Karp–Rabin

The Karp–Rabin hash function (Definition 1.39) was originally developed for solving the exact string matching problem. The idea is to compute the hash values or fingerprints $H(P)$ and $H(T[j..j+m))$ for all $j \in [0..n-m]$.

- If $H(P) \neq H(T[j..j+m))$, then we must have $P \neq T[j..j+m)$.
- If $H(P) = H(T[j..j+m)$, the algorithm compares P and $T[j..j+m)$ in brute force manner. If $P \neq T[j..j+m)$, this is a false positive.

The text factor fingerprints are computed in a sliding window fashion. The fingerprint for $T[j+1..j+1+m) = \alpha T[j+m]$ is computed from the fingerprint for $T[j..j+m) = T[j]\alpha$ in constant time using Lemma 1.40:

$$\begin{aligned} H(T[j+1..j+1+m)) &= (H(T[j]\alpha) - H(T[j]) \cdot r^{m-1}) \cdot r + H(T[j+m])) \bmod q \\ &= (H(T[j..j+m)) - T[j] \cdot r^{m-1}) \cdot r + T[j+m]) \bmod q \ . \end{aligned}$$

A hash function that supports this kind of sliding window computation is known as a rolling hash function.

Algorithm 2.17: Karp-Rabin

Input: text $T = T[0 \ldots n)$, pattern $P = P[0 \ldots m)$
Output: position of the first occurrence of P in T

Choose q and r; $s \leftarrow r^{m-1} \bmod q$
$hp \leftarrow 0; ht \leftarrow 0$
for $i \leftarrow 0$ **to** $m-1$ **do** $hp \leftarrow (hp \cdot r + P[i]) \bmod q$ // $hp = H(P)$
for $j \leftarrow 0$ **to** $m-1$ **do** $ht \leftarrow (ht \cdot r + T[j]) \bmod q$
for $j \leftarrow 0$ to $n-m-1$ **do**
    if $hp = ht$ **then if** $P = T[j \ldots j+m)$ **then** return j
    $ht \leftarrow ((ht - T[j] \cdot s) \cdot r + T[j+m]) \bmod q$
if $hp = ht$ **then if** $P = T[j \ldots j+m)$ **then** return j
return n

On an integer alphabet:

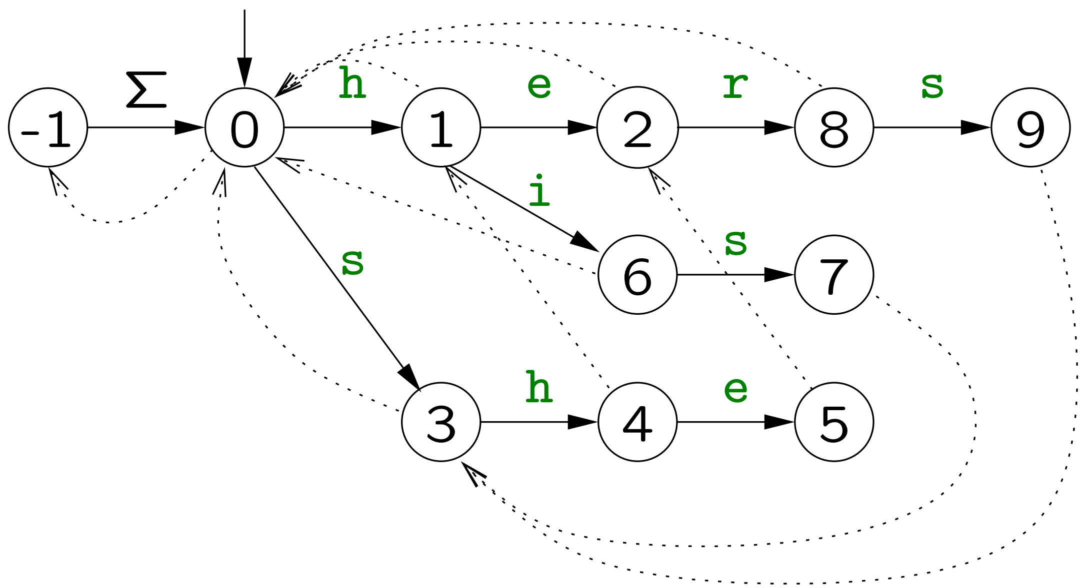
- The worst case time complexity is $\mathcal{O}(mn)$.
- The average case time complexity is $\mathcal{O}(m+n)$.

Aho–Corasick Algorithm

Given a text T and a set $\mathcal{P} = \{P_1.P_2, \ldots, P_k\}$ of patterns, the multiple exact string matching problem asks for the occurrences of all the patterns in the text. The Aho–Corasick algorithm is an extension of the Morris–Pratt algorithm for multiple exact string matching.

Aho–Corasick uses the trie $\mathit{trie}(\mathcal{P})$ as an automaton and augments it with a failure function similar to the Morris-Pratt failure function.

Example 2.18: Aho–Corasick automaton for $\mathcal{P} = \{\texttt{he}, \texttt{she}, \texttt{his}, \texttt{hers}\}$.



Algorithm 2.19: Aho–Corasick
Input: text T, pattern set $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$.
Output: all pairs (i, j) such that P_i occurs in T ending at j.

(1) Construct AC automaton
(2) $v \leftarrow root$
(3) **for** $j \leftarrow 0$ **to** $n - 1$ **do**
(4)   **while** *child*$(v, T[j]) = \bot$ **do** $v \leftarrow$ *fail*(v)
(5) $v \leftarrow$ *child*$(v, T[j])$
(6)   **for** $i \in$ *patterns*(v) **do** output (i, j)

Let S_v denote the string that node v represents.

- $root$ is the root and *child*() the child function of the trie.
- *fail*$(v) = u$ such that S_u is the longest proper suffix of S_v represented by any trie node u.
- *patterns*(v) is the set of pattern indices i such that P_i is a suffix of S_v.

At each stage, the algorithm computes the node v such that S_v is the longest suffix of $T[0..j]$ represented by any node.

Algorithm 2.20: Aho–Corasick trie construction
Input: pattern set $\mathcal{P} = \{P_1, P_2, \ldots, P_k\}$.
Output: AC trie: $root$, *child*() and *patterns*().

Create new node $root$
for $i \leftarrow 1$ **to** k **do**
  $v \leftarrow root$; $j \leftarrow 0$
  while *child*$(v, P_i[j]) \neq \bot$ **do**
    $v \leftarrow$ *child*$(v, P_i[j])$; $j \leftarrow j + 1$
  while $j < |P_i|$ **do**
    Create new node u
    child$(v, P_i[j]) \leftarrow u$
    $v \leftarrow u$; $j \leftarrow j + 1$
  patterns$(v) \leftarrow \{i\}$

This is the standard trie insertion (Algorithm 1.3) except for the computation of *patterns*():

- The creation of a new node v initializes *patterns*(v) to $\emptyset$.
- At the end, $i \in$ *patterns*(v) iff v represents P_i.

Algorithm 2.21: Aho–Corasick automaton construction
Input: AC trie: $root$, *child*() and *patterns*()
Output: AC automaton: *fail*() and updated AC trie

```
Create new node fallback
for c ∈ Σ do child(fallback, c) ← root
fail(root) ← fallback
queue ← {root}
while queue ≠ ∅ do
    u ← popfront(queue)
    for c ∈ Σ such that child(u, c) ≠ ⊥ do
        v ← child(u, c)
        w ← fail(u)
        while child(w, c) = ⊥ do w ← fail(w)
        fail(v) ← child(w, c)
        patterns(v) ← patterns(v) ∪ patterns(fail(v))
        pushback(queue, v)
```

The algorithm does a breath first traversal of the trie. This ensures that correct values of *fail*() and *patterns*() are already computed when needed.

fail(v) is correctly computed on lines (8)–(11):

- The nodes that represent suffixes of S_v that are exactly *fail*$^*(v) = \{v, \mathit{fail}(v), \mathit{fail}(\mathit{fail}(v)), \ldots, root\}$.
- Let $u = \mathit{parent}(v)$ and $\mathit{child}(u, c) = v$. Then $S_v = S_u c$ and a string S is a suffix of S_u iff Sc is suffix of S_v. Thus for any node w
  - If $w \in \mathit{fail}^*(v)$, then $\mathit{parent}(\mathit{fail}(v)) \in \mathit{fail}^*(u)$.
  - If $w \in \mathit{fail}^*(u)$ and $\mathit{child}(w, c) \neq \bot$, then $\mathit{child}(w, c) \in \mathit{fail}^*(v)$.
- Therefore, $\mathit{fail}(v) = \mathit{child}(w, c)$, where w is the first node in $\mathit{fail}^*(u)$ other than u such that $\mathit{child}(w, c) \neq \bot$.

patterns(v) is correctly computed on line (12):

$$\begin{aligned} \mathit{patterns}(v) &= \{i \mid P_i \text{ is a suffix of } S_v\} \\ &= \{i \mid P_i = S_w \text{ and } w \in \mathit{fail}^*(v)\} \\ &= \{i \mid P_i = S_v\} \cup \mathit{patterns}(\mathit{fail}(v)) \end{aligned}$$

Assuming σ is constant:

- The search time is $\mathcal{O}(n)$.
- The space complexity is $\mathcal{O}(m)$, where $m = ||\mathcal{P}||$.
  - Implementation of *patterns*() requires care (exercise).
- The preprocessing time is $\mathcal{O}(m)$, where $m = ||\mathcal{P}||$.
  - The only non-trivial issue is the while-loop on line (10).
  - Let $root, v_1, v_2, \ldots, v_\ell$ be the nodes on the path from root to a node representing a pattern P_i. Let $w_j =$ *fail*(v_j) for all j. Let *depth*(v) be the depth of a node v (*depth*$(root) = 0$).
  - When processing v_j and computing $w_j =$ *fail*(v_j), we have *depth*$(w_j) =$ *depth*$(w_{j-1}) + 1$ before line (10) and *depth*$(w_j) \leq$ *depth*$(w_{j-1}) + 1 - t_j$ after line (10), where t_j is the number of rounds in the while-loop.
  - Thus, the total number of rounds in the while-loop when processing the nodes $v_1, v_2, \ldots, v_\ell$ is at most $\ell = |P_i|$, and thus over the whole algorithm at most $||\mathcal{P}||$.

The analysis when σ is not constant is left as an exercise.