Sarah Ertel
Patrick Greher
Eugen Ljavin

1	2	3	4	Σ
7,5	10	5,5	7,5	30,5

a wirft ein false negative

Übungsblatt Nr. 9

(Abgabetermin 28.06.2018)

Aufgabe 1

a)

Algorithm 1: Checks whether two words are shuffled to a third one or not

```
1  function isShuffled(String w, String u, String v)
2  n ← u.length;
3  m ← v.length;
4  if w.length ≠ n + m then
5  |  return false;
6  end
7  boolean[n][m] match;
8  for i ← 1; i < n; i ← i + 1 do
9  |  match[i][0] ← match[i − 1][0] and w[i − 1] == u[i − 1];
10 |  for j ← 1; j < m; j ← j + 1 do
11 |  |  match[0][j] ← match[0][j − 1] and w[j − 1] == v[j − 1];
12 |  |  match[i][j] ← ((w[i + j − 1] == u[i − 1]) and match[i − 1][j]) or
   |  |    ((w[i + j − 1] == v[j − 1]) and match[i][j − 1]);
13 |  end
14 end
15 return match[n − 1][m − 1];
```

match[0][0] muss true sein

b)

Sei n die Länge des Wortes u und m die Länge des Wortes v.
Es wird in zwei verschachtelten Schleifen über n und m iteriert. Die Laufzeit ist folglich $\mathcal{O}(n\ m)$.

korrekt

Aufgabe 3

a)

Die Hashfunktion muss zu einem Wort u und einenem Anagramm v von u denselben Hashwert zurodnen können.
Zu einem Wort w, das kein Anagramm von u ist, muss die Hashfunktion einen anderen Hashwert zurückliefern.

Zu einem oder zu allen?

b)

Die Addition ist kommutativ.
Zwei Permutationen ergeben somit stets dieselbe Summe, unabhängig der Reihenfolge, in

der die Elemente der Permutation addiert werden.
Zwei Anagramme werden somit aufgrund der Kommutativität der Addition, auf der die Hashfunktion h basiert, stets auf denselben Hashwert abgebildet.

korrekt

c)

Die Hashfunktion h bildet alle Wörter, deren Buchstaben dieselbe Summe ergeben, auf denselben Hashwert ab. Da somit Wörter, die keine Anagramme sind, auf denselben Hashwert abgebildet werden (nicht kollisionsresistent) können, lassen sich Anagramme nicht zuverlässig erkennen.

korrekt

d)

$$h(w_1...w_n) = \prod_{i=1}^{n} \texttt{getBytes}(w_i) \bmod \sum_{i=1}^{n} \texttt{getBytes}(w_i) + n$$

Die Wahrscheinlichkeit ist sehr gering, dass sowohl die Summe als auch das Produkt von zwei unterschiedlichen Wörtern gleich ist. Ist also die Summe zweier Wörter gleich, wird sich das Produkt höchstwahrscheinlich unterscheiden wodurch das Gesamtergebnis unterschiedlich ist. Dennoch besteht weiterhin die Möglichkeit, dass zwei Wörter, die keine Anagramme sind, auf denselben Hashwert abgebildet werden. Durch das konkatenieren der Länge des Wortes (+ steht für den Konkatenationsoperator) wird des Weiteren die Eigenschaft von Anagrammen berücksichtigt, dass ein Anagramm v eines Wortes v dieselbe Länge hat. a=1, b=2, c=4, bbcaa = 16 mod 10 + 5 = 11, bbca = 16 mod 9 + 4 = 11

Zwei Anagramme werden weiterhin auf denselben Hashwert abgebildet, da auch das Produkt kommutativ ist. Das stimmt.

Aufgabe 4

a)

i)

$a = 2$
$b = 2$
$m = 2$ korrekt

ii)

$a = 1$
$b = 1$
$m = 118$ korrekt

b)

i)

S	Hashwert
13, 78	3
45	0
64	4
116	1

korrekt

ii)

S	Hashwert
13	3 ($i = 0$)
45	0 ($i = 0$)
64	4 ($i = 0$)
78	2 ($i = 4$)
116	1 ($i = 0$)

korrekt

c)

78 ist ein Vielfaches von 13, denn $78 = 6 \cdot 13$. Da $78 = 3 \mod 5$ und $6 \cdot 13 \mod 5 = 1 \cdot 3 \mod 5 = 3 \mod 5$, gilt stets $a \cdot 78 + b \mod m = a \cdot 13 + b \mod m$ für alle a, b.

Notation beachten, sonst korrekt

d)

Gesucht ist ein m, das bezüglich der Modulo Operation mind. 5 unterschiedliche Ergebnisse liefern kann. Dies ist mit 0, 1, 2, 3, 4 sowie mit 5 (siehe vorherige Aufgabe) nicht möglich. Somit ist 6 das kleinstmögliche m mit $a = 1$ und $b = 0$.

korrekt