^{O(n\log n)}}}$ (D.C. Oppen, ACM STOC 1973)

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \;:\; A \text{ is true}\}$$

is EXPTIME-hard

- Let
$$L \in TIME(2^{Cn})$$
- Let $M = M_u$ be 2^{Cn}-time bounded 1-tape TM accepting L
- we show
$$L \leq_p Z_P$$
by constructing for input v with $|v| = n$ a predicate
$$H_n(u\#v) \in L_P$$
which is true iff $M = M_u$ started with v halts in an accepting state.
- length of the computation:
$$t = 2^{Cn}$$
- size of the numbers involved

$$\begin{aligned}
\psi(w) &\leq p^{|w|} \\
&\leq 2^{(\log p)\cdot((t+4)\cdot(t+1)+1))} \quad \text{(lemma 1)} \\
&\leq 2^{(\log p)\cdot((2^{Cn}+4)\cdot(2^{Cn}+1)+1))} \\
&\leq 2^{2^{3Cn}}
\end{aligned}$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \quad \equiv \quad & a = 0 \wedge c = 0 \\ & \vee \left(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \right. \\ & \left. \wedge\, c = b + \ldots + b \quad (i \text{ times})) \right. \end{aligned}$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \; \wedge \; a \leq p_n \; \rightarrow \; a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \quad \equiv \quad & a = 0 \wedge c = 0 \\ & \vee \, (\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \\ & \wedge \, c = b + \ldots + b \quad (i \text{ times})) \end{aligned}$$

$n \rightarrow n+1$**:**

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \to a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \equiv\ & a = 0 \wedge c = 0 \\ & \vee (\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \\ & \wedge c = b + \ldots + b \quad (i \text{ times})) \end{aligned}$$

$n \to n+1$:

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

$$\begin{aligned} a_1 = a_2 &= \lfloor \sqrt{a} \rfloor \\ &= \sqrt{a} - b \quad \text{with} \quad b < 1 \\ a_3 + a_4 &= 2b\sqrt{a} - b^2 \\ &= 2b(\lfloor \sqrt{a} \rfloor + b) - b^2 \\ &= 2b\lfloor \sqrt{a} \rfloor + b^2 \\ &< 2b\lfloor \sqrt{a} \rfloor + 1 \end{aligned}$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \equiv\ & a = 0 \wedge c = 0 \\ & \vee \left(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \right. \\ & \left. \wedge\, c = b + \ldots + b \quad (i \text{ times})\right) \end{aligned}$$

$n \rightarrow n+1$:

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

$$\begin{aligned} a_1 = a_2 &= \lfloor \sqrt{a} \rfloor \\ &= \sqrt{a} - b \quad \text{with} \quad b < 1 \\ a_3 + a_4 &= 2b\sqrt{a} - b^2 \\ &= 2b(\lfloor \sqrt{a} \rfloor + b) - b^2 \\ &= 2b\lfloor \sqrt{a} \rfloor + b^2 \\ &< 2b\lfloor \sqrt{a} \rfloor + 1 \end{aligned}$$

the naive recursion:

$$\begin{aligned} m_{n+1}(a,b,c) \equiv\ & \exists p, a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & m_n(a_1, a_2, p) \wedge \\ & m_n(a_1, b, c_1) \wedge m_n(a_2, c_1, c_2) \wedge \\ & m_n(a_3, b, c_3) \wedge m_n(a_4, b, c_4) \wedge \\ & c = c_2 + c_3 + c_4 \wedge a = p + a_3 + a_4 \end{aligned}$$

2.2 Expressing multiplication $a \cdot b = c$ for bounded a in Z_P

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \quad \equiv \quad & a = 0 \wedge c = 0 \\ & \vee \left(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \right. \\ & \left. \wedge\, c = b + \ldots + b \quad (i \text{ times})\right) \end{aligned}$$

$n \rightarrow n+1$:

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

$$\begin{aligned} a_1 = a_2 \quad &= \quad \lfloor \sqrt{a} \rfloor \\ &= \quad \sqrt{a} - b \quad \text{with} \quad b < 1 \\ a_3 + a_4 \quad &= \quad 2b\sqrt{a} - b^2 \\ &= \quad 2b(\lfloor \sqrt{a} \rfloor + b) - b^2 \\ &= \quad 2b\lfloor \sqrt{a} \rfloor + b^2 \\ &< \quad 2b\lfloor \sqrt{a} \rfloor + 1 \end{aligned}$$

the naive recursion:

$$\begin{aligned} m_{n+1}(a,b,c) \quad \equiv \quad & \exists p, a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & m_n(a_1, a_2, p) \wedge \\ & m_n(a_1, b, c_1) \wedge m_n(a_2, c_1, c_2) \wedge \\ & m_n(a_3, b, c_3) \wedge m_n(a_4, b, c_4) \wedge \\ & c = c_2 + c_3 + c_4 \wedge a = p + a_3 + a_4 \end{aligned}$$

unfortunately the length would grow too fast

$$|m_n| \geq 5^n$$

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \quad \equiv \quad & a = 0 \wedge c = 0 \\ & \vee \left(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times})\right. \\ & \left. \wedge\, c = b + \ldots + b \quad (i \text{ times})\right) \end{aligned}$$

$n \rightarrow n+1$:

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

$$\begin{aligned} m_{n+1}(a,b,c) \quad \equiv \quad & \exists a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & m_n(a_1,b,c_1) \wedge m_n(a_2,c_1,c_2) \wedge \\ & m_n(a_3,b,c_3) \wedge m_n(a_4,b,c_4) \wedge \\ & c = c_2 + c_3 + c_4 \end{aligned}$$

recursion with parameters:

$$\begin{aligned} m_{n+1}(a,b,c) \quad \equiv \quad & \exists p, a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & \forall d, e, f. \\ & (((d = a_1 \wedge e = a_2 \wedge f = p) \vee \\ & (d = a_1 \wedge e = b \wedge f = c_1) \vee \\ & (d = a_2 \wedge e = c_1 \wedge f = c_2) \vee \\ & (d = a_3 \wedge e = b \wedge f = c_3) \vee \\ & (d = a_4 \wedge e = b \wedge f = c_4) \\ & \rightarrow m_n(d,e,f)) \\ & \wedge\, c = c_2 + c_3 + c_4 \wedge a = p + a_3 + a_4) \end{aligned}$$

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \equiv\ & a = 0 \wedge c = 0 \\ & \vee \Big(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \\ & \wedge c = b + \ldots + b \quad (i \text{ times})\Big) \end{aligned}$$

$n \rightarrow n+1$**:**

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

$$\begin{aligned} m_{n+1}(a,b,c) \equiv\ & \exists a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & m_n(a_1,b,c_1) \wedge m_n(a_2,c_1,c_2) \wedge \\ & m_n(a_3,b,c_3) \wedge m_n(a_4,b,c_4) \wedge \\ & c = c_2 + c_3 + c_4 \end{aligned}$$

recursion with parameters:

$$\begin{aligned} m_{n+1}(a,b,c) \equiv\ & \exists p, a_1, \ldots, a_4, c_1, \ldots, c_4. \\ & \forall d, e, f. \\ & (((d = a_1 \wedge e = a_2 \wedge f = p) \vee \\ & (d = a_1 \wedge e = b \wedge f = c_1) \vee \\ & (d = a_2 \wedge e = c_1 \wedge f = c_2) \vee \\ & (d = a_3 \wedge e = b \wedge f = c_3) \vee \\ & (d = a_4 \wedge e = b \wedge f = c_4) \\ & \rightarrow m_n(d,e,f)) \\ & \wedge c = c_2 + c_3 + c_4 \wedge a = p + a_3 + a_4) \end{aligned}$$

length of m_n: *counting length of variables as* 1

$$L(n) = |m_n(a,b,c)|$$

then

$$\begin{aligned} L(1) &= O(1) \\ L(n+1) &= L(n) + O(1) \\ L(n) &= O(n) \end{aligned}$$

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proof: obviously by induction on n

$n = 1$:

$$2^{2^1} = 4$$

$$\begin{aligned} m_1(a,b,c) \equiv\ & a = 0 \wedge c = 0 \\ & \vee \Big(\bigvee_{i=1}^{4} (a = 1 + \ldots + 1 \quad (i \text{ times}) \\ & \wedge c = b + \ldots + b \quad (i \text{ times})\Big) \end{aligned}$$

$n \rightarrow n+1$**:**

Lemma 5. *For every $a \in \mathbb{N}$ there are natural numbers*

$$a_1, a_2, a_3, a_4 \leq \lfloor \sqrt{a} \rfloor$$

such that

$$a = a_1 \cdot a_2 + a_3 + a_4$$

length of m_n: *counting length of variables as* 1

$$L(n) = |m_n(a,b,c)|$$

then

$$\begin{aligned} L(1) &= O(1) \\ L(n+1) &= L(n) + O(1) \\ L(n) &= O(n) \end{aligned}$$

size of operands a If

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow c = a \cdot b$$

then

$$m_{n+1}(a,b,c) \wedge a \leq p_n^2 + 2p_n \rightarrow c = a \cdot b$$

$$\begin{aligned} p_1 &= 4 \\ p_{n+1} &> p_n^2 \end{aligned}$$

Lemma 6.

$$p_n \geq 2^{2^n}$$

Proof. easy induction

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \text{ is true}\}$$

is EXPTIME-hard

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \ \wedge \ a \leq p_n \ \rightarrow \ a \cdot b = c$$

proving lemma 3:

- for $|v| = n$ and $M = M_u$ obtain predicate $H_n(M,v)$ by replacing in $H(u\#v)$ every occurrence of a predicate $a = b \cdot c$ by $m_{3Cn}(a,b,c)$

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \textit{ is true}\}$$

is EXPTIME-hard

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \ \wedge \ a \leq p_n \ \rightarrow \ a \cdot b = c$$

proving lemma 3:

- for $|v| = n$ and $M = M_u$ obtain predicate $H_n(M,v)$ by replacing in $H(u\#v)$ every occurrence of a predicate $a = b \cdot c$ by $m_{3Cn}(a,b,c)$

- operands a in $m_{3Cn}(a,b,c)$ small enough.

$$p_{3Cn} \geq 2^{2^{3Cn}} \geq \psi(w)$$

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \textit{ is true}\}$$

is EXPTIME-hard

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \ \wedge \ a \leq p_n \ \rightarrow \ a \cdot b = c$$

proving lemma 3:

- for $|v| = n$ and $M = M_u$ obtain predicate $H_n(M,v)$ by replacing in $H(u\#v)$ every occurrence of a predicate $a = b \cdot c$ by $m_{3Cn}(a,b,c)$

- operands a in $m_{3Cn}(a,b,c)$ small enough.

$$p_{3Cn} \geq 2^{2^{3Cn}} \geq \psi(w)$$

- length measured in variables (Lemma 2):

$$|H_{3Cn}(u\#v)| = |H(u\#v)| \cdot O(L(3Cn)) = O(n^2)$$

- indexing variable names with binary or decimal numers

$$|H_{3Cn}(u\#v)| = O(n^2 \log n)$$

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \;:\; A \text{ is true}\}$$

is EXPTIME-hard

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proving lemma 3:

- for $|v| = n$ and $M = M_u$ obtain predicate $H_n(M,v)$ by replacing in $H(u\#v)$ every occurrence of a predicate $a = b \cdot c$ by $m_{3Cn}(a,b,c)$

- operands a in $m_{3Cn}(a,b,c)$ small enough.

$$p_{3Cn} \geq 2^{2^{3Cn}} \geq \psi(w)$$

- length measured in variables (Lemma 2):

$$|H_{3Cn}(u\#v)| = |H(u\#v)| \cdot O(L(3Cn)) = O(n^2)$$

- indexing variable names with binary or decimal numers

$$|H_{3Cn}(u\#v)| = O(n^2 \log n)$$

3 A lower bound

- time hierarchy theorem

$$P \subsetneq EXPTIME$$

- $T_P \in P$ and T_P EXPTIME-hard would imply $EXPTIME \subseteq P$

Lemma 7.

$$T_P \notin P$$

2.1 EXPTIME hardness

proof system

$$Z_P = (\Sigma_P, L_P, A_P, S_P)$$

Lemma 3. *The language of true predicates of Z_P*

$$T_P = \{A \in L_P \ : \ A \text{ is true}\}$$

is EXPTIME-hard

Lemma 4. *There is a predicate $m_n(a,b,c)$ of Z_P and there are numbers*

$$p_n \geq 2^{2^n}$$

such that

$$m_n(a,b,c) \wedge a \leq p_n \rightarrow a \cdot b = c$$

proving lemma 3:

- for $|v| = n$ and $M = M_u$ obtain predicate $H_n(M,v)$ by replacing in $H(u\#v)$ every occurrence of a predicate $a = b \cdot c$ by $m_{3Cn}(a,b,c)$

- operands a in $m_{3Cn}(a,b,c)$ small enough.

$$p_{3Cn} \geq 2^{2^{3Cn}} \geq \psi(w)$$

- length measured in variables (Lemma 2):

$$|H_{3Cn}(u\#v)| = |H(u\#v)| \cdot O(L(3Cn)) = O(n^2)$$

- indexing variable names with binary or decimal numers

$$|H_{3Cn}(u\#v)| = O(n^2 \log n)$$

3 A lower bound

- time hierarchy theorem

$$P \subsetneq EXPTIME$$

- $T_P \in P$ and T_P EXPTIME-hard would imply $EXPTIME \subseteq P$

Lemma 7.

$$T_P \notin P$$

exercise: try to derive a concrete lower bound for the run time $t(n)$ of Turing machines deciding Z_P, e.g.

$$t(n) \geq 2^{\sqrt[3]{n}}$$