Cook-Levin theorem: Proof from Sipser Text

- Let $N = (Q, \Sigma, \Gamma, \delta_M, q_s, q_a, q_r)$ be a *fixed* 1-tape non-deterministic Turing machine.
- Runs in time $p(n)$, a polynomial.
- Let w be an input to N.
- All computation paths of N on w have length $t = p(|w|)$.
- Let $\Delta = Q \cup \Gamma \cup \{\#\}$.
- Each configuration of N on w is a length $t + 3$ string with $\#$ at the start and at the end.
- Define a table T with $(t + 3)$ columns and $(t + 1)$ rows where each entry of T contains a symbol from Δ.
- A table that satisfies the following three conditions is defined to be an *accepting* table.
  - The first row is the initial configuration: $C_0 = \# q_s w_1 w_2 \ldots w_n \sqcup^{t-n} \#$.
  - The last row is an accepting configuration.
  - For $0 \leq i \leq t$, the i-th row is a configuration C_i such that for all $0 \leq i \leq t - 1$, $C_i \vdash C_{i+1}$.
- Then, N accepts w if and only if there is an accepting table.
- One accepting table for each accepting computation path of N on w.
- In fact, one table associated with each computation path of N on w.

Cook-Levin theorem: legal windows

Let T be a table. Define 2×3 windows in T as follows. For $0 \leq i \leq t-1$ and $0 \leq j \leq t$, the (i,j)-th window consists of the six entries in $T(i,j)$, $T(i,j+1)$, $T(i,j+2)$, $T(i+1,j)$, $T(i+1,j+1)$, and $T(i+1,j+2)$. Such a window is a *legal window* if it is one of the following:

- State as the center symbol of the top row (a *critical* window):
  - For all transitions $\delta(p,a)$ that includes (q,d,R) the following are legal windows: For all $b \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} b & p & a \\ \hline b & d & q \end{array}\right]$.
  - For all transitions $\delta(p,a)$ that includes (q,d,L) the following are legal windows:
    - For all $b \in \Gamma$, $\left[\begin{array}{c|c|c} b & p & a \\ \hline q & b & d \end{array}\right]$.
    - $\left[\begin{array}{c|c|c} \# & p & a \\ \hline \# & q & d \end{array}\right]$.
- State as the right-most symbol of the top row:
  - For all transitions from state p that includes (q,d,R) (for whatever symbol read) the following are legal windows: For all $b \in \Gamma$, $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} c & b & p \\ \hline c & b & d \end{array}\right]$.
  - For all transitions from state p that includes $(q,-,L)$ (for whatever symbol read and whatever symbol written) the following are legal windows: For all $b \in \Gamma$, $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} c & b & p \\ \hline c & q & b \end{array}\right]$.
- State as the left-most symbol of the top row:
  - For all transitions $\delta(p,a)$ that includes (q,d,R) the following are legal windows: For all $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} p & a & c \\ \hline d & q & c \end{array}\right]$.
  - For all transitions $\delta(p,a)$ that includes $(-,d,L)$ (for whatever state it moves to) the following are legal windows: For all $b \in \Gamma$, $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} p & a & c \\ \hline b & d & c \end{array}\right]$.
  - For all transitions $\delta(p,a)$ that includes (q,d,L) the following are legal windows (moving left from the left-most end of the tape): For all $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} p & a & c \\ \hline q & d & c \end{array}\right]$.

Cook-Levin theorem: legal windows

- No state in the top row:
  - For all $a \in \Gamma \cup \{\#\}$, $b, c \in \Gamma$, $\left[\begin{array}{c|c|c} a & b & c \\ \hline a & b & c \end{array}\right]$.
  - For all $a, b \in \Gamma$, $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} a & b & c \\ \hline a & b & c \end{array}\right]$.
  - For all transitions to $(q, -, L)$ (from whatever state, on whatever symbol read, and whatever symbol written)

    For all $a \in \Gamma \cup \{\#\}$, $b, c \in \Gamma$, $\left[\begin{array}{c|c|c} a & b & c \\ \hline a & b & q \end{array}\right]$.
  - For all transitions from $\delta(-, a)$ to $(-, d, L)$ (from whatever state to whatever state)

    For all $b, c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} a & b & c \\ \hline d & b & c \end{array}\right]$.
  - For all transitions from $\delta(-, a)$ to $(q, -, R)$ (from whatever state and on whatever symbol written)

    For all $b \in \Gamma$, $c \in \Gamma \cup \{\#\}$, $\left[\begin{array}{c|c|c} a & b & c \\ \hline q & b & c \end{array}\right]$.

Note that the number of legal windows is finite.

Cook-Levin theorem: Correctness

Claim: Let T be a computation table whose first row is the start configuration and the last row is an accepting configuration. Then, T is an accepting table if and only if, for all $0 \leq i \leq t - 1$, $0 \leq j \leq t$, the (i, j)-th window in T is legal.

Proof of Claim: The claim follows from the Lemma below by induction.

Lemma: Let the i-th row of T, for some $0 \leq i \leq t-1$, be a valid configuration C_i. Then, the $i+1$-th row of T is a valid configuration C_{i+1} such that $C_i \vdash C_{i+1}$ if and only if, for all $0 \leq j \leq t$, the (i, j)-th window is legal.

One direction of the lemma follows by considering legal windows as dictated by the two consecutive configurations C_i and C_{i+1}.

In the other direction, suppose the i-th row of T is a valid configuration C_i and, for all $0 \leq j \leq t$, the (i, j)-th window is legal. First, note that there is exactly one symbol in each cell so that overlapping symbols in adjacent (left-to-right) cells are same. The lemma follows from the following four observations:

1. The symbol that is *not* adjacent to a state symbol in the upper configuration appears unchanged in the bottom configuration.

2. A symbol (other than the boundary symbol #) that is not adjacent to a state symbol in the upper configuration appears as the middle symbol in the top row of a legal window whose top row does not have a state symbol.

3. In a legal window whose top row does not contain a state symbol, the middle symbol in the top row and the bottom row are the same.

4. For all legal windows with the state symbol as the middle symbol, the corresponding transition of N fixes all the three symbols in the bottom row of the window. This also ensures that the adjacent windows are consistent.

Cook-Levin theorem: reduction from an $\mathcal{NP}$ machine

A reduction machine takes as input a string w (that is an input to N) and produces a formula F such that F is satisfiable if and only if there is an accepting table.

- In fact, each satisfying assignment to the variables of F will correspond to one accepting table.
- For $0 \leq i \leq t$, $0 \leq j \leq t+2$, the (i,j)-th entry of every table is associated with Boolean variables $X_{i,j,s}$ for all $s \in \Delta$.
  - The variable $X_{i,j,s}$ is TRUE iff the the (i,j)-th entry of the table has the symbol s in it.
- The formula F is the conjunction of four sub-formulas:
  - A subformula F_{cell} that is satisfiable iff each entry in the table has exactly one symbol from Δ in it. Formula F_{cell} ensures that there is exactly one symbol in each cell so that overlapping symbols in adjacent (left-to-right or top-to-bottom) windows are same.
  - A subformula F_{start} that is satisfiable iff the first row of the table is the initial configuration of N on w.
  - A subformula F_{accept} that is satisfiable iff the last row of the table is an accepting configuration of N on w.
  - A subformula F_{move} that is satisfiable iff the each row of the table is a configuration that follows legally from the configuration in the previous row of the table.

Cook-Levin theorem: polynomial time reduction

- Construction of the legal windows: polynomial time.
- Number of variables: $(t+1) \times (t+3) \times |\Delta|$: a polynomial.
- Size of the formulas F_{start} and F_{accept} is $O(t)$ fragments with each fragment of size $O(\log n)$: a polynomial.
- Size of the formulas F_{cell} and F_{move} is $O(t^2)$ fragments with each fragment of size $O(\log n)$: a polynomial.
- Generating each subformula is polynomial time and hence generating the complete formula is polynomial time.