

Aufgabe 9: Aufwand für banale und schnelle Exponentiation im Vergleich

Betrachten Sie in dieser Aufgabe die Exponentiation im Bereich der natürlichen Zahlen (die Argumente übertragen sich auf andere Halbgruppen, aber das ist weniger relevant).

Für $a \in \mathbb{N}$ bezeichne $\|a\|$ die “Grösse” von a , also $\|a\| = \log |a| =$ die Anzahl der Ziffern in der Binärdarstellung von a . Sie wissen (oder überzeugen sich davon),

- dass sich die Grösse bei der Multiplikation additiv verhält, d.h. $\|a * b\| = \|a\| + \|b\|$ (also insbesondere gilt bei Exponentiation: $\|a^k\| = k \cdot \|a\|$);
- dass Aufwand für eine Multiplikation $(a, b) \mapsto a * b$ multiplikativ von den Grössen der Operanden abhängt, d.h. wie $c \cdot \|a\| \cdot \|b\|$ mit einer Konstanten c . Das gilt jedenfalls für die “Schulmethode”. Der Einfachheit halber können Sie $c = 1$ annehmen.

Sei nun $a \in \mathbb{N}$ und $N = 2^n - 1$. Betrachten Sie die Aufgabe, die Zahl $a^N = a^{2^n - 1}$ zu berechnen. Man kann das entweder mit der “banalen” oder mit der “schnellen” Methode machen:

```
a)  x ← a
    for i from 1 to N - 1 do
      x ← x * a
    end for
    Return(x)

b)  x ← a, y ← a
    for i from 1 to n - 1 do
      y ← y * y
      x ← x * y
    end for
    Return(x)
```

Beachten Sie: die Anzahl der Schleifendurchläufe bei Algorithmus a) ist exponentiell grösser als die bei Algorithmus b). Entsprechend ist die Anzahl der Multiplikationen bei Algorithmus a) gleich $N - 1$ und bei Algorithmus b) gleich $2(n - 1)$, ebenfalls ein exponentieller Sprung.

1. Zeigen Sie, dass der Algorithmus b) korrekt ist!
2. Bestimmen Sie nun den Aufwand der beiden Verfahren, indem Sie feststellen, welche Operanden in den jeweiligen Schleifendurchläufen miteinander multipliziert werden, wie gross sie sind und was die Multiplikation in Abhängigkeit von ihrer Grösse demnach kostet.
Hinweis: Sie sollten herausfinden, dass die Kosten in beiden Fällen $\mathcal{O}(N^2)$ betragen!