More on negative results

- We proved that the following problems are not in P:

  ATM

  Incompressible strings

  A certain language in EXP

- By reduction, we proved that more problems are not in P

- These problems do not include many we really care about,

  like SAT

- It is believed that SAT is not in P (equivalently, $P \neq NP$).

- In fact, most people believe that SAT $\notin$ TIME($2^{0.01n}$)

- The best result in this direction is SAT $\notin$ TIME(n^2)

  We now prove it, in fact for a much simpler language.

- Recall a string is palindrome if it reads the same both ways
  Example: 00100, 10100101

- Definition: PAL := $\{w : w \in \{0,1\}^n$ and w is palindrome$\}$

  Can you think of a TM that decides PAL,

  and what is its running time?

- Recall a string is palindrome if it reads the same both ways
  Example: 00100, 10100101

- Definition: PAL := {w : w $\in$ $\{0,1\}^n$ and w is palindrome}

- Claim: PAL $\in$ TIME($c\, n^2$) for a constant c

- Proof:

M :=

“ On input w

??????

- Recall a string is palindrome if it reads the same both ways
  Example: 00100, 10100101

- Definition: PAL := {w : w $\in$ $\{0,1\}^n$ and w is palindrome}

- Claim: PAL $\in$ TIME($c\ n^2$) for a constant c

- Proof:

M :=

“ On input w
  1) If all symbols in w are crossed, ACCEPT
  2) Scan the tape and read first and last uncrossed symbols.
  3) If they are equal, cross them, and goto 1)
  4) If they are different, REJECT.”

- Can you decide PAL faster?

- Theorem: PAL $\notin$ TIME(ε n^2) for a constant ε

- Intuitively, the reason is information bottleneck

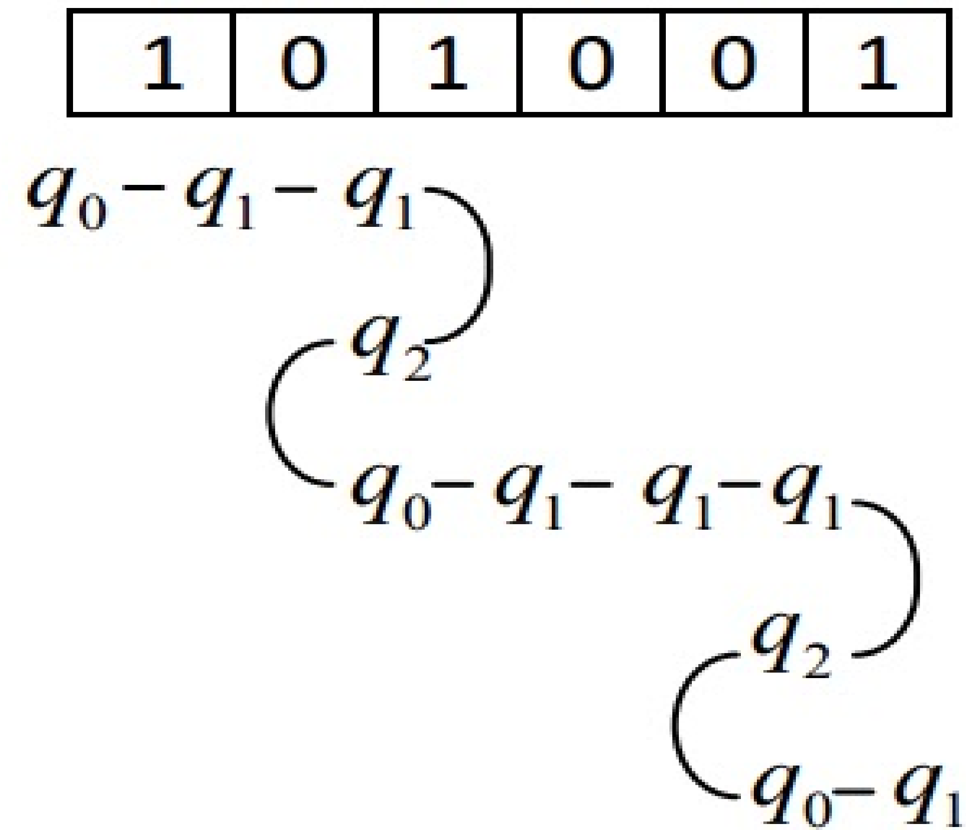
A TM can only “carry” a constant amount of information across the tape, and so needs to scan the tape n times. Each scan takes n steps, for a total of n^2 steps.

We now formalize this intuition.

● Definition: A crossing sequence of TM M on input w and boundary i, abbreviated i-CS, is the sequence of states that M is in when crossing the i-th cell boundary on input w.

● Detail: We think of one step as first change state then move

Example:



1-CS = q_1

2-CS = (q_1 , q_2 , q_0)

3-CS = q_1

4-CS = q_1

5-CS = (q_1 , q_2 , q_0)

6-CS = q_1

Img source: http://smartclassacademy.blogspot.com/2012/11/two-way-finite-automata.html

- **Definition**: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- **Theorem**: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- **Proof**:

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

If you have such v and w, how do you complete the proof?

- Definition: L := { $x\ 0^n\ x^R$: $|x| = n$}
- Theorem: L $\notin$ TIME($\varepsilon\ n^2$) for a constant ε
- Proof:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

If you have such v and w, how do you complete the proof?

Write $v = x\ 0^n\ x^R$

$w = y\ 0^n\ y^R$

Let M be a TM that decides L. M accepts v and w

M on input $x\ 0^n\ y^R$???

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

If you have such v and w, how do you complete the proof?

Write $v = x\, 0^n\, x^R$
$w = y\, 0^n\, y^R$

Let M be a TM that decides L. M accepts v and w

M on input $x\, 0^n\, y^R$ accepts but $x\, 0^n\, y^R \notin \mathrm{PAL}$ since $x \neq y^R$

M accepts x 0^n x^R	M accepts y 0^n y^R	M accepts x 0^n y^R
q_0 0 0 0 0	q_0 1 0 0 1	q_0 0 0 0 1
# q_1 0 0 0	# q_0 0 0 1	# q_1 0 0 1
# 0 q_2 0 0	# 0 q_2 0 1	# 0 q_2 0 1
# 0 x q_3 0	# 0 # q_5 1	# 0 # q_5 1
# 0 x 0 q_4	# 0 q_6 # 1	# 0 q_6 # 1
# 0 x q_4 0	# q_4 0 # 1	# q_4 0 # 1
# 0 q_4 x 0	q_4 # 0 # 1	q_4 # 0 # 1
# q_4 0 x 0	# q_4 0 # 1	# q_4 0 # 1
q_4 # 0 x 0	# 0 q_A # 1	# 0 q_A # 1
# q_4 0 x 0		
# 0 q_A x 0		

Crossing sequence at boundary 2

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

$$\boxed{\begin{array}{l}\text{Find } v \neq w,\ v \in L,\ w \in L,\ i \in \{n, n+1, \ldots, 2n-1\} \text{ such that} \\ \text{the TM on inputs } v \text{ and } w \text{ has the same } i\text{-CS.}\end{array}}$$

It remains to show that such v and w exist.

- Definition: L := { x 0^n x^R : |x| = n}
- Theorem: L $\notin$ TIME(ε n^2) for a constant ε
- Proof:

Find v ≠ w, v ∈ L, w ∈ L, i ∈ {n, n+1, …, 2n-1} such that the TM on inputs v and w has the same i-CS.

Let M be a TM that decides L in time t.

Claim: For every v ∈ L, there is i ∈ {n, n+1, …, 2n-1} such that the i-CS of M on v has length ≤ t/n.

Proof:

- Definition: L := { x 0^n x^R : |x| = n}
- Theorem: L $\notin$ TIME(ε n^2) for a constant ε
- Proof:

Find v $\neq$ w, v $\in$ L, w $\in$ L, i $\in$ {n, n+1, …, 2n-1} such that the TM on inputs v and w has the same i-CS.

Let M be a TM that decides L in time t.

Claim: For every v $\in$ L, there is i $\in$ {n, n+1, …, 2n-1} such that the i-CS of M on v has length $\leq$ t/n.

Proof:
Each state in a CS counts for a computation step.
No step is counted twice.
If for every i $\in$ {n, n+1, …, 2n-1} the i-CS has length > t/n,
?????????

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

$$\boxed{\begin{array}{l}\text{Find } v \neq w,\ v \in L,\ w \in L,\ i \in \{n, n+1, \ldots, 2n-1\} \text{ such that} \\ \text{the TM on inputs } v \text{ and } w \text{ has the same } i\text{-CS.}\end{array}}$$

Let M be a TM that decides L in time t.

Claim: For every $v \in L$, there is $i \in \{n, n+1, \ldots, 2n-1\}$ such that the i-CS of M on v has length $\leq t/n$.

Proof:
Each state in a CS counts for a computation step.
No step is counted twice.
If for every $i \in \{n, n+1, \ldots, 2n-1\}$ the i-CS has length $> t/n$,
M would take $> t$ steps. ■

- **Definition**: $L := \{ x\,0^n\,x^R : |x| = n\}$
- **Theorem**: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- **Proof**:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

The number of CS of length $\leq t/n$ is at most

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\, \varepsilon\, n^2\,)$ for a constant ε
- Proof:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

The number of CS of length $\leq t/n$ is at most

$n \cdot t/n \cdot q^{t/n}$ where q is the number of states of the TM.

n = choice of i

t/n = choice of length of CS

$q^{t/n}$ = sequence of states

The number of inputs $x\, 0^n\, x^R \in L$ with $|x| = n$ is

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

$$\boxed{\begin{array}{l}\text{Find } v \neq w,\ v \in L,\ w \in L,\ i \in \{n, n+1, \ldots, 2n-1\} \text{ such that} \\ \text{the TM on inputs } v \text{ and } w \text{ has the same } i\text{-CS.}\end{array}}$$

The number of CS of length $\leq t/n$ is at most
$n \bullet t/n \bullet q^{t/n}$ where q is the number of states of the TM.

n = choice of i
t/n = choice of length of CS
$q^{t/n}$ = sequence of states

The number of inputs $x\, 0^n\, x^R \in L$ with $|x| = n$ is 2^n
Note $n \bullet t/n \bullet q^{t/n} \leq \varepsilon\, n^2 \bullet q^{\varepsilon\, n} < 2^n$ for small enough ε.
So v and w exist by ?

- Definition: $L := \{ x\, 0^n\, x^R : |x| = n\}$
- Theorem: $L \notin \mathrm{TIME}(\varepsilon\, n^2)$ for a constant ε
- Proof:

Find $v \neq w$, $v \in L$, $w \in L$, $i \in \{n, n+1, \ldots, 2n-1\}$ such that the TM on inputs v and w has the same i-CS.

The number of CS of length $\leq t/n$ is at most
$n \cdot t/n \cdot q^{t/n}$ where q is the number of states of the TM.

n = choice of i
t/n = choice of length of CS
$q^{t/n}$ = sequence of states

The number of inputs $x\, 0^n\, x^R \in L$ with $|x| = n$ is 2^n
Note $n \cdot t/n \cdot q^{t/n} \leq \varepsilon\, n^2 \cdot q^{\varepsilon\, n} < 2^n$ for small enough ε.
So v and w exist by pigeonhole principle. ■

- Theorem: PAL $\notin$ TIME(ε n^2) for a constant ε

- We have completed the proof of this theorem

- We now define multi-tape TM,

  and show they can decide PAL much faster

- So far, 1-tape TM

- Definition: A k-tape TM is a TM with k tapes.

  Each tape has its own head moving independently

  Transition functions have the following range and domain:

  $\delta : Q \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L,R\}^k$

- Theorem: PAL $\in$ TIME(????) on 2-tape TM.

- Theorem: PAL $\in$ TIME(10 n) on 2-tape TM.

- Proof:
  M := “On input w

- Theorem: PAL $\in$ TIME(10 n) on 2-tape TM.

- Proof:
  M := "On input w

  Copy w on second tape.

  Bring head on 1st tape at the beginning.

  Bring head on 2nd tape at the end.

  Compare symbol-by-symbol,
  moving 1st head forward and 2nd backward.

  If any two symbols are different, REJECT.

  If head on 1st tape reaches the end, ACCEPT." ■

MAJOR OPEN QUESTION

SAT $\in$ TIME(10 n) on 2-tape TM ?