### DHBW MANNHHEIM

### 2. Semester Cyber Security

# Algorithmen und Komplexität

 $N.W. \ \mathcal{E} \ J.T$ 

#### Eigenschaften der Groß-O-Notation

- 1. Geben Sie die Definition der  $\mathcal{O}$ -Notation an.
- 2. Es sei  $f \in \mathcal{O}(h_1)$  und  $g \in \mathcal{O}(h_2)$ . Zeigen Sie, dass  $f \cdot g \in \mathcal{O}(h_1 \cdot h_2)$  gilt.
- 3. Beweisen Sie, dass für alle  $f: \mathbb{N} \to \mathbb{R}_+$  gilt, dass  $f \in \mathcal{O}(f)$ .
- 4. Beweisen Sie, dass für  $f, g : \mathbb{N} \to \mathbb{R}_+$  und  $d \in \mathbb{R}_+$  gilt, dass  $g \in \mathcal{O}(f) \to d \cdot g \in \mathcal{O}(f)$ .
- 5. Beweisen Sie, dass für  $f, g, h : \mathbb{N} \to \mathbb{R}_+$  gilt, dass  $f \in \mathcal{O}(h) \land g \in \mathcal{O}(h) \to f + g \in \mathcal{O}(h)$ .
- 6. Beweisen Sie, dass für  $f, g, h : \mathbb{N} \to \mathbb{R}_+$  gilt, dass  $f \in \mathcal{O}(g) \land g \in \mathcal{O}(h) \to f \in \mathcal{O}(h)$ .
- 7. Angenommen  $f, g, h: \mathbb{N} \to \mathbb{R}_+$ . Außerdem wird angenommen, dass der Grenzwert von

$$\lim_{n\to\infty}\frac{f(n)}{g(n)}$$

existiert. Beweisen sie, dass dann auch  $f \in \mathcal{O}(g)$  gilt.

8. Es seien  $f, g \in \mathbb{R}_+$ . Geben Sie die Definition  $f \sim g$  an.

1) O(9) = { } \ R\_+^n | \ \frac{1}{4} \ \in \ \mathread \mathread

2) Je O(h,) , ge O(h2) J.g e O(h1.h2)

h, ha ∈ N C, ca ∈ R+ ne N

 $\forall n \in \mathbb{N}: (n \ge k_n -> \int (n) \le c_n \cdot h_n(n))$  $\forall n \in \mathbb{N}: (n \ge k_n -> g(n) \le c_n \cdot h_n(n))$ 

ل:= max (لر, لر) := در. در

 $\int (n) \cdot g(n) \leq c_{\lambda} \cdot h_{\lambda} \cdot (n) \cdot c_{\lambda} \cdot h_{\lambda} \cdot (n)$ 

(n) - q(n) = C, C2 · h, (n) · h2 (n)

∠ ) /(n) · q(n) ← C · h, (n) · h, (n)

 $\Rightarrow \int g \in O(h_1 \cdot h_2)$ 

3) J E O(1)

Definiere l=0 C=1

4n∈ (N: ()(n) = c.)(n))

4) 9 € O() -> d. 9 € O()

l'∈ IN c'∈ R

∀n ∈ W: (n ≥ l' → q(n) ≤ c'. ∫(n)) Ungleichung Id

Yne IN: (n ≥ h' -> d. g(n) ∈ c'·d. f(n))

h:= h' c := d.c'

Vn ∈ IN: (n ≥ 1 -> d. g(n) € c. f(n))

=> d.a (0(1)

P

5)  $\int \in O(h) \quad \Lambda \quad g \in O(h) \quad -> \int f + g \in O(h)$ 

h, ha Ell c, ca ER+

 $\forall n \in \mathbb{N} : (n \ge k_1 \longrightarrow \int_{\mathbb{N}} (n) \le c_1 \cdot h(n))$  $\forall n \in \mathbb{N} : (n \ge k_2 \longrightarrow g(n) \le c_2 \cdot h(n))$ 

L:= max(u1, u2) (:= (1+c2

 $\int(n) + g(n) \leq c_{\lambda} \cdot h(n) + c_{\lambda} \cdot h(n)$ 

J(n) + g(n) & ((1 + c2) · h(n)

f(n) + g(n) ≤ c · h(n)

=> 1 + 9 & O(h)

6) 
$$\int e O(g) \wedge g e O(h) -> \int e O(h)$$
  
 $|u_1|u_2 \in |u| \quad c_1, c_2 \in |R_+|$ 

$$\forall_n \in (\mathbb{N} : (n \ge k_1 -> )(n) \le c_1 \cdot g(n))$$
  
 $\forall_n \in \mathbb{N} : (n \ge k_2 -> g(n) \le c_2 \cdot h(n))$ 

$$\frac{\int_{0}^{\infty} (x)}{g(x)} = \Lambda \quad \text{isd} \quad \Box$$

#### Groß-O-Notation

- 1. Zeigen Sie, dass  $n^2 \in \mathcal{O}(2^n)$  ist.
- 2. Zeigen Sie auch, dass  $n^3\mathcal{O}(2^n)$  gilt.
- 3. Zeigen Sie:  $\log_2(n) \in \mathcal{O}(\ln(n+1))$
- 4. Zeigen Sie, dass  $\ln^2(n) \in \mathcal{O}(\sqrt{n})$  gilt.
- 5. Versuchen Sie zu zeigen, dass  $n^{\alpha} \in \mathcal{O}(2^n)$ , wenn angenommen werden kann, dass  $\alpha \in \mathbb{N}$  vorausgesetzt ist.

Adjabe Ur. 2

$$n^2 \in O(2)$$

Cim 
$$\frac{2}{n\rightarrow\infty}$$
 = 0 Siehe S. 15 im Skript für elen geneuen Rewers.

a) 
$$n^3 \in O(2^n)$$

$$\frac{n^3}{2^n}$$
  $\frac{CH}{Ch(2)\cdot 2^n}$   $\frac{CH}{Ch(2)^3\cdot 2^n}$   $\frac{CH}{Ch(2)^3\cdot 2^n}$   $\frac{CH}{Ch(2)^3\cdot 2^n}$ 

$$\lim_{n\to\infty} \frac{6}{(n\alpha)^3} \cdot 2^n = 0$$

$$(n (n) = \frac{(og_2 (n))}{(og_2 (e))}$$
  $\longrightarrow (og_2 (e)) \cdot (n(n)) = (og_2 (n))$ 

$$\frac{(n(n))}{(n(n+1))} => z.z. \quad (n(n)) \in O((n(n+1))$$

$$\lim_{n\to\infty}\frac{\ln(n)}{\ln(n+n)}=1$$

4) 
$$(n^2(n) \in O(\sqrt{n})$$

$$\frac{(n^{2}(n))}{\sqrt{n^{2}}} = \frac{2 \cdot (n(n))}{\sqrt{n}} = \frac{2 \cdot (n(n) \cdot 2 \cdot \sqrt{n^{2}})}{\sqrt{n}} = \frac{2 \cdot (n(n) \cdot 2 \cdot \sqrt{n})}{\sqrt{n}} = \frac{2 \cdot (n(n) \cdot 2 \cdot \sqrt{n})}{\sqrt{n}} = \frac{2 \cdot (n(n) \cdot 2 \cdot \sqrt{n})}{\sqrt{n}} = \frac{2 \cdot (n(n$$

$$= 4 \cdot (n(n) \cdot \frac{\sqrt{n}}{n})$$

$$= 4 \cdot (n(n) \cdot \frac{1}{\sqrt{n}})$$

5) 
$$\alpha \in \Omega$$
 $\alpha \in \Omega$ 
 $\beta(n) = n^{\alpha}$ 
 $\beta(n) = \alpha \cdot \alpha \cdot 1$ 
 $\beta(n) = \alpha \cdot (\alpha - 1) \cdot n^{\alpha - 2}$ 
 $\beta(n) = \alpha \cdot (\alpha - 1) \cdot n^{\alpha - 2}$ 
 $\beta(n) = \alpha \cdot (\alpha - 1) \cdot n^{\alpha - 2}$ 

#### Rekurrenzgleichungen

Lösen Sie folgende Rekurrenzgleichungen:

- 1.  $x_{n+2} = x_{n+1} + x_n$  für welche gilt:  $x_0 = 0$  und  $x_1 = 1$
- 2.  $x_{n+2} = 4 \cdot x_{n+1} 4 \cdot x_n + 1$  für welche gilt:  $x_0 = 1$  und  $x_1 = 3$
- 3.  $a_{n+2} = \frac{1}{6} \cdot a_{n+1} + \frac{1}{6} \cdot a_n$  für welche gilt:  $a_0 = 0$  und  $a_1 = \frac{5}{6}$
- 4.  $a_{n+2} = -\frac{1}{2} \cdot a_{n+1} + \frac{1}{2} \cdot a_n$  für welche gilt:  $a_0 = 2$  und  $a_1 = 1$
- 5.  $a_{n+2}=a_{n+1}+2\cdot a_n+1$  für welche gilt:  $a_0=0$  und  $a_1=-\frac{1}{2}$
- 6.  $a_{n+2}=a_n+2$  für welche gilt:  $a_0=2$  und  $a_1=1$
- 7.  $a_{n+2} = 2 \cdot a_n a_{n+1}$  für welche gilt:  $a_0 = 0$  und  $a_0 = 3$
- 8.  $a_{n+2} = 7 \cdot a_{n+1} 10 \cdot a_n$  für welche gilt:  $a_0 = 0$  und  $a_0 = 3$
- 9.  $a_{n+1} = 2^n \cdot a_n$  für welche gilt:  $a_1 = 1$
- 10. Stellen Sie mit dem Ansatz  $a_k := f(2^k)$  eine Rekurrenzgleichung auf und lösen Sie diese.

$$f(n) = 2 \cdot f(n \setminus 2) + \log_2(n)$$

Es gelten folgende Anfangsbedingungen:  $x_0 = 0$  und  $x_1 = 1$ 

Homogener Teil

$$X_n = \chi^n$$

$$\lambda_{v_{49}} = \lambda_{v_{40}} + \lambda_{v_{10}} | : \gamma_{v_{10}}$$

$$y_s = y + \sqrt{1 - \gamma_s (-(\sqrt{3}))}$$

$$\lambda_{1/2} = \frac{1}{2} \pm \sqrt{\frac{1}{2}^2 + 1}$$

$$= \frac{1}{2} \pm \frac{\sqrt{5}}{2}$$

$$\lambda_1 = \frac{1 + \sqrt{5}}{2} \qquad \lambda_2 = \frac{1 - \sqrt{5}}{2}$$

$$\chi_n = 0. \left(\frac{1+\sqrt{5}}{2}\right)^n + 0. \left(\frac{1+\sqrt{5}}{2}\right)^n$$

Inhomogener Teil liegt nicht vor -> wird cusse cossen

# LGS llit den Anfangsbædingungen

$$X_0 = O = A + B$$

$$x_1 = 1 = 0 \cdot \frac{1 + \sqrt{5}}{2} + 3 \cdot \frac{1 - \sqrt{5}}{2}$$

$$1 = -\beta \cdot \frac{1+15}{2} + \beta \cdot \frac{1-15}{2}$$

$$1 = -\beta \cdot \left(\frac{1}{a} + \frac{\sqrt{s'}}{a}\right) + \beta \cdot \left(\frac{1}{a} - \frac{\sqrt{s'}}{a}\right)$$

$$1 = -\frac{1}{2} \left( 5 - \frac{\sqrt{5}}{2} \right) + \frac{1}{2} \left( 5 - \frac{\sqrt{5}}{2} \right)$$

$$\frac{1}{2} = -\frac{\sqrt{5}}{2} \cdot \beta \quad | : \left( -\frac{\sqrt{5}}{2} \right)$$

$$\frac{1/2}{-1/5} = \frac{1}{5} = \frac{1}{1/5} = \frac{1}{5}$$

$$\frac{1}{15} = 0$$

$$X_n = \frac{1}{15} \cdot \frac{1+N_5}{2} - \frac{1}{N_5} \cdot \frac{1-N_5}{2}$$

a) Xn+2 = 4. xn+1 - 4. xn +1

Homogener Teic

Xn+2 = 4. xnm - 4. xn

 $X_n = \lambda^n$ 

ντ3 = 4. χ - 4. χ [: χ ]

 $\lambda^2 = 4 \cdot \lambda - 4 \quad |-\lambda^2|(-\lambda)$ 

0 = \2 - 4\1 + 4 |PQ

 $\lambda_{1/2} = 2 \pm \sqrt{4-4}$ 

- 2 ± 0

 $\lambda_1 = 2$   $\lambda_2 = 2$   $\mathcal{L}$   $\lambda_1 = \lambda_2$ 

 $X_n = \alpha \cdot \alpha^n + \beta \cdot \alpha^n \cdot n$ 

Inhomogenen Teil Losen

Xn+2 = 4. xn+1 - 4. xn +1

> = xn

8 = 48 - 48 +1

r - 1

Xn = Q. 2 + B.2.n+1

LGS Mit den Anlengsbedingengen

Xo = 1 = Q +1 1-1

 $X_{1} = 3 = 0.2 + 0.2 + 1$ 

d = 0

3=20+11-11:2

1 = B

 $\times_{n} = 2^n \cdot n + 1$ 

3) 
$$a_{n+2} = \frac{1}{6} \cdot a_{n+1} + \frac{1}{6} \cdot a_n$$

$$\lambda^{n+2} = \frac{1}{6} \cdot \lambda^{n+1} + \frac{1}{6} \cdot \lambda^{n} \left( \frac{1}{2} \lambda^{n} \right) \cdot (-\lambda)$$

$$= \lambda^{2} - \frac{1}{6} \lambda - \frac{1}{6} \qquad |PQ|$$

$$= \frac{1}{12} \pm \sqrt{\frac{25}{144}}$$

$$=\frac{1}{12}\pm\frac{5}{12}$$

$$\lambda_1 = \frac{6}{12} \qquad \lambda_2 = \frac{-4}{12}$$

$$=\frac{1}{2}$$
  $=-\frac{1}{3}$ 

$$Q_n = \chi \cdot \frac{1}{2} + \beta \cdot -\frac{1}{3}$$

$$\alpha_{\lambda} = \frac{5}{6} = \lambda \cdot \frac{1}{3} + \beta \cdot -\frac{1}{3}$$

$$\alpha_{n} = \left(\frac{1}{a}\right)^{n} - 1 \cdot \left(-\frac{1}{3}\right)^{n}$$

#### Master Theorem

- 1. Geben Sie die Definition des Master-Theorems an.
- 2. Schätzen Sie mit Hilfe des Master-Theorems die Komplexität von f<br/> ab.  $f(n) = 2 \cdot f(n \backslash 2) + n$
- 3. Schätzen Sie  $g(n) = 4 \cdot g(n \setminus 3) + (\frac{2}{3})^2 \cdot n$  mit Hilfe des Master-Theorems ab.
- 4. Schätzen Sie  $g(n) = 4 \cdot g(n \setminus 5) + (\frac{3}{2})^3 \cdot n^2$  mit Hilfe des Master-Theorems ab.
- 5. Schätzen Sie  $g(n) = 4 \cdot g(n \setminus 3) + 2 \cdot n^{\log_3(4)} + n$  mit Hilfe des Master-Theorems ab.

Adjable 19r. 4

1) Maski - Theorem

 $O_{+}B \in IN$ ,  $S \in R_{+}$ 

f: IN -> IR+ and & had alse Form:

$$\int (n) = Q \cdot \int (n / \beta) \cdot O(n^{\delta})$$

3 Falle

1. 
$$\alpha < \beta^{\delta} \rightarrow \beta \in O(n^{\delta})$$

2. 
$$\alpha = \beta^{8} - > \lambda \in O((\log_{\beta}(n) \cdot n^{6}))$$

3. 
$$\alpha > \beta_{\epsilon} \rightarrow \beta \in O(\nu_{\alpha\beta} k_{\alpha})$$

a) 
$$g(n) = 4 \cdot g(n/3) + (\frac{2}{3})^2 \cdot n$$
  
 $d = 4 \cdot \beta = 3 \cdot \delta = 1$ 

3) 
$$g(n) = 4 \cdot g(n//5) + (\frac{3}{2})^3 \cdot n^2$$

$$\int e O(n^2)$$

4) 
$$q(n) = 4 \cdot q(n/3) + 2 \cdot n^{(093)(4)} + n$$

- 1. Geben Sie die Gleichung an, mit der wir Merge Sort definiert haben. Alternativ ist auch der Pythoncode von Merge Sort akzeptabel.
- 2. Wir haben die Funktion, die für zwei sortierte Listen  $L_1, L_2$  berechnet, wie viele Vergleichsoperationen beim Aufruf von  $merge(L_1, L_2)$  geschehen, mit cmpCount bezeichnet. geben Sie die Ungleichung an, die wir für das Verhältnis zwischen  $\#L_1, \#L_2$  und  $cmpCount(L_1, L_2)$  aufgestellt haben.
- 3. Schätzen Sie mit Hilfe des Master-Theorems die Komplexität von MergeSort ab.

## a) Formale Definition:

n:= (en(L) 112 -> Sort(L) = L  $n > 2 \rightarrow \text{merge} \left( \text{Sort} \left( \angle \left[ : n / / 2 \right] \right), \text{Sort} \left( \angle \left[ : n / / 2 \cdot 1 \right] \right) \right)$ merge (L1, [3) = C1 merge ([], La) = G C+ E3 1 C2 + E3: 1. X1 < X2 -> merge ([X1|R1], [X2|R]) = [X1] + merge (R1, [10|R]) 2.  $\times_1 > \times_2 \rightarrow$  merge ( $[\times_1 | R_1], [\times_2 | R_2]) = [\times_2] +$  merge ( $[\omega | R_2], R_2)$ 

- 6) cmpCount((,, (2) & #4, + #62
- c)  $2 \cdot \int (n/2) \cdot O(n) = \int (n)$ d=2, B=2 S=1 2 = 2 -> 2. Fac  $f(n) \in O((\log_2(n) \cdot n))$

### Code:

del 80++(C) n = len(l)if n<a: redurn L return merge (SOrt(L[:n//2]), sort(L[n//2:1))

del merge (L, La):

if 4 = []: redurn La return La X1, R1 = 4, [0], 4, [1.3 x2, R2 = L2 COJ, C2[1:] if  $x_1 \leq x_2$ : return [x1] + merge (R1, La)

redurn [x3] + mage (c, R2)

#### ${\bf Sortier problem}$

- 1. Definieren Sie:
  - (a) Partielle Ordnung
  - (b) Lineare Ordnung
  - (c) Quasiordnung
  - (d) Totale-Quasiordnung
- 2. Geben Sie die Definition des Sortierproblems an.

# Sortierproblem

## Partielle Ordnung

- 1. Vx e S: x = x (Relaxiv)
- 2.  $\forall x,y \in S : (X \leq \gamma \wedge \gamma \leq x \rightarrow x = y)$  (anti-Stimmetrie)
- 3. Vx, y, z ES: (X = Y A Y = Z -> X = Z) ( transitio)

### Cineare Ordnung

- 1. Partiell geordnet
- 2. Vx,y es: ("x=y v y=x) (Cireor)

# Quasi Ordneurg

- 1.  $\forall x \in S : x \in x$  (legleriv) 2.  $\forall x, y, z \in S : (x \leq y \ x \ y \leq z \ -> x \leq z)$  (transitiv)

# Totale Quesiordneury

- 1. Owasiondness
- ((ivea.) 2. Vx, y ES: (xey v yex)

# Sortier problem

gegeben sei < U, <> in totales aussiordnung.

Cish Cisk aust

gesucht ist S mit Jolganden Bedingugen

1. H; ∈ {0, ..., (en(s)-2}: S[i] & S[i]+1

2.  $\forall x \in M : count(x, L) = count(x, S)$ 

#### Sortieralgorithmen

- 1. Insertion Sort
  - (a) Formale Defintion
  - (b) Implementierung
  - (c) Komplexität
- 2. Selection Sort
  - (a) Formale Defintion
  - (b) Implementierung
  - (c) Komplexität
- 3. Merge Sort
  - (a) Formale Defintion
  - (b) Implementierung
  - (c) Komplexität
  - (d) Komplexität im Master-Theorem
- 4. Quicksort
  - (a) Formale Defintion
  - (b) Implementierung
  - (c) Komplexität
- 5. Counting Sort
  - (a) Formale Defintion mit allen Phasen
  - (b) Implementierung
  - (c) Komplexität
- 6. Radix Sort
  - (a) Vorgehensweise
  - (b) Implementierung
- 7. Heapsort
  - (a) Formale Defintion
  - (b) Implementierung
  - (c) Komplexität

algabe Ur. 7 7) Formale Definition Dic to List() = II a) Formale Definition h + Ni( 1 h. fop() = <p, \_> del 50.1(C): -> h. to CisiCI = CpI + h. remover to CisiC) Sort([]) = [] if (== c3. return [] Sort ([x3+R) = insert(x, sord(R)) inserial (x, []) = [x]X, R = CC03, CC1:1 return insert (x, sort(R)) XCY -> insert ([x3,[y]+R) = [xf+Cy]+R del inself ( + ( C): -> insert (X], [Y]+R) = [Y] + insert (x, R) retur [x] Y, R = ([0], L[1:] p84 O(u)if x = y: return [x] + [x]+ R return [y] + insert(x,R) average { ·n2+O(n) Formale Definition Code Sout([]) - [] del Sort(L): X := min (L) if L=- []: return [] -> Sord(() = [X] + Sort(delek(x, ()) delek (x, []) = [] X = min(L) redem [2] + delek(x, L) delak (x, [x]+R) = R def deak(x, L): -> de(ek (x, [y]+R) = de(ek(x, R) retem [] 1/ x== LOJ: 4·n2 +0(1) retim ([1:] immer return [LCO] + delek (x, LT1:3) Formace Definition: Coole: del n: (en(L) SOL4 (C):  $n < 2 \rightarrow Sort(C) = C$ n = len(L): n ≥ 2 -> sort(1) = merge (Sort(L[:n112], L[n112:]) il n < 2: Rtum L merge ( G, []) = G redun merge (Sort (L C: n(123), Sort (Cn(12:3)) merge ([], (2) = (2 Ly + [] 1 La + [] 1 x 1 4 x Old nerge ((1, (2): > merge ( [x, 1R, ], [x2 | R2]) = [x, ] + merge (R, , [x2, R2]) LiteIn LateIn x >x2 1 4 == []: return La -> merge ([x, [R,], [x, [Ro]) - [x,] + merge ([x, [A,] | Re) il ( == []: return G O((og 2 (N-n) x, R, = LEOS, LEX:3 x2, R2 = C[03, C[1:] if x1 <= x2: redurn [23+ merge (Ru, Ca) is x, xxa: return [x2] + merge (L, R2) Formace Definition Code Sort([])=[] del sort(1)

if (== F]:

return L XR= L[O], L[x:]

S= [y for y in R if y = x] B= [y for y in R if y = x]

return Sort(S) + [x3 + sort(8)

Sort (KZ+P) = Sort ( [Y & P | Y C x ] + [ ] + Sort ( [Y & R | Y > x ] )

worsh case: O(n2)

average : O(n. (oga (n))

#### ADTs + Set und Maps

- 1. Geben Sie die formale Definition von ADTs an.
- 2. Geben Sie die formale Definition des ADT Stack an.
- 3. Beschreiben Sie was ein Generator in einem
- 4. Beschreiben Sie den Shunting-Yard-Algorithmus.
- 5. Geben Sie die formale Definition des ADT Map an.
- 6. Was haben geordnete Binärbäume, AVL Bäume, Tries und co. miteinander zu tun, was verbindet sie?
- 7. Geben Sie die formale Definition und die Komplexität von geordneten Binärbäumen an.
- 8. Geben Sie die formale Definition und die Komplexität von AVL Bäumen an.
- 9. Geben Sie die formale Definition und die Komplexität von Tries an.
- 10. Beschreiben Sie, was eine Prioritätswarteschlange ist.
- 11. Geben Sie die formale Definition und die Komplexität von Prioritätswarteschlangen an.
- 12. Geben Sie die formale Definition und die Komplexität des Heaps an.