A Field Guide to the proof of the Cook-Levin Theorem

We start with a (possibly non-deterministic) Turing Machine \( M \) and input string \( w \). We want to construct a Boolean expression \( B \) that is satisfiable if and only if \( M \) accepts \( w \). We are guaranteed that \( M \) halts after \( p(n) \) steps, where \( n = |w| \).

As \( M \) processes \( w \) it goes through a sequence of configurations \( \alpha_0, \alpha_1, \ldots, \alpha_{p(n)} \).

We use \( X_{ij} \) to represent the \( j^{th} \) symbol of the \( i^{th} \) configuration. So if \( \alpha_4 \) is \( 11q_200 \) then \( X_{40} = 1 \), \( X_{41} = 1 \), \( X_{42} = q_2 \), etc. This is just notation; the \( X_{ij} \)s do not appear in \( B \). By padding the right end of the configuration with blanks we have such an \( X_{ij} \) for \( 0 \leq i \leq p(n) \) and \( 0 \leq j \leq p(n) \).

For every \( i \) and \( j \) and every state and tape symbol \( A \) we have a Boolean variable \( Y_{ijA} \). These are used in the expression \( B \). We will use these in such a way that if \( Y_{ijA} \) is True then \( X_{ij} \) is \( A \).

\( F_j \) is a Boolean expression made out of the \( Y_{ijA} \)s that says the \( j^{th} \) symbol of the last configuration \( \alpha_{p(n)} \) is a final state.

\( N_i \) is a Boolean expression made out of the \( A_{ij} \)s and \( B_{ij} \)s defined below that says that each configuration \( \alpha_{i+1} \) is correctly derived from the previous configuration \( \alpha_i \) according to the transitions of our Turing Machine \( M \).

\( A_{ij} \) is a Boolean expression made out of the \( Y_{ijA} \)s that says the state symbol of the \( i^{th} \) configuration is at position \( j \) and that the \( j-1^{st} \), \( j^{th} \), and \( j+1^{st} \) symbols of the \( i+1^{st} \) configuration are correct for the corresponding transition of \( M \).

\( B_{ij} \) is a Boolean expression made out of the \( Y_{ijA} \)s that says that either the state symbol of configuration \( \alpha_i \) is a position \( j-1 \) or position \( j+1 \) (and so symbol \( j \) is covered by \( A_{ij} \)) or else position \( j \) of configuration \( \alpha_i \) has a tape symbol that is copied correctly to configuration \( \alpha_{i+1} \).