Cook's Theorem

Joel Lepak

Youngstown State University

q_i	s_i	q_f	s_f	$direction$
$q0$	B	$q1$	B	R
$q1$	1	$q1$	1	R
$q1$	B	$q2$	1	R

$$f(x) = x + 1$$

q_i	s_i	q_f	s_f	$direction$
$q0$	B	$q1$	B	R
$q1$	1	$qODD$	B	R
$q1$	B	$q2$	B	R
$qODD$	B	$q2$	1	R
$qODD$	1	$qEVEN$	B	R
$qEVEN$	B	$q2$	B	R
$qEVEN$	1	$qODD$	B	R

Parity Check—returns 0 if even, 1 if odd

P $\rightarrow$ polynomial time. "Easy."

Input of length N computed in $p(N)$ time.

- ◇ Computing $x + y$.
- ◇ Alphabetic sorting

NP $\rightarrow$ nondeterministic polynomial time.

Input of length N computed in $p(N)$ time by non-deterministic algorithm/TM

- ◇ Determining if a set of items with given sizes can fit in a given number of bins
- ◇ Satisfiability: Given a list of boolean clauses (e.g. $(x_1 + x_2)(x_3 + \bar{x}_2)$), does there exist a combination of truth values for which all clauses can be satisfied simultaneously?

$$P \subseteq NP$$

Nondeterminism

- multiple paths, or exponentially parallel computing
- **Nondeterministic Turing Machine** - not restricted to only one possible final state for a given initial state, e.g.

q_i	s_i	q_f	s_f	*direction*
q_1	A	q_1	B	L
q_1	A	q_2	C	R
q_1	A	q_1	B	R
$\vdots$				

- **Nondeterministic Algorithm** - using a **"goto both"** instruction.

for $i = 1$ to N

goto both $label_1, label_2$

$label_1$: $x_i = T$; continue

$label_2$: $x_i = F$; continue

end

if $F(x_1, \ldots, x_n) = T$ then return yes

else return no

Satisfiablility (SAT)

$\rightarrow$ Determining if a set of clauses can be simultaneously satisfied.

$$(x_1 + x_2)(\bar{x}_1 + x_3)(\bar{x}_1 + \bar{x}_2)$$

Satisfiable - (multiple solutions).

$$(x_1 + x_2)(\bar{x}_1 + x_3)(x_2 + \bar{x}_3)(\bar{x}_1 + \bar{x}_2)(x_3)$$

Satisfiable - $x_1 = F, x_2 = T, x_3 = T$.

$$(x_1 + \bar{x}_2)(\bar{x}_1 + \bar{x}_2)(\bar{x}_1 + x_2)(x_1 + x_2)$$

Not satisfiable.

Polynomial Reducibility

$A \leq_P B \iff$ every instance of A can be translated to an instance of B in polynomial time.

NP-Completeness

A is NP-Complete ("Hard") if

$$A \in NP \quad \text{and} \quad \forall B \in NP, B \leq_P A.$$

SAT is NP-Complete

- ◇ find a way to translate any problem to an instance of SAT

Properties of a general problem $A \in \mathcal{NP}$:

- ◇ can be solved by a nondeterministic TM in time $t \leq p(N)$
- ◇ therefore only $2p(N)+1$ squares can possibly be visited by the TM head
- ◇ TM is given an input I of length N
- ◇ TM has a number M different states
- ◇ TM has an alphabet of A symbols
- ◇ M and A do not depend on the input

Boolean variables:

- ◇ Q_{tm} = (after step t the TM is in state q_m).
- ◇ S_{tlx} = (after step t symbol x is in square l).
- ◇ H_{tl} = (after step t the TM head is at square l).

General Conditions for any TM

◇ TM is always in exactly 1 state:

$$(Q_{t0} + \ldots + Q_{tM}) \quad \text{(at least one state)}$$

$t = 0 \ldots p(N) \rightarrow O(p(N))$ clauses

$$(\bar{Q}_{tm} + \bar{Q}_{tm'}) \quad \text{(no more than one state)}$$

$t = 0 \ldots p(N)$, $m, m' = 0 \ldots M \rightarrow O(p(N))$ clauses

◇ Each TM square always contains exactly 1 symbol:

$$(S_{tl0} + \ldots + S_{tlA}) \quad \text{(at least one symbol)}$$

$t = 0 \ldots p(N), l = 0..2p(N) \rightarrow O(p^2(N))$ clauses

$$(\bar{S}_{tlx} + \bar{S}_{tlx'}) \quad \text{(no more than one symbol)}$$

$t = 0 \ldots p(N)$, $l = 0 \ldots 2p(N)$, $x, x' = 0 \ldots A \rightarrow O(p^2(N))$ clauses

- ◇ The TM head is always over exactly 1 square:

$$(H_{t0} + \ldots + H_{t(2p(N))})$$

$$(\bar{H}_{tl} + \bar{H}_{tl'})$$

- ◇ TM is in correct initial state.

$$(Q_{0(init)})(H_{0(init)})$$

- ◇ A symbol cannot change unless the TM head is over its square.

$$(H_{tl} + \bar{S}_{tlx} + S_{(t+1)lx})$$

t, l, x range over all their values $\rightarrow O(p^2(N))$ clauses

The TM behaves according to the algorithm it is running

- $\diamond$ TM evaluates function of input as true

$$(Q_{p(N)(true)})$$

- $\diamond$ Input is in initial position

$$(S_{0(init)I_1})(S_{0(init+1)I_2})\ldots+(S_{0(init+N-1)I_N})$$

- $\diamond$ TM changes state according to it instructions

$$(\bar{H}_{tl}+\bar{Q}_{tm}+\bar{S}_{tlx}+H_{(t+1)l'})$$

$$(\bar{H}_{tl}+\bar{Q}_{tm}+\bar{S}_{tlx}+Q_{(t+1)m'})$$

$$(\bar{H}_{tl}+\bar{Q}_{tm}+\bar{S}_{tlx}+S_{(t+1)lx'})$$

(If all conditions are met for a given TM state at time t, the TM must be in the given next state at time $t+1$)

$t=0\ldots p(N)$, $l=0\ldots 2p(N)$, $m=0\ldots M$, $x=0\ldots A \rightarrow O(p^2(N))$ clauses

All clauses can be satisfied.

$$\Longleftrightarrow$$

A TM exists which accepts input as true.

Satisfiability can be solved "quickly"

$$\Longleftrightarrow$$

All problems in NP can be solved "quickly"