Tuesday, April 10, 2018 8:24 AM

Padding + Succinctness

Consequences of measuring complexity as a fcn. of input length:

- artificially expand input → running time decreases.
- shrink input → running time increases.

Padding Suppose $L \in EXP$ ($L \in TIME(2^{n^k})$ for const. k)

$$PAD_L = \{x\#^N \mid x \in L \quad N = 2^{|x|^k}\}$$

TM that decides PAD_L:

→ verify that the string of #'s has correct length
→ Run TM for L on x (ignoring #'s)

Running time is linear!

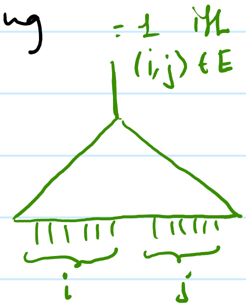
Conversely: Intuition suppose L is P-complete
$SUCCINCT_L$ encodes inputs of L exp. shorter

If hard instances of L are exp. shorter then it is a candidate to be EXP-complete.

Succinct Encodings:

- Instead of specifying a graph by enumerating edges + vertices.
- Specify n = # vertices (written in binary)
- Give a circuit:

circuit size poly in the length of the inputs $= 2\log n$



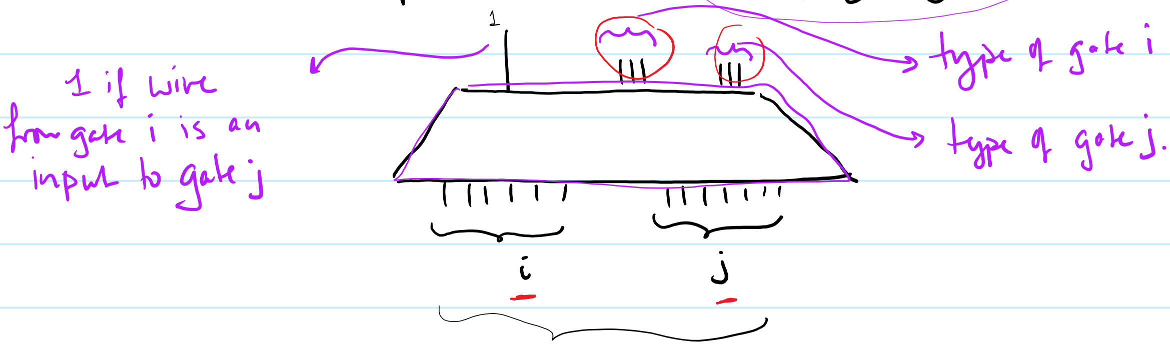
Tuesday, April 10, 2018 8:24 AM

Not all graphs can be specified succinctly but perhaps some problems are still hard even when input graphs are restricted to graphs that can be specified this way.

Succinct Encodings of Instances of CVAL (variable-free ckt).

Small circuit encodes big circuit.

(1) m = # nodes in big circuit (written in binary)
(2) Specification of circuit that takes $2 \log m$ inputs
size of circuit is $O(\text{poly}(\log m))$.



SUCCINCT-CVAL: given a succinctly encoded variable-free Boolean ckt, does it output 1?

Theorem: SUCCINT-CVAL is EXP-complete. [poly-time reduction].

if SUCCINCT-CVAL $\in$ PSPACE then EXP = PSPACE
SUCCINCT-CVAL $\notin$ P. (know P $\neq$ EXP).

~~From~~ last time: if CVAL $\in$ L.
then P = L.

Tuesday, April 10, 2018 8:24 AM

input size $n = \text{poly}(\log(m))$.

SUCCINCT-CVAL $\in$ EXP m = # nodes in big circuit

Run through all k: $1 \le k \le m$

output type of k.

Run through all (k, ℓ) $1 \le k, \ell \le m$

Output (k, ℓ) if (k, ℓ) is in the ckt.

Explicit description of the circuit has size $O(m)$ time $O(m^2)$ to produce

$n = (\log m)^k$

$k n = \log m$

$m = 2^{kn}$.

Solve CVAL in time $\text{poly}(m)$.

Input length $\ge \log m$.

$\text{poly}(m) \le m^k \le 2^{k \cdot n}$ $O(2^{n^k})$

Reduction: $\forall\ L \in \text{EXP}$ $L \propto$ SUCCINCT-CVAL.

$x \xrightarrow{\text{computable in time poly}(|x|)}$ Succinct description of C_x.

Size of C_x: $2^{|x|^k}$

Encoding of C_x $|x|^k$ bits.

$x \in L$ iff C_x evaluates to 1.

Tuesday, April 10, 2018 8:24 AM

Same tableau ckt as in proof that CVAL is P-complete.

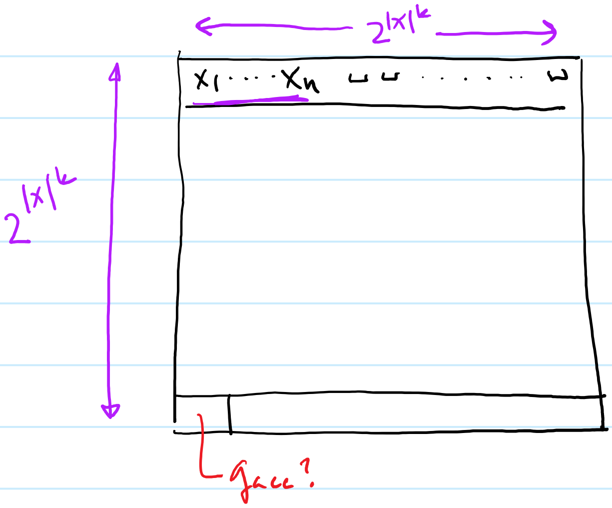
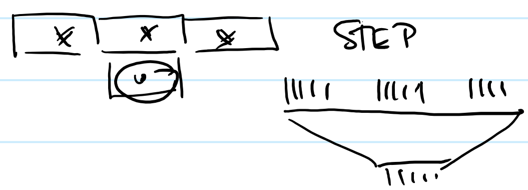


Tableau represents computation of M on input x

Can express tableau as ckt.



How to express C_x using only $O(|x|^c)$ bits?

\# gates in STEP is s

\# bits to encode a cell = r $\quad \log(|\Sigma| + |\Sigma| \cdot |Q|)$

$r \leq s$.

What the small ckt does.

Gate label (row, col, i)

Here is a decision procedure to determine type of gate

circuit.

time poly in length of (row, col, i)

$\log(|x|^k) \cdot s$

For row 0: $\quad 1 \leq i \leq r$

(0, col, i) $\quad$ if col $\leq |x|$ $\quad$ (row, col, i) is i^{th} bit of encoding of x_{col}.

hard-coded into circuit.

if col $> |x|$ $\quad$ (row, col, i) is i^{th} bit of encoding of $\sqcup$

For row > 0: gates are gates in STEP

(row, col, i) only depends on i $\Rightarrow O(s)$

Wed April 11, 2018 - page 5

Tuesday, April 10, 2018 8:24 AM

How to determine edges

$\langle row, col, i \rangle \quad \langle row', col', j \rangle$

row = row' col = col' edge is internal to STEP
O(s) decision procedure

Output is 0 unless

row = row' − 1.
col = col' − {0, 1, −1}
i is an output node
j is an input node.
i connects to j according to rules of STEP.

can determine in poly time.

Finally can hard-code outputs of

$(2^{|x|^k}, 0, -)$.

Summary: First Complexity classes:

$L \subseteq P \subseteq PSPACE \subseteq EXP$

1st Separations via diagonalization: $P \neq EXP$
$L \neq PSPACE$.

1st major open questions:

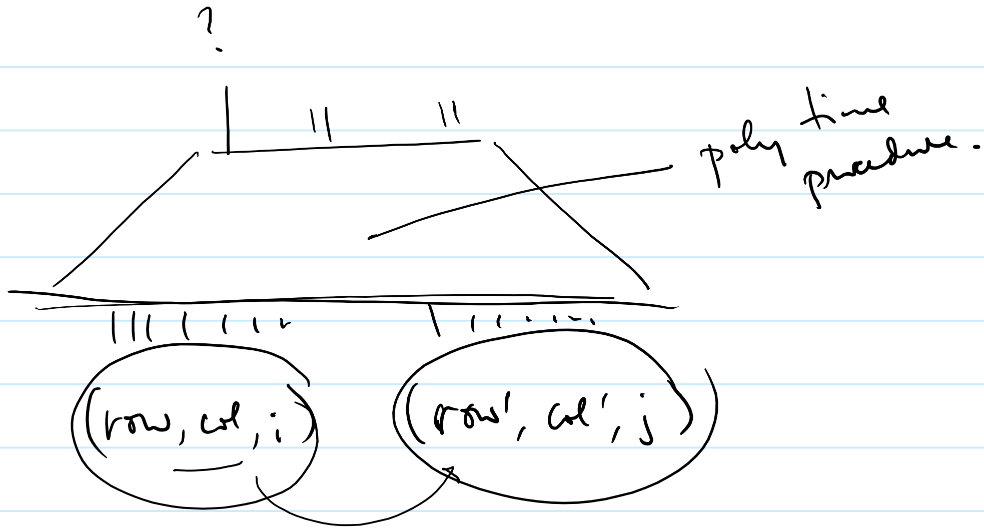
$L \stackrel{?}{=} P \qquad P \stackrel{?}{=} PSPACE$

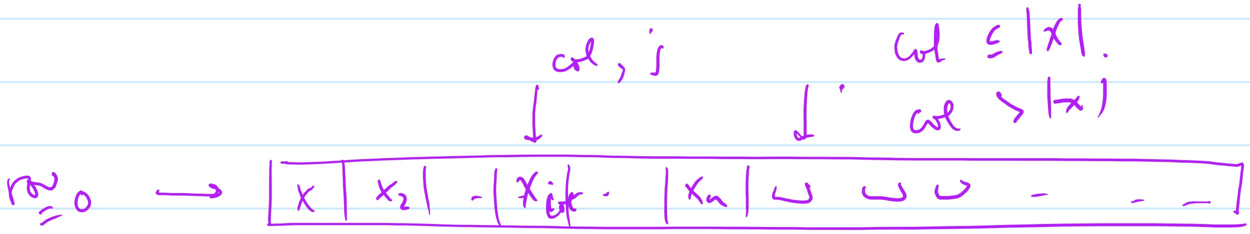
Complete Problems: CVAL is P-complete.
Succ-CVAL is EXP-complete.

Wed April 11, 2018 - page 5.5

10:25 AM

Wednesday, April 11, 2018 8:53 AM





Wed April 11, 2018 - page 6

Tuesday, April 10, 2018 8:24 AM

Can computers replace methematicians?

$$L = \{ (x, 1^k) \mid \text{Statement } x \text{ has a proof of length} \le k \}$$

A yes answer is among the many profound implications that would result if P = NP.

NP : Non-deterministic Polynomial Time

Recall the definition of a TM:

$$\delta : Q \times \Sigma \longrightarrow Q \times \Sigma \times \{R, L, -\}$$

In a non-deterministic machine we have instead:

$$\Delta : Q \times \Sigma \longrightarrow P(Q \times \Sigma \times \{R, L, -\})$$

power set: set of all subsets.

A configuration can have 0, 1, or more next configurations.

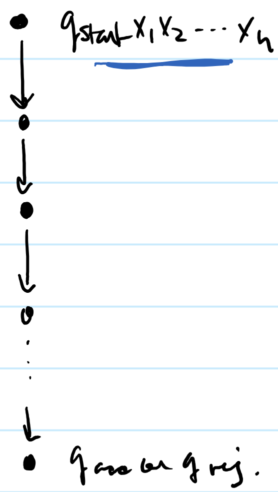
For a given TM M on input x, can build a configuration graph.

nodes $\longleftrightarrow$ configurations.

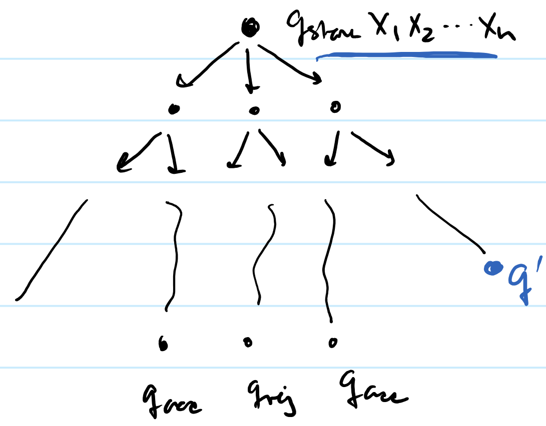
$(c_1, c_2) \longleftrightarrow$ c_2 is reachable from c_1 in one step.

Tuesday, April 10, 2018 8:24 AM

Deterministic TM



Non-deterministic TM



In order for an NTM to accept or reject x
in time t(n): space s(n)

- All computation paths must terminate.
- Length of longest root to leaf path is $\leq t(|x|)$.
- Space: max # tape cells used on any root to leaf path $\leq s(|x|)$

Note
Asymmetric definition!

- Accept if any leaf is an accept.
- Reject if all leaves are reject.

NTIME (f(n)) : languages decidable by a multi-tape NTM that runs in $\leq f(n)$ steps along any computation path where n is the length of the input.

NSPACE (f(n)) : languages decidable by a multi-tape NTM that touches $\leq f(n)$ cells of worktape along any computation path.

Wednesday, April 11, 2018 8:22 AM

Time Classes: $NP = \bigcup_{k \geq 1} NTIME(n^k)$

$NEXP = \bigcup_{k \geq 1} NTIME(2^{n^k})$

Useful alternative view of NP:

Is there a way to prove that $x \in L$ with a poly-sized proof y that can be verified by a poly-time verifier?

$L \in NP \iff \exists$ polytime verifier (TM) R and constant k such that $x \in L$ iff $\exists y$ $|y| \leq |x|^k$ and R accepts (x, y).

$L = \{x \mid \exists y \; |y| \leq |x|^k \; (x, y) \in L(R)\}$

Example: $3SAT = \{\phi \mid \phi$ is a 3-CNF formula for which $\exists$ assignment A $(\phi, A) \in L(R)\}$

$L(R) = \{(\phi, A) \mid A$ is a satisfying assignment for $\phi\}$.

A is a witness that $\phi \in 3SAT$.
R is a poly time TM.

Other examples: Independent Set, Hamiltonian Cycle, etc...