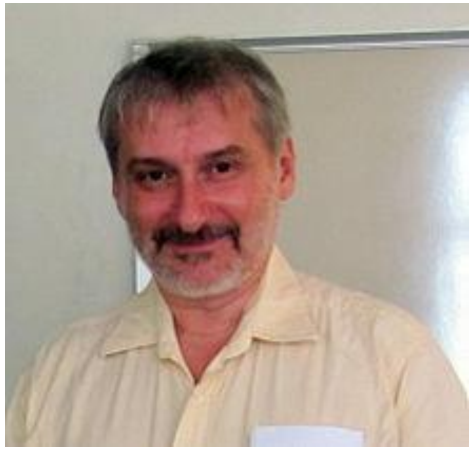
The Cook Theorem

The SAT problem

- The satisfiability problem for propositional logic
  - historically *first* problem known to be NP-complete!

- **Cook-Levin Theorem (1971):** The SAT problem is NP-complete.
- **Proof:**
  - **Membership in NP:** Easy
  - **NP-hardness:** Much harder!



SAT is NP

- Input: a propositional logic formula of size n (with propositions P, $|P| < n$)
- Certificate: a valuation $v: P \to \{T, F\}$
- Verification: in $\Theta(n)$ time, evaluate the formula with truth assignments v

SAT is NP-hard

- Let L be any language in $\mathbf{NP}$. There must exist an NDTM M that recognizes L in time $c \cdot |x|^l$. For an input x, we'll construct (in polynomial time) a formula $\varphi_M(x)$ such that

$$x \in L \text{ iff. } \varphi_M(x) \text{ is satisfiable}$$

The Reduction

- **Idea:**
  - $\varphi_M(x)$ should describe "how M accepts x"
  - Assume $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$
  - Encoding attributed to Madhusudan and Viswanathan

The Reduction

- **Idea:**
  - $\varphi_M(x)$ should describe "how M accepts x"
  - Assume $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$
  - Encoding adapted from Madhusudan and Viswanathan

Proposition Name	Meaning if set to T	Total Number
Symb(b, p, i)	Tape stores b in cell p at time i	$O\left(\lvert x\rvert^{2l}\right)$
Hd(h, i)	Tape head in cell h at time i	$O\left(\lvert x\rvert^{2l}\right)$
State(q, i)	State is q at time i	$O\left(\lvert x\rvert^{l}\right)$

Overall Reduction

$$\varphi_M(x) \equiv \varphi_{initial} \wedge \varphi_{consistent} \wedge \varphi_{transition} \wedge \varphi_{accept}$$

where

- $\varphi_{initial}$ says that "configuration at time 0 is the initial configuration with input x"
- $\varphi_{consistent}$ says that "at each time, truth values to propositions encode a valid configuration"
- $\varphi_{transition}$ says that "configuration at each time follows from the previous one by taking a transition"
- φ_{accept} says that "the last configuration is an accepting configuration"

Initial Condition

$\varphi_{initial} \equiv$

$\text{State}(q_0, 0)$	"At time 0, state is q_0"
$\wedge_{p=1}^{n} \text{Symb}\left(x_p, p, 0\right)$	"At time 0, cells 1 through n hold x"
$\wedge_{p=n+1}^{c \cdot n^l} \text{Symb}(\text{" "},\ p,\ 0)$	"At time 0, all other cells are blank"
$\wedge\ \text{Hd}(1, 0)$	"At time 0, head at the leftmost position"

Consistency

$\varphi_{consistent} \equiv$

$\wedge_{i=0}^{c \cdot n^l} \nabla\big(\mathrm{State}(q_0, i), \dots, \mathrm{State}(q_m, i)\big)$ "At time i, state is unique"

$\wedge_{i=0}^{c \cdot n^l} \wedge_{p=1}^{c \cdot n^l} \nabla\big(\mathrm{Symb}(b_1, p, i), \dots, \mathrm{Symb}(b_t, p, i)\big)$ "Tape cells contain unique symbols"

$\wedge_{i=0}^{c \cdot n^l} \nabla\big(\mathrm{Hd}(1, i), \dots, \mathrm{Hd}(c \cdot n^l, i)\big)$ "At any time, tape head is in one cell"

Transition Consistency

"If head is not in position p, then symbol does not change"

$$\varphi_{transition} \equiv \bigwedge_{i=0}^{c\cdot n^l} \bigwedge_{p=1}^{c\cdot n^l} \begin{pmatrix} \neg \mathrm{Hd}(p,i) \rightarrow \bigwedge_b \big(\mathrm{Symb}(b,p,i) \wedge \mathrm{Symb}(b,p,i{+}1)\big) \\ \wedge \quad \big(\mathrm{Hd}(p,i) \rightarrow \bigwedge_q \bigwedge_b \Delta_{q,b}^{i,p}\big) \end{pmatrix}$$

"If head is in position p, then a transition is taken"

Acceptance

$$\varphi_{accept} \equiv \bigvee_{\substack{q_{acc} \in F \\ 0 \leq i \leq c \cdot n^{l}}} \mathrm{State}(q_{acc}, i)$$