Motivation Background

String Matching

Strings provide the primary means of interfacing to machines. Consequently, string matching is central to numerous, widely-used systems and tools:

- Compilers and interpreters, command processors (e.g., bash), text-processing tools (sed, awk, ...)
- Document searching and processing, e.g., grep, Google, NLP tools, ...
- Editors and word-processors
- File versioning and compression, e.g., rcs, svn, rsync, ...
- Network and system management, e.g., intrusion detection, performance monitoring, ...
- Computational biology, e.g., DNA alignment, mutations, evolutionary trees, ...

Topics

1. Intro
   - Motivation
   - Background
2. RE
   - Regular expressions
3. FSA
   - DFA and NFA
4. To DFA
   - RE Derivatives
   - McNaughton-Yamada
5. Trie
   - Tries
6. grep
   - Using Derivatives
   - KMP
   - Aho-Corasick
   - Shift-And
7. agrep
   - Levenshtein Automaton
8. Fing.print
   - Rabin-Karp
   - Rolling Hashes
   - Common Substring and rsync
9. Suffix trees
   - Overview
   - Applications
   - Suffix Arrays

Terminology

String: List $S[1..i]$ of characters over an alphabet $\Sigma$.

Substring: A string $P[1..j]$ such that for $P[1..j] = S[l+1..l+j]$ for some $l$.

Prefix: A substring $P$ of $S$ occurring at its beginning

Suffix: A substring $P$ of $S$ occurring at its end

Subsequence: Similar to substring, but the the elements of $P$ need not occur contiguously in $S$.

For instance, $bcd$ is a substring of $abcde$, while $de$ is a suffix, $abcd$ is a prefix, and $acd$ is a subsequence. A substring (or prefix/suffix/subsequence) $T$ of $S$ is said to be proper if $T \neq S$. 

CSE 548: (Design and) Analysis of Algorithms

String Algorithms

R. Sekar
String Matching Problems

Given a "pattern" string \( p \) and another string \( s \):

**Exact match:** Is \( p \) a substring of \( s \)?

**Match with wildcards:** In this case, the pattern can contain wildcard characters that can match any character in \( s \)

**Regular expression match:** In this case, \( p \) is regular expression

**Substring/prefix/suffix:** Does a (sufficiently long) substring/prefix/suffix of \( p \) occur in \( s \)?

**Approximate match:** Is there a substring of \( s \) that is within a certain edit distance from \( p \)?

**Multi-match:** Instead of a single pattern, you are given a set \( p_1, \ldots, p_n \) of patterns. Applies to all above problems.

Language of Regular Expressions

Notation to represent (potentially) infinite sets of strings over alphabet \( \Sigma \).

Let \( R \) be the set of all regular expressions over \( \Sigma \). Then,

- **Empty String**: \( \epsilon \in R \)
- **Unit Strings**: \( \alpha \in \Sigma \Rightarrow \alpha \in R \)
- **Concatenation**: \( n_1, r_2 \in R \Rightarrow n_1 r_2 \in R \)
- **Alternative**: \( n_1, r_2 \in R \Rightarrow (n_1 \mid r_2) \in R \)
- **Kleene Closure**: \( r \in R \Rightarrow r^* \in R \)

Regular Expression

- \( a \): stands for the set of strings \( \{a\} \)
- \( a \mid b \): stands for the set \( \{a, b\} \)
  - *Union* of sets corresponding to REs \( a \) and \( b \)
- \( ab \): stands for the set \( \{ab\} \)
  - Analogous to set *product* on REs for \( a \) and \( b \)
    - \((a|b)(a|b)\): stands for the set \( \{aa, ab, ba, bb\} \).
- \( a^* \): stands for the set \( \{\epsilon, a, aa, aaa, \ldots\} \) that contains all strings of zero or more \( a \)'s.
  - Analogous to *closure* of the product operation.
Regular Expression Examples

(a|b)*: Set of strings with zero or more a's and zero or more b's:
{ε, a, b, aa, ab, ba, bb, aaa, aab, ...}

(a*b)*: Set of strings with zero or more a's and zero or more b's such that all a's occur before any b:
{ε, a, b, aa, ab, bb, aaa, aab, abb, ...}

(a*b)*: Set of strings with zero or more a's and zero or more b's:
{ε, a, b, aa, ab, ba, bb, aaa, aab, ...}

Semantics of Regular Expressions

Semantic Function \( \mathcal{L} \): Maps regular expressions to sets of strings.

\[
\begin{align*}
\mathcal{L}(\varepsilon) &= \{\varepsilon\} \\
\mathcal{L}(\alpha) &= \{\alpha\} \quad (\alpha \in \Sigma) \\
\mathcal{L}(r_1 | r_2) &= \mathcal{L}(r_1) \cup \mathcal{L}(r_2) \\
\mathcal{L}(r_1 r_2) &= \mathcal{L}(r_1) \cdot \mathcal{L}(r_2) \\
\mathcal{L}(r^*) &= \{\varepsilon\} \cup (\mathcal{L}(r) \cdot \mathcal{L}(r^*))
\end{align*}
\]

Finite State Automata

Regular expressions are used for specification, while FSA are used for computation.
FSAs are represented by a labeled directed graph.

- A finite set of states (vertices).
- Transitions between states (edges).
- Labels on transitions are drawn from \( \Sigma \cup \{\varepsilon\} \).
- One distinguished start state.
- One or more distinguished final states.

Finite State Automata: An Example

Consider the Regular Expression \((a | b)^*a(a | b)\).
\( \mathcal{L}((a | b)^*a(a | b)) = \{aa, ab, aaa, aab, baa, bab, aaaa, aaab, abaa, abab, baaa, ...\} \).
The following (non-deterministic) automaton determines whether an input string belongs to \( \mathcal{L}((a | b)^*a(a | b)) \):

Diagram:
Determinism

\[(a \mid b)^* a(a \mid b)\]:

Nondeterministic:
(NFA)

Deterministic:
(DFA)

Acceptance Criterion

A finite state automaton (NFA or DFA) **accepts** an input string \(x\)

... if beginning from the start state

... we can trace some path through the automaton

... such that the sequence of edge labels spells \(x\)

... and end in a final state.

Or, there exists a path in the graph from the start state to a final
state such that the sequence of labels on the path spells out \(x\)

Recognition with an NFA

Is \(abab \in \mathcal{L}(a \mid b)^* a(a \mid b)\)?

Input: \(a\ b\ a\ b\)

Path 1: \(1\ 1\ 1\ 1\ 1\) Accept
Path 2: \(1\ 1\ 1\ 2\ 3\)
Path 3: \(1\ 2\ 3\ \bot\ \bot\)

Accept

Recognition with a DFA

Is \(abab \in \mathcal{L}(a \mid b)^* a(a \mid b)\)?

Input: \(a\ b\ a\ b\)

Path: \(1\ 2\ 4\ 2\ 4\) Accept
### NFA vs. DFA

For every NFA, there is a DFA that accepts the same set of strings.

- NFA may have transitions labeled by $\epsilon$. (Spontaneous transitions)
- All transition labels in a DFA belong to $\Sigma$.
- For some string $x$, there may be *many* accepting paths in an NFA.
- For all strings $x$, there is *one unique* accepting path in a DFA.
- Usually, an input string can be recognized *faster* with a DFA.
- NFAs are typically *smaller* than the corresponding DFAs.

### Converting RE to FSA

**NFA**: Compile RE to NFA (Thompson’s construction [1968]), then match.

**DFA**: Compile to DFA, then match

(A) Convert NFA to DFA (Rabin-Scott construction), minimize

(B) Direct construction: RE derivatives [Brzozowski 1964].
   - More convenient and a bit more general than (A).

(C) Direct construction of [McNaughton Yamada 1960]
   - Can be seen as a (more easily implemented) specialization of (B).
   - Used in Lex and its derivatives, i.e., most compilers use this algorithm.

### NFA vs. DFA

$n = $ Size of Regular Expression (pattern)  
$m = $ Length of Input String (subject)

<table>
<thead>
<tr>
<th></th>
<th>NFA</th>
<th>DFA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size of Automaton</td>
<td>$O(n)$</td>
<td>$O(2^n)$</td>
</tr>
<tr>
<td>Recognition time per input string</td>
<td>$O(n \times m)$</td>
<td>$O(m)$</td>
</tr>
</tbody>
</table>

So, why bother with DFA?

- In many practical applications, the pattern is fixed and small, while the subject text is very large. So, the $O(mn)$ term is dominant over $O(2^n)$
- For many important cases, DFAs are of polynomial size
- In many applications, exponential blow-ups don't occur, e.g., compilers.
Derivative of Regular Expressions

The derivative of a regular expression $R$ w.r.t. a symbol $x$, denoted $\partial_x[R]$ is another regular expression $R'$ such that $L(R) = L(xR')$.

Basically, $\partial_x[R]$ captures the suffixes of those strings that match $R$ and start with $x$.

**Examples**
- $\partial_a[a(b|c)] = b|c$
- $\partial_a[(a|b)cd] = cd$
- $\partial_a[(a|b)\ast cd] = (a|b)\ast cd$
- $\partial_a[(a|b)\ast cd] = d$
- $\partial_a[(a|b)\ast cd] = \emptyset$

**inclEps($R$):** A predicate that returns true if $\epsilon \in L(R)$.

- $\text{inclEps}(a) = \text{false}$, $\forall a \in \Sigma$
- $\text{inclEps}(R_1|R_2) = \text{inclEps}(R_1) \lor \text{inclEps}(R_2)$
- $\text{inclEps}(R_1R_2) = \text{inclEps}(R_1) \land \text{inclEps}(R_2)$
- $\text{inclEps}(R^*) = \text{true}$

Note $\text{inclEps}$ can be computed in linear-time.

Definition of RE Derivative (2)

<table>
<thead>
<tr>
<th>$\partial_a[a]$</th>
<th>$\epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\partial_a[b]$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$\partial_a[R_1</td>
<td>R_2]$</td>
</tr>
<tr>
<td>$\partial_a[R^*]$</td>
<td>$\partial_a[R]\ast$</td>
</tr>
<tr>
<td>$\partial_a[R_1R_2]$</td>
<td>$\partial_a[R_1R_2]\partial_a[R_2]$ if $\text{inclEps}(R_1)$</td>
</tr>
<tr>
<td></td>
<td>$\partial_a[R_1]R_2$ otherwise</td>
</tr>
</tbody>
</table>

Note: $L(\epsilon) = \{\epsilon\} \neq L(\emptyset) = \{\}$

DFA Using Derivatives: Illustration

Consider $R_1 = (a|b)\ast a(a|b)$
- $\partial_a[R_1] = R_1|a(a|b) = R_2$
- $\partial_b[R_1] = R_1$
- $\partial_a[R_2] = R_1|a(b)\epsilon = R_3$
- $\partial_b[R_2] = R_1|\epsilon = R_4$
- $\partial_a[R_3] = R_1|a(b)\epsilon = R_3$
- $\partial_b[R_3] = R_1|\epsilon = R_4$
- $\partial_a[R_4] = R_1|a(b) = R_2$
- $\partial_b[R_4] = R_1$
McNaughton-Yamada Construction

Can be viewed as a simpler way to represent derivatives
- Positions in RE are numbered, e.g., \((a^1b^2)^*a^3(a^4b^5)^6\).
- A derivative is identified by its beginning position in the RE
- Or more generally, a derivative is identified by a set of positions
- Each DFA state corresponds to a position set (pset)

\[
\begin{align*}
R_1 & \equiv \{1, 2, 3\} \\
R_2 & \equiv \{1, 2, 3, 4, 5\} \\
R_3 & \equiv \{1, 2, 3, 4, 5, 6\} \\
R_4 & \equiv \{1, 2, 3, 6\}
\end{align*}
\]

McNaughton-Yamada (MY) Vs Derivatives

- Conceptually very similar
- MY takes a bit longer to describe, and its correctness a bit harder to follow.
- MY is also more mechanical, and hence is found in most implementations
- Derivatives approach is more general
  - Can support some extensions to REs, e.g., complement operator
  - Can avoid some redundant states during construction
    - Example: For \(ac|bc\), DFA built by derivative approach has 3 states, but the one built by MY construction has 4 states
    - The derivative approach merges the two c's in the RE, but with MY, the two c's have different positions, and hence operations on them are not shared.

Avoiding Redundant States

- Automata built by MY is not optimal
  - Automata minimization algorithms can be used to produce an optimal automaton.
- Derivatives approach associates DFA states with derivatives, but does not say how to determine equality among derivatives.
- There is a spectrum of techniques to determine RE equality
  - MY is the simplest: relies on syntactic identity
  - At the other end of the spectrum, we could use a complete decision procedure for RE equality.
    - In this case, the derivative approach yields the optimal RE!
  - In practice we would tend to use something in the middle
    - Trade off some power for ease/efficiency of implementation
RE to DFA conversion: Complexity

- Given DFA size can be exponential in the worst case, we obviously must accept worst-case exponential complexity.
- For the derivatives approach, it is not immediately obvious that it even terminates!
  - More obvious for McNaughton-Yamada approach, since DFA states correspond to position sets, of which there are only $2^n$.
- Derivative computation is linear in RE size in the general case.
- So, overall complexity is $O(n^2)$
- Complexity can be improved, but the worst-case $2^n$ takes away some of the rationale for doing so.
- Instead, we focus on improving performance in many frequently occurring special cases where better complexity is achievable.

RE Matching: Summary

- Regular expression matching is much more powerful than matching on plain strings (e.g., prefix, suffix, substring, etc.)
- Natural that RE matching algorithms can be used to solve plain string matching
- But usually, you pay for increased power: more complex algorithms, larger runtimes or storage, etc.

We study the RE approach because it seems to not only do RE matching, but yield simpler, more efficient algorithms for matching plain strings.

String Lookup

Problem: Determine if $s$ equals any of the strings $p_1, \ldots, p_k$.
- Equivalent to the question: does the RE $p_1[p_2] \cdots [p_k]$ match $s$?
- We can use the derivative approach, except that derivatives are very easy to compute.
- Results in an FSA that is a tree
- More commonly known as a trie

Trie Example

$$R_0 = \text{top}|\text{tool}|\text{tooth}|\text{at}|\text{sunk}|\text{sunny}$$

$$R_1 = \partial_t[R_0] = \text{ap}|\text{oool}|\text{ooth}$$

$$R_2 = \partial_o[R_1] = \text{p}|\text{oool}|\text{oth}$$

$$R_3 = \partial_p[R_2] = \epsilon$$

$$R_4 = \partial_o[R_2] = \text{l}|\text{th}$$

$$R_5 = \partial_p[R_4] = \epsilon$$

$$R_6 = \partial_t[R_5] = \text{h}, R_7 = \partial_h[R_6] = \epsilon$$

$$R_8 = \partial_o[R_6] = \text{t}, R_9 = \partial_t[R_8] = \epsilon$$

$$R_{10} = \partial_{\text{unk}}[R_9] = \text{unk}|\text{unny}$$

$$R_{11} = \partial_o[R_10] = \text{uk}|\text{nny}$$

$$R_{12} = \partial_o[R_11] = \text{k}|\text{ny}$$

$$R_{13} = \partial_k[R_{12}] = \epsilon$$

$$R_{14} = \partial_o[R_{13}] = y, R_{15} = \partial_y[R_{14}] = \epsilon$$
Trie Construction Summary

- A versatile data structure for dictionaries, or more generally, sets of strings.
- Derivatives of REs in this context can be computed very quickly (in time proportional to the number of "|" operators in the RE).
- Overall time for trie construction is linear in the size of input.
- Tries amenable to more efficient representation and implementation, as compared to DFAs in general.

Trie Summary

- A data structure for string sets with sublinear complexity.
  - Support $O(l)$ membership and max. common prefix (MCP) queries.
  - $l$ is size of query string (or the size of MCP).
  - Set union/intersection are linear in size of the smaller set.
  - Sublinear in input size when one input trie is larger than the other.
  - Can support set difference as well — with same complexity.
- When viewed as an FSA, can support operations such as language intersection efficiently.
  - Example: find all dictionary words matching $t(a-z)p(a-z)*$.
    - Use a trie to represent all words in a dictionary.
    - Query could be answered in time sublinear in dictionary size.
    - With our example trie, we examine only 4 of 16 nodes in the trie.

Implementing Transitions

How to implement transitions?

Array: Efficient, but unacceptable space when $|\Sigma|$ is large.

Linked list: Space-efficient, but slow.

Hash tables: Mid-way between the above two options, but noticeably slower than arrays. Collisions are a concern.
- But customized hash tables for this purpose can be developed.
- Alternatively, since transition tables are static, we can look for perfect hash functions.

Specialized representations: For special cases such as exact search, we could develop specialized alternatives that are more efficient than all of the above.

Exact Search

- Determine if a pattern $P[1..n]$ occurs within text $S[1..m]$.
  - Find $j$ such that $P[1..n] = S[j:(j+n-1)]$.
- An RE matching problem: Does $\Sigma^*P\Sigma^*$ match $S$?
  - Note: $\Sigma^*$ matches any arbitrary string (incl. $\epsilon$).
- We consider $\Sigma^*p$ since it can identify all matches.
  - A match can be reported each time a final state is reached.
  - In contrast, $\Sigma^*P\Sigma^*$ may identify just one match.
**Intro RE FSA to DFA Trie grep agrep Fing.print Suffix trees**

**Using Derivatives** KMP Aho-Corasick Shift-And

---

**Exact Search Example**

Consider $R_0 = (\Sigma^0)^* a^1 a^2 b^3 a^4 b^5 a^6 a^7 b^8$

We use McNaughton-Yamada. Recall that with this technique:

- States are identified by position sets.
- A position denotes a derivative starting at that position.
- A position set indicates the union of REs corresponding to each position.

For instance, position set $\{0, 2, 3\}$ represents $R_0|a^2 b^3 a^4 b^5 a^6|b^3 a^4 b^5 a^6 a^7$

---

**Improving Exact Search: Observations**

The DFA has a linear structure, with states 1 to $n + 1$:

- State $i$ is reached on matching the prefix $P[1..i-1]$

The largest element of $\text{pset}(i)$ is $i$

If you are in state $i$ after scanning $S[k]$:

- Let $P' = P[1..i-1] = S[..k]$
- “Unwinding” of $\Sigma^*$: A prefix of $P'$ can be matched against $\Sigma^*$, while the rest can match $P[1..j-1]$

So, $\text{pset}(i)$ includes every $j$ such that $P[1..j-1] = P[1..i-1]$

---

**Improving Exact Search: Key Ideas**

**Main Idea**

- Remember only the largest $j < i$ in $\text{pset}(i)$
  - You can look at $\text{pset}(j)$ for the next smaller element
  - Add failure links from state $i$ to $j$ for this purpose

- Two positions per $\text{pset} \implies O(n)$ construction time
Exact Search: KMP Automaton

- Only two positions per state: \{j, i\}
- Two trans per state: forward and fail
- If the symbol at both positions is the same, then the next state has the pset \{j+1, i+1\}
- Otherwise, the match at \(j\) cannot advance on the symbol at \(i\). So, we use the fail link to identify the next shorter prefix that can advance:
  - Follow fail link to state \(u\) with pset \{\(k, j\)\} and see if that match can advance
  - Otherwise, follow the fail link from \(u\) and so on.
- Failure link chase is amortized \(O(1)\) time, while other steps are \(O(1)\) time.

KMP Algorithm

\[
\begin{align*}
\text{BuildAuto}(P[1..m]) & \\
  j &= 0 \\
  \text{for } i = 1 \text{ to } m & \text{ do} \\
  & \text{fail}[i] = j \\
  & \text{while } j > 0 \text{ and } P[i] \neq P[j] \text{ do} \\
  & \quad j = \text{fail}[j] \\
  & \quad j++ \\
\end{align*}
\]

1. Simple, avoids explicit representation of states/transitions.
2. Each state has two transitions: normal and failure.
   - Normal transition at state \(i\) is on \(P[i]\)
   - Fail links are stored in an array \(\text{fail}[i]\)
3. \(\text{BuildAuto}\) is like matching pattern with itself!
4. Algorithm is unbelievably short and simple!

Multi-pattern Exact Search

- Can we extend KMP to support multiple patterns?
- Yes we can! It is called Aho-Corasick (AC) automaton
  - Note that AC algorithm was published before KMP!
  - Today, many systems use AC (e.g., grep, snort), but not KMP.
- KMP looks like a linear automaton plus failure links.
  - Aho-Corasick looks like a trie extended with failure links.
  - Failure links may go to a non-ancestor state
- Failure link computations are similar
- McNaughton-Yamada and the derivatives algorithms build an automaton similar to AC, just as they did for KMP.
- One can understand Aho-Corasick as a specialization of these algorithms, as we did in the case of KMP.
- Or, as a generalization of KMP

Aho-Corasick Automaton

- As with KMP, we can think of AC as a specialization of MY.
  - Retain just the largest two numbers \(i\) and \(j\) in the pset.
  - Use the value of \(j\) as target for failure link, and to find \(j'\) in the successor state's pset \{\(j', i+1\)\}
- But there is an extra wrinkle:
  - With KMP, there is one pattern; we keep two positions from it.
  - With AC, we have multiple patterns, so a state's pset will contain positions from multiple patterns.
    - If two patterns share a prefix, the automaton state reached by this prefix will contain the next positions from both patterns.
  - We will simply retain one of these positions, say, from the higher numbered pattern.
  - To avoid clutter in our example, we omit numbering of positions that will be dropped this way.
Aho-Corasick Example

Consider RE

\[(\Sigma^0)^* (top^3$top^3$|tool$tool$|t^1o^2ü^8$ü^8$|p^8e^n$e^n|op^8e^n$e^n|o^1ö^2z^6$z^6$)^n)\]

- To reduce clutter, positions that always occur with other positions are not numbered, e.g., o in top (occurs with first o in tooth)
- Figure omits failure links that go to start state.

Alternative Approaches for Exact Search

- DFA approach had significant preprocessing (“compiling”) costs, but optimized runtime — exactly \(m\) comparisons.
- KMP reduces compile-time by shifting more work (up to \(2m\) comparisons) to runtime.
- DFA states contain information about all matching prefixes, but KMP states retain just the two longest ones.
- Other prefixes are essentially being computed at runtime by following fail links.
- Can we remember even less in automaton states?
  - Can we leave all matching prefixes to be computed at runtime?
  - 1 while also simplifying automaton structure

Parallel Exact Search

- Key Idea: Maintain all matching prefixes at runtime.
- Simultaneously advance the state of all these prefixes after reading next input character.
  - So, there will only be \(O(m)\) “comparisons” total.
- How can we do this?
  - Think of KMP automaton, strip off all failure links
  - The automaton is now linear: each state has a single successor
  - On the next input symbol, the prefix will
    - either be extended by transitioning to the successor state
    - or, the symbol doesn’t match, and this match is aborted

Bit-parallel Exact Search: Shift-And Method

- A search for match begins on each symbol \(S[k]\) in input
  - Think of placing a token in start state each time you slide \(P\) over \(S\)
  - If symbols continue to match, tokens advance through successive states until they reach the final state.
  - If there is a mismatch, the corresponding token “disappears” or “dies”
Bit-parallel Exact Search: Shift-And Method

- At any time, token for matches beginning at \( S[k - n] \) through \( S[k] \) will be in the automaton.
- Use a bitvector \( T[0..n] \) to record these tokens.
- \( T[j] \) indicates if the token for match beginning at \( S[k - j] \) is still alive, i.e., \( S[k - j..k - 1] = P[1..j] \)
- \( T[n] = 1 \) indicates a completed match.

Shift-And Method Illustration

\[
\begin{array}{cccccccc}
M_k & a & M_{k-1} & a & M_{k-2} & b & M_{k-3} & a & M_{k-4} & b & M_{k-5} & a & M_{k-6} & a & M_{k-7}
\end{array}
\]

Each time \( k \) is incremented, advance tokens forward by one state:

- \( T[j] \) advances if \( S[k] \) matches the transition label.
- Use a bitvector \( \delta[0..n] \) to record transitions.
- \( \delta_x[j] = 1 \) if the transition out of state \( j \) is labeled \( x \)
- In other words, \( \delta_x[j] = 1 \) iff \( P[j + 1] = x \)
- Note \( \delta_a = 01101011, \delta_b = 00010100 \). (Note that bitvector indices go from right to left, while string indices go left-to-right.)
- This means that when \( k \) is incremented, \( T \) should be updated as:

\[
T = [(T \& \delta S[k]) \ll 1] + 1
\]

Shift-And Method Illustration

\[
\begin{array}{cccccccc}
T_0 & a & T_1 & a & T_2 & b & T_3 & a & T_4 & b & T_5 & a & T_6 & a & T_7
\end{array}
\]

\( k=11 \)

\[
\begin{array}{ll}
S & aabdaababaaba \\
P & aababaa \\
T & 00100011 \\
\delta_a & 01101011 \\
T_{new} & 01000011
\end{array}
\]

\( k=12 \)

\[
\begin{array}{ll}
S & aabdaababaaba \\
P & aababaa \\
T & 01000011 \\
\delta_a & 01101011 \\
T_{new} & 10000111
\end{array}
\]
### Shift-And Method Illustration

<table>
<thead>
<tr>
<th>k=13</th>
<th>k=14</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>aabcdaababaaba</td>
</tr>
<tr>
<td>P</td>
<td>aababaa</td>
</tr>
<tr>
<td>T</td>
<td>10000111</td>
</tr>
<tr>
<td>δb</td>
<td>00010100</td>
</tr>
<tr>
<td>T\text{new}</td>
<td>00001001</td>
</tr>
</tbody>
</table>

### Approximate Search

Approach 1: Use edit-distance algorithm
- Expensive
- Does not allow for multiple patterns
  - Unless you try the patterns one-by-one

Approach 2: Levenshtein Automaton
- Can be much faster, especially when \( p \) is small.
- Supports multiple patterns
- Enables applications such as spell-correction

### Levenshtein Automaton

No errors permitted.
Levenshtein Automaton

- Up to one missing character (deletion).

- Up to one deletion and one insertion.

- Up to one deletion, or insertion, or substitution

- Up to a total of two deletions, insertions, or substitution
We extend the notation to explicitly include of the current position \( k \) in \( T \).

With this extension, our original equation for \( T \) becomes

\[
T^k = \| (T^{k-1} \& \delta_S[k]) \| \leq 1
\]

Extending this to the case of \( U \), we have

\[
U^k = T^{k-1} \quad // \text{move } \uparrow, \text{i.e., Insertion of } S[k]
\]

| \( T^{k-1} \leq 1 \) \quad // \text{move } \nearrow \text{ with substitution} |
| \( T^k \leq 1 \) \quad // \text{move } \swarrow \text{ with deletion} |
| \( [(U^{k-1} \& \delta_S[k]) \leq 1]1 \quad // \text{move } \rightarrow |

Convert to DFA (subset construction)

- Potentially \( O(n^k) \) states, where \( k \) is the max edit distance permitted

Adapt Shift-and algorithm

- We already know how to maintain \( T[0..n] \)
- Need to extend to compute \( U \) from \( T \), \( V \) from \( U \) and so on.

When a word \( w \) is misspelled, we want to find the closest matching word in the dictionary

- Or, list all matches within an edit distance of \( l \)

Approach:

- Build Levenshtein automaton for \( w \) with \( l + 1 \) “layers”
- Run the dictionary trie through the automaton
- List all matches

Alternatively, a DFA for the Levenshtein automaton could be built, and the trie run through this DFA.

The DFA could be directly constructed as well, without going through an NFA and powerset construction.
Using arithmetic for exact matching

Problem: Given strings $P[1..n]$ and $T[1..m]$, find occurrences of $P$ in $T$ in $O(n+m)$ time.

Idea: To simplify presentation, assume $P, T$ range over $[0-9]$
- Interpret $P[1..n]$ as digits of a number $p = 10^{n-1}P[1] + 10^{n-2}P[2] + \cdots + 10^nP[n]$
- Similarly, interpret $T[i..(i+n-1)]$ as the number $t_i$
- Note: $P$ is a substring of $T$ at $i$ iff $p = t_i$
- To get $t_{i+1}$, shift $T[i]$ out of $t_i$, and shift in $T[i+m]$: $t_{i+1} = (t_i - 10^{n-1}T[i]) \cdot 10 + T[i+n]$

We have an $O(n+m)$ algorithm. Almost: we still need to figure out how to operate on $n$-digit numbers in constant time!

Carter-Wegman-Rabin-Karp Algorithm

Difficulty with Rabin-Karp: Need to generate random primes (not easy).

New Idea: Make the radix random, as opposed to the modulus
- We still compute modulo a prime $q$, but it is not random.

Alternative interpretation: We treat $P$ as a polynomial $p(x) = \sum_{i=1}^{n} P[n-i] \cdot x^i$

and evaluate this polynomial at a randomly chosen value of $x$

What is the likelihood of false matches? Note that false match occurs when $p(x) = t_i(x)$, or when $p(x) - t_i(x) = 0$.

Arithmetic modulo prime defines a field, so an $(n-1)$th degree polynomial has $n-1$ roots
- i.e., $(n-1)/q$ of the $q$ possible choices of $x$ result in a false match.

Rabin-Karp Fingerprinting

Key Idea
- Instead of working with $n$-digit numbers,
  - perform all arithmetic modulo a random prime number $q$,
  - where $q > n^2$ fits within wordsize
- All observations made on previous slide still hold
  - Except that $p = t_i$ does not guarantee a match
  - Typically, we expect matches to be infrequent, so we can use $O(n)$ exact-matching algorithm to confirm probable matches.

Rolling Hashes

RK and CWRK are examples of rolling hashes
- Hash computed on text within a sliding window

Key point: Incremental computation of hash as the window slides.

Polynomial-based hashes are easy to compute incrementally:
$t_{i+1} = (t_i - x^nT[i]) \cdot x + T[i+n]$

Complexity:
- $x^n$ is fixed once the window size is chosen
- Takes just two multiplications, one modulo per symbol
- $O(m+n)$ multiplication/modulo operations in total
Other Rolling Hashes

In some contexts, multiplication/modulo may be too expensive.

**Alternatives:**
- Use shifts, cyclic shifts, substitution maps and xor operations, avoiding multiplications altogether.
- Need considerable research to find good fingerprinting functions.
- Example: Adler32 — used in zlib (used everywhere) and rsync.

\[
A_l = 1 + \sum_{k=0}^{l-1} t_{i+k} \mod 65521
\]

\[
B = \sum_{k=1}^{n} A_k = n + \sum_{k=0}^{n-1} (n-k)t_{i+k} \mod 65521
\]

\[
H = (B \ll 16) + A
\]

Rolling Hash and Common Substring Problem

- To find a common substring of length \( l \) or more
  - Compute rolling hashes of \( P \) and \( T \) with window size \( l \)
  - Takes \( O(n + m) \) time.
  - \( O(nm) \) possible collisions, so expected number of collisions increases.
  - Unless collision probability is of the order of \( 1/nm \), expected runtime can be nonlinear.

- Can find longest common substring (LCS) using a binary-search like process, with a total complexity of \( O((n + m)\log(n + m)) \)

zlib/gzip, rsync, binary diff, etc.

**rsync:** Synchronizes directories across network
- Need to minimize data transferred
  - A diff requires entire files to be copied to client side first!
  - Uses timestamps (or whole-file checksums) to detect unchanged files
  - For modified files, uses Adler-32 to identify modified regions
  - Find common substrings of certain length, say, 128-bytes
  - Relies on stronger MD-5 hash to verify unmodified regions

**gzip:** Uses rolling hash (Adler-32) to identify text that repeated from previous 32KB window
- Repeating text can be replaced with a “pointer:” (offset, length).

**Binary diff:** Many programs such as xdelta and svn need to perform diffs on binaries; they too rely on rolling hashes.
- **diff** depends critically on line breaks, so does poorly on binaries

Suffix Trees [Weiner 1973]

- A versatile data structure with wide applications in string search and computational biology
- “Compressed” trie of all suffixes of a string appended with “$”
  - Linear chains in the trie are compressed
  - Edges can now be substrings.
  - Each state has at least two children.
  - Leaves identify starting position of that suffix.
- **Key point: Can be constructed in linear time!**
- **Supports sublinear exact match queries, and linear LCS queries**
  - With linear-time preprocessing on the text (to build suffix tree),
  - yields better runtime than techniques discussed so far.
- **Applicable to single as well as multiple patterns or texts!**
Suffix Tree Example

Key Property Behind Suffix Trees
Substrings are prefixes of suffixes

- Failure links used only during construction
- Uses end-marker “$”
- Leaves identify starting position of suffix
- Typically, it is the text we preprocess, not the pattern.

Images from Wikipedia commons

Finding Substrings and Suffixes

Is \( p \) a substring of \( t \)?

Example: Is \( anan \) a substring of \( banana \)?

Solution:

- Follow path labeled \( p \) from root of suffix tree for \( t \).
- If you fail along the way, then “no,” else “yes”
- \( p \) is a suffix if you reach a leaf at the end of \( p \)
- \( O(|p|) \) time, independent of \( |t| \) — great for large \( t \)

Counting # of Occurrences of \( p \)

How many times does “anan” occur in \( t \)?

Solution:

- Follow path labeled \( p \) from root of suffix tree for \( t \).
- Count the number of leaves below.
- \( O(|p|) \) time if additional information (# of leaves below) maintained at internal nodes.

Self-LCS (Or, Longest Common Repeat)

What is the longest substring that repeats in \( t \)?

Solution:

- Find the deepest non-leaf node with two or more children!
- In our example, it is \( ana \).
**LC extension of \(i\) and \(j\)**

**Longest Common Extension**

Longest common prefix of suffixes starting at \(i\) and \(j\)

- Locate leaves labeled \(i\) and \(j\).
- Find their least common ancestor (LCA).
- The string spelled out by the path from root to this LCA is what we want.

**LCS with another string \(p\)**

- We can use the same procedure as LCR, if suffixes of \(p\) were also included in the suffix tree.
- Leads to the notion of generalized suffix tree.

**Generalized Suffix Trees**

Suffix trees for multiple strings \(p_1, \ldots, p_n\)

**Example:** att, tag, gat

Simple solution:

1. Build suffix tree for string att\#tag\#gat\#
2. For every leaf node, remove any text after the first \# symbol.

**LCS of \(p\) and \(t\):** Build GST for \(s\) and \(t\), find deepest node that has descendants corresponding to \(s\) and \(t\)

**LCS of \(p_1, \ldots, p_k\):** Build GST for \(p_1\) to \(p_k\), find deepest node that has descendants from all of \(p_1, \ldots, p_n\)

**Find strings in database containing \(q\):**

- Build a suffix tree of all strings in the database
- Follow path that spells \(q\)
- \(q\) occurs in every \(p_i\) that appears below this node.
**Suffix Arrays [Manber and Myers 1989]**

- **Drawbacks of suffix trees:**
  - Multiple pointers per internal node: significant storage costs
  - Pointer-chasing is not cache-friendly
- **Suffix arrays address these drawbacks.**
  - Requires same asymptotic storage \(O(n)\) but constant factors a lot smaller — 4x or so.
  - Instead of navigating down a path in the tree, relies on binary search
    - Increases asymptotic cost by \(O(\log n)\), but can be faster in practice due to better cache performance etc.

**Finding Suffix Arrays**

- Maintaining LCP of successive suffixes speeds up algorithms
  - Search for substring \(p\) in \(O(|p| + \log |t|)\)
  - Count number of occurrences of \(p\) in \(O(|p| + \log |t|)\) time
  - Search for longest common repeat \(O(|t|)\) time
- Use binary search to locate suffixes etc.

<table>
<thead>
<tr>
<th>(i)</th>
<th>(T_i)</th>
<th>(A_i)</th>
<th>(T_A)</th>
<th>LCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mississippi$</td>
<td>12</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ississippi$</td>
<td>11</td>
<td>i$</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>ssissippi$</td>
<td>8</td>
<td>ippi$</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>ssissippi$</td>
<td>5</td>
<td>ississippi$</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>ississippi$</td>
<td>2</td>
<td>ississippi$</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>ssissippi$</td>
<td>1</td>
<td>mississippi$</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>sippi$</td>
<td>10</td>
<td>pi$</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>ippi$</td>
<td>9</td>
<td>ppi$</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>ppi$</td>
<td>7</td>
<td>sippi$</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>pi$</td>
<td>4</td>
<td>sississippi$</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>i$</td>
<td>6</td>
<td>ssippi$</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>$</td>
<td>3</td>
<td>ssissippi$</td>
<td>3</td>
</tr>
</tbody>
</table>