5.3 **Substring Search**

- introduction
- brute force
- Knuth–Morris–Pratt
- Boyer–Moore
- Rabin–Karp

**Substring search**

**Goal.** Find pattern of length $M$ in a text of length $N$.

Typically $N \gg M$

- **pattern** → NEEDLE
- **text** → INAHAYSTACK NEEDLE IN A
- **match**

**Substring search applications**

**Goal.** Find pattern of length $M$ in a text of length $N$.

Typically $N \gg M$

- **pattern** → NEEDLE
- **text** → INAHAYSTACK NEEDLE IN A
- **match**
**Substring search applications**

**Goal.** Find pattern of length $M$ in a text of length $N$. Typically $N \gg M$.

- **Pattern** → NEEDLE
- **Text** → INAHAYSTACK NEEDLE IN A
- **Match**

**Computer forensics.** Search memory or disk for signatures, e.g., all URLs or RSA keys that the user has entered.

http://citp.princeton.edu/memory

**Electronic surveillance.**

Need to monitor all internet traffic. (security)

No way! (privacy)

Well, we're mainly interested in "ATTACK AT DAWN"

OK. Build a machine that just looks for that.

"ATTACK AT DAWN" substring search machine found

**Screen scraping.** Extract relevant data from web page.

**Ex.** Find string delimited by `<b>` and `</b>` after first occurrence of pattern Last Trade:

http://finance.yahoo.com/q?s=goog

---

**Identify patterns indicative of spam.**

- PROFITS
- LOSE WEIGHT
- herbal Viagra
- There is no catch.
- This is a one-time mailing.
- This message is sent in compliance with spam regulations.
Screen scraping: Java implementation

Java library. The `indexOf()` method in Java’s `String` data type returns the index of the first occurrence of a given string, starting at a given offset.

```java
public class StockQuote {
    public static void main(String[] args) {
        String name = "http://finance.yahoo.com/q?s=";
        In in = new In(name + args[0]);
        String text = in.readAll();
        int start = text.indexOf("Last Trade:", 0);
        int from = text.indexOf("<b>", start);
        int to = text.indexOf("<"/b>", from);
        String price = text.substring(from + 3, to);
        StdOut.println(price);
    }
}
```

Caveat. Must update program if Yahoo format changes.

5.3 SUBSTRING SEARCH

Brute-force substring search

Check for pattern starting at each text position.

<table>
<thead>
<tr>
<th>i</th>
<th>j</th>
<th>i+j</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>

Check for pattern starting at each text position.

<table>
<thead>
<tr>
<th>i</th>
<th>j</th>
<th>i+j</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>

public static int search(String pat, String txt) {
    int M = pat.length();
    int N = txt.length();
    for (int i = 0; i <= N - M; i++) {
        int j;
        for (j = 0; j < M; j++)
            if (txt.charAt(i+j) != pat.charAt(j)) break;
        if (j == M) return i; // index in text where pattern starts
    }
    return N; // not found
}
Substring search quiz 1

What is the worst-case running time of brute-force substring search as a function of the number of characters in the pattern $M$ and text $N$?

A. $M + N$
B. $M^2$
C. $MN$
D. $N^2$
E. I don’t know.

---

Brute-force substring search: alternate implementation

Same sequence of character compares as previous implementation.
- $i$ points to end of sequence of already-matched characters in text.
- $j$ stores # of already-matched characters (end of sequence in pattern).

<table>
<thead>
<tr>
<th>$i$</th>
<th>$j$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>C</td>
<td>A</td>
<td>D</td>
<td>A</td>
<td>B</td>
<td>R</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td></td>
<td></td>
<td>A</td>
<td>D</td>
<td>A</td>
<td></td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
<td>D</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td></td>
</tr>
</tbody>
</table>

```java
public static int search(String pat, String txt)
{
    int i, N = txt.length();
    int j, M = pat.length();
    for (i = 0, j = 0; i < N && j < M; i++)
    {
        if (txt.charAt(i) == pat.charAt(j)) j++;
        else { i--; j = 0; }
    }
    if (j == M) return i - M;
    else return N;
}
```

---

Backup

In many applications, we want to avoid backup in text stream.
- Treat input as stream of data.
- Abstract model: standard input.

Brute-force algorithm needs backup for every mismatch.

```
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
A A A A A A A A A A A A A A
```

Approach 1. Maintain buffer of last $M$ characters.
Approach 2. Stay tuned.

---

Algorithmic challenges in substring search

Brute-force is not always good enough.

**Theoretical challenge.** Linear-time guarantee.

**Practical challenge.** Avoid backup in text stream.

Now is the time for all people to come to the aid of their party. Now is the time for all good people to come to the aid of their party. Now is the time for every good person to come to the aid of their party. Now is the time for all good people to come to the aid of their party. Now is the time for all good Republicans to come to the aid of their party. Now is the time for all good Democrats to come to the aid of their party. Now is the time for all good people to come to the aid of their party. Now is the time for all good people to come to the aid of their party. Now is the time for all good Republicans to come to the aid of their party. Now is the time for all good Democrats to come to the aid of their party. Now is the time for all good people to come to the aid of their party. Now is the time for all good Republicans to come to the aid of their party. Now is the time for all good Democrats to come to the aid of their party.
Knuth–Morris–Pratt substring search

Intuition. Suppose we are searching in text for pattern BAAAAAAA.
- Suppose we match 5 chars in pattern, with mismatch on 6th char.
- We know previous 6 chars in text are BAAAA.
- Don’t need to back up text pointer!

Knuth–Morris–Pratt algorithm. Clever method to always avoid backup!

Deterministic finite state automaton (DFA)

DFA is abstract string-searching machine.
- Finite number of states (including start and halt).
- Exactly one state transition for each char in alphabet.
- Accept if sequence of state transitions leads to halt state.

<table>
<thead>
<tr>
<th>state</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat.charAt(j)</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>C</td>
</tr>
<tr>
<td>dfa[i][j]</td>
<td>B</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

Internal representation
- If in state j reading char c:
  - if j is 6 halt and accept
  - else move to state dfa[c][j]

Graphical representation

Knuth–Morris–Pratt demo: DFA simulation

A A B A C A A B A B A C A A
**Interpretation of Knuth–Morris–Pratt DFA**

**Q.** What is interpretation of DFA state after reading in $\text{txt}[i]$?

**A.** State = number of characters in pattern that have been matched.

**Ex.** DFA is in state 3 after reading in $\text{txt}[0..6]$. Length of longest prefix of $\text{pat}[]$ that is a suffix of $\text{txt}[0..i]$

```
  0  1  2  3  4  5  6  7  8
  B  C  B  A  A  B  A  C  A
```

**Substring search quiz 2**

Which state is the DFA in after processing the following input?

A. 0
B. 1
C. 3
D. 4
E. I don’t know.

```
ABABABABCAABACABACABACABACABABAB
```

**Knuth–Morris–Pratt substring search: Java implementation**

Key differences from brute-force implementation.
- Need to precompute $\text{dfa}[][]$ from pattern.
- Text pointer $i$ never decrements.

```java
public int search(String txt) {
    int i, j, N = txt.length();
    for (i = 0, j = 0; i < N && j < M; i++)
        if (j == M) return i - M;
        else return N;
}
```

Running time.
- Simulate DFA on text: at most $N$ character accesses.
- Build DFA: how to do efficiently? [warning: tricky algorithm ahead]

**Knuth–Morris–Pratt substring search: Java implementation**

Key differences from brute-force implementation.
- Need to precompute $\text{dfa}[][]$ from pattern.
- Text pointer $i$ never decrements.
- Could use input stream.

```java
public int search(In in) {
    int i, j;
    while (!in.isEmpty() && j < M) {
        if (j == M) return i - M;
        else return NOT_FOUND;
    }
```
Knuth–Morris–Pratt demo: DFA construction

How to build DFA from pattern?

Include one state for each character in pattern (plus accept state).

Constructing the DFA for KMP substring search for A B A B A C

How to build DFA from pattern?

Match transition. If in state j and next char c == pat.charAt(j), go to j+1.

Mismatch transition. If in state j and next char c != pat.charAt(j), then the last j-1 characters of input are pat[1..j-1], followed by c.

Running time. Seems to require j steps.

To compute dfa[c][j]: Simulate pat[1..j-1] on DFA and take transition c.

Ex. dfa['A'][5] = 1
simulate BABA

dfa['B'][5] = 4
simulate BABAB

How to build DFA from pattern?
How to build DFA from pattern?

Mismatch transition. If in state \( j \) and next char \( c \neq \text{pat.charAt}(j) \), then the last \( j-1 \) characters of input are \( \text{pat}[1..j-1] \), followed by \( c \).

To compute \( \text{dfa}[c][j] \): Simulate \( \text{pat}[1..j-1] \) on DFA and take transition \( c \).

Running time. Takes only constant time if we maintain state \( x \).

\[
\begin{array}{c|c|c|c|c|c|c}
 & 0 & 1 & 2 & 3 & 4 & 5 \\
\hline
\text{pat.charAt}(j) & A & B & A & B & A & C \\
\hline
\text{dfa}()[j] & B & C & A & B & A & C \\
\end{array}
\]

Constructing the DFA for KMP substring search: Java implementation

For each state \( j \):
- Copy \( \text{dfa}()[x] \) to \( \text{dfa}()[j] \) for mismatch case.
- Set \( \text{dfa}[	ext{pat.charAt}(j)][j] \) to \( j+1 \) for match case.
- Update \( x \).

```java
public KMP(String pat) {
    this.pat = pat;
    M = pat.length();
    dfa = new int[R][M];
    dfa[pat.charAt(0)][0] = 1;
    for (int x = 0, j = 1; j < M; j++) {
        for (int c = 0; c < R; c++)
            dfa[c][j] = dfa[c][x];
        dfa[pat.charAt(j)][j] = j+1;
        x = dfa[pat.charAt(j)][x];
    }
}
```

Running time. \( M \) character accesses (but space/time proportional to \( R M \)).

Knuth–Morris–Pratt demo: DFA construction in linear time

Constructing the DFA for KMP substring search for \( A B A B A C \)

KMP substring search analysis

**Proposition.** KMP substring search accesses no more than \( M + N \) chars to search for a pattern of length \( M \) in a text of length \( N \).

**Pf.** Each pattern character accessed once when constructing the DFA; each text character accessed once (in the worst case) when simulating the DFA.

**Proposition.** KMP constructs \( \text{dfa}[] \) in time and space proportional to \( R M \).

**Larger alphabets.** Improved version of KMP constructs \( \text{nfa}[] \) in time and space proportional to \( M \).
Knuth–Morris–Pratt: brief history

- Independently discovered by two theoreticians and a hacker.
  - Knuth: inspired by esoteric theorem, discovered linear algorithm
  - Pratt: made running time independent of alphabet size
  - Morris: built a text editor for the CDC 6400 computer
- Theory meets practice.

Boyer–Moore: mismatched character heuristic

**Intuition.**
- Scan characters in pattern from right to left.
- Can skip as many as \( M \) text chars when finding one not in the pattern.

5.3 Substring Search

- Introduction
- Brute force
- Knuth–Morris–Pratt
- Boyer–Moore
- Rabin–Karp

Cyclic Rotation

A string \( s \) is a cyclic rotation of \( t \) if \( s \) and \( t \) have the same length and \( s \) is a suffix of \( t \) followed by a prefix of \( t \).

<table>
<thead>
<tr>
<th>( s )</th>
<th>( t )</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>ROTATEDSTRING</td>
</tr>
<tr>
<td>no</td>
<td>ROTATEDSTRING</td>
</tr>
</tbody>
</table>

**Problem.** Given two binary strings \( s \) and \( t \), design a linear-time algorithm to determine if \( s \) is a cyclic rotation of \( t \).
Boyer–Moore: mismatched character heuristic

Q. How much to skip?

Case 1. Mismatch character not in pattern.

before

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . T L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

after

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . T L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

mismatch character 'T' not in pattern: increment i one character beyond 'T'

Case 2a. Mismatch character in pattern.

before

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . N L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

after

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . N L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

mismatch character 'N' in pattern: align text 'N' with rightmost pattern 'N'

Case 2b. Mismatch character in pattern (but heuristic no help).

before

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . E L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

aligned with rightmost E?

<table>
<thead>
<tr>
<th>txt</th>
<th>. . . . . . . E L E . . . . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>pat</td>
<td>N E E D L E</td>
</tr>
</tbody>
</table>

mismatch character 'E' in pattern: align text 'E' with rightmost pattern 'E'?
Boyer–Moore: mismatched character heuristic

Q. How much to skip?

A. Precompute index of rightmost occurrence of character $c$ in pattern.
(-1 if character not in pattern)

```
<table>
<thead>
<tr>
<th></th>
<th>N</th>
<th>E</th>
<th>D</th>
<th>L</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td></td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>A</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>B</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>C</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>D</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td>-1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
</tr>
</tbody>
</table>
...|
| L | -1| -1| -1| -1|  4|
| M | -1| -1| -1| -1|  4|
| N | -1|  0|  0|  0|  0|
...|
```

right = new int[R];
for (int c = 0; c < R; c++)
  right[c] = -1;
for (int j = 0; j < M; j++)
  right[pat.charAt(j)] = j;

Boyer–Moore: Java implementation

```
public int search(String txt)
{
  int N = txt.length();
  int M = pat.length();
  int skip;
  for (int i = 0; i <= N-M; i += skip)
  {
    skip = 0;
    for (int j = M-1; j >= 0; j--)
      if (pat.charAt(j) != txt.charAt(i+j))
      {
        skip = Math.max(1, j - right[txt.charAt(i+j)]);
        break;
      }
  }
  if (skip == 0) return i;  // match
  return N;
}
```

Boyer–Moore: analysis

Property. Substring search with the Boyer–Moore mismatched character heuristic takes about $\sim N/M$ character compares to search for a pattern of length $M$ in a text of length $N$. sublinear

Worst-case. Can be as bad as $\sim MN$.

```
i 0 1 2 3 4 5 6 7 8 9
---
skip| B | B | B | B | B | B | B | B | B | B
```

Boyer–Moore variant. Can improve worst case to $\sim 3N$ character compares by adding a KMP-like rule to guard against repetitive patterns.

5.3 Substring Search

- introduction
- brute force
- Knuth–Morris–Pratt
- Boyer–Moore
- Rabin–Karp
Rabin–Karp fingerprint search

Basic idea = modular hashing.
- Compute a hash of pat[0..M-1].
- For each i, compute a hash of txt[i..M+i-1].
- If pattern hash = text substring hash, check for a match.

```
pat.charAt(i)
  i 0 1 2 3 4
    2 6 5 3 5 % 997 = 613

txt.charAt(i)
  i 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
    3 1 4 1 5 9 2 6 5 3 5 8 9 7 9 3
  0 3 1 4 1 5 9 % 997 = 508
  1 4 1 5 9 2 % 997 = 201
  2 4 1 5 9 2 % 997 = 715
  3 1 5 9 2 6 % 997 = 971
  4 5 9 2 6 5 % 997 = 442
  5 9 2 6 5 3 % 997 = 929
  6 return i = 6

```

modular hashing with R = 10 and hash(s) = s (mod 997)

Efficiently computing the hash function

Modular hash function. Using the notation $t_i$ for $\text{txt.charAt}(i)$,
we wish to compute

$$x_i = t_i R^{M-1} + t_{i+1} R^{M-2} + \ldots + t_{i+M-1} R^0 \pmod{Q}$$

Intuition. $M$-digit, base-$R$ integer, modulo $Q$.

Horner’s method. Linear-time method to evaluate degree-$M$ polynomial.

```
// Compute hash for M-digit key
private long hash(String key, int M)
{
  long h = 0;
  for (int j = 0; j < M; ++j)
    h = (h * R + key.charAt(j)) % Q;
  return h;
}
```

$$26535 = 2*10000 + 6*1000 + 5*100 + 3*10 + 5 = ((2*10 + 6) * 10 + 5) * 10 + 3) * 10 + 5$$

Modular arithmetic

Math trick. To keep numbers small, take intermediate results modulo $Q$.

Ex.

$$\begin{align*}
10000 &\equiv (30 + 535) \pmod{997} \\
&= (30 + 535) \pmod{997} \\
&= 1695 \pmod{997} \\
&= 698 \pmod{997}
\end{align*}$$

$$\begin{align*}
(a + b) \pmod{Q} &= ((a \pmod{Q}) + (b \pmod{Q})) \pmod{Q} \\
(a \times b) \pmod{Q} &= ((a \pmod{Q}) \ast (b \pmod{Q})) \pmod{Q}
\end{align*}$$

two useful modular arithmetic identities

Efficiently computing the hash function

Challenge. How to efficiently compute $x_{i+1}$ given that we know $x_i$.

$$x_{i+1} = t_i R^{M-1} + t_{i+1} R^{M-2} + \ldots + t_{i+M-1} R^0$$

Key property. Can update ”rolling” hash function in constant time!

```
private long hash(String key, int M)
{
  long h = 0;
  for (int j = 0; j < M; ++j)
    h = (h * R + key.charAt(j)) % Q;
  return h;
}
```

$$\begin{align*}
\text{current value} &\quad \text{subtract leading digit} \\
\text{new value} &\quad \text{multiply by radix} \\
\text{new value} &\quad \text{add new trailing digit} \\
\end{align*}$$

(Precompute $R^M$)

```java
public long computeHash(String key, int M)
{
  long h = 0;
  for (int j = 0; j < M; ++j)
    h = (h * R + key.charAt(j)) % Q;
  return h;
}
```
Rabin–Karp substring search example

First R entries: Use Horner’s rule.
Remaining entries: Use rolling hash (and % to avoid overflow).

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>% 997 = 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>% 997 = (3*10 + 1) % 997 = 31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>% 997 = (31*10 + 4) % 997 = 314</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>% 997 = (314*10 + 1) % 997 = 150</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>% 997 = (150*10 + 5) % 997 = 508</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>% 997 = ((508 + 3*(997 - 30))*10 + 9) % 997 = 201</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>% 997 = ((201 + 1*(997 - 30))*10 + 2) % 997 = 715</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>% 997 = ((715 + 4*(997 - 30))*10 + 6) % 997 = 971</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>% 997 = ((971 + 1*(997 - 30))*10 + 5) % 997 = 442</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>% 997 = ((442 + 5*(997 - 30))*10 + 3) % 997 = 929</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>return 1-M+1 = 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Rabin–Karp: Java implementation

```java
public class RabinKarp {
    private long patHash; // pattern hash value
    private int M; // pattern length
    private long Q; // modulus
    private int R; // radix
    private long RM1; // R^(M-1) % Q

    public RabinKarp(String pat) {
        M = pat.length();
        R = 256;
        Q = 1000000007;
        RM1 = 1;
        for (int i = 1; i <= M-1; i++)
            RM1 = (R * RM1) % Q;
        patHash = hash(pat, M);
    }

    private long hash(String key, int M) {
        // As before
    }

    public int search(String txt) {
        // See next slide
    }
}
```

Rabin–Karp analysis

**Theory.** If \( Q \) is a sufficiently large random prime (about \( M\ N^2 \)), then the probability of a false collision is about \( 1/N \).

**Practice.** Choose \( Q \) to be a large prime (but not so large to cause overflow). Under reasonable assumptions, probability of a collision is about \( 1/Q \).

**Monte Carlo version.**
- Always runs in linear time.
- Extremely likely to return correct answer (but not always!).

**Las Vegas version.**
- Always returns correct answer.
- Extremely likely to run in linear time (but worst case is \( M\ N \)).

Monte Carlo version. Return match if hash match.

```java
public int search(String txt) {
    int N = txt.length();
    int txtHash = hash(txt, M);
    if (patHash == txtHash) return 0;
    for (int i = M; i < N; i++)
        txtHash = (txtHash + Q - RM1*txt.charAt(i-M) % Q) % Q;
    if (patHash == txtHash) return i - M + 1;
    return N;
}
```

Las Vegas version. Modify code to check for substring match if hash match; continue search if false collision.
Rabin–Karp fingerprint search

Advantages.
- Extends to two-dimensional patterns.
- Extends to finding multiple patterns.

Disadvantages.
- Arithmetic ops slower than char compares.
- Las Vegas version requires backup.
- Poor worst-case guarantee.

Q. How would you extend Rabin–Karp to efficiently search for any one of \( P \) possible patterns in a text of length \( N \)?

Substring search cost summary

Cost of searching for an \( M \)-character pattern in an \( N \)-character text.

<table>
<thead>
<tr>
<th>algorithm</th>
<th>version</th>
<th>operation count</th>
<th>backup in input?</th>
<th>correct?</th>
<th>extra space</th>
</tr>
</thead>
<tbody>
<tr>
<td>brute force</td>
<td></td>
<td>( MN )</td>
<td>yes</td>
<td>yes</td>
<td>1</td>
</tr>
<tr>
<td>Knuth-Morris-Pratt</td>
<td>full DFA (Algorithm 5.6)</td>
<td>( 2N )</td>
<td>no</td>
<td>yes</td>
<td>MR</td>
</tr>
<tr>
<td></td>
<td>mismatch transitions only</td>
<td>( 3N )</td>
<td>no</td>
<td>yes</td>
<td>( M )</td>
</tr>
<tr>
<td>Boyer-Moore</td>
<td>full algorithm</td>
<td>( 3N )</td>
<td>yes</td>
<td>yes</td>
<td>( R )</td>
</tr>
<tr>
<td></td>
<td>mismatched char heuristic only (Algorithm 5.7)</td>
<td>( MN )</td>
<td>yes</td>
<td>yes</td>
<td>( R )</td>
</tr>
<tr>
<td>Rabin-Karp†</td>
<td>Monte Carlo (Algorithm 5.8)</td>
<td>( 7N )†</td>
<td>no</td>
<td>yes</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Las Vegas</td>
<td>( 7N )†</td>
<td>yes</td>
<td>yes</td>
<td>1</td>
</tr>
</tbody>
</table>

† probabilistic guarantee, with uniform hash function