

In this experiment, a rolling hash has been used. It is basically like a sliding window of size of pattern to look. If the output of hash function and that of window and pattern is same, then there might be a hit. We must then manually check all characters to verify. It achieves  $O(n+m)$  time complexity in best (average) function if the hash function is good, but  $O(nm)$  if hash function is too simple. In rolling hash, we remove contribution of outgoing char and add that of incoming character.

This is much better than precomputing the entire hash and storing in array.

To implement this, we must first convert our pattern and first  $m$  characters of text into numeric hash value using base  $d$  ( $ASCII \leq 256$ ) and a large number  $q$ . Each character gives it's positional weight to hash.

The rolling hash step is,

$$\text{txt\_val} = (d \times (\text{txt\_val} - \text{text}[i] \times \text{hash}) + \text{text}[i+m]) \% q$$

if  $\text{txt\_val} = \text{pat\_val} \rightarrow$  do brute force checking

The graph of the Time Execution shows a few large spikes in the data. This may be due to the expected string being in the end of string or may spurious matches to check. Overall as size of pattern to check increases, the time required increases.