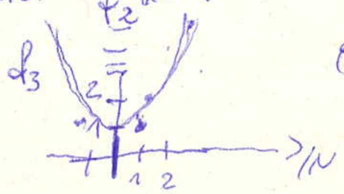
Komplexität

Die Komplexität von einem Verfahren (Algorithmus) wird durch die Landau'sche $\mathcal{O}$-Notation beschrieben:

seien $f, g : \mathbb{N}^k \to \mathbb{R}$ Funktionen. Oft ist $k = 2$,

z.B. $f_1 : \mathbb{N}^2 = \mathbb{N}\times\mathbb{N} \to \mathbb{R}$ $f_1(a,b) = a+b$ oder $f_2 : \mathbb{N}^2 = \mathbb{N}\times\mathbb{N} \to \mathbb{R}$ $f_2(a,b) = a \cdot b$



$k = 1$ $f_3 : \mathbb{N} \to \mathbb{R}$ $n \mapsto n^2 + 1$

$f_4 : \mathbb{N} \to \mathbb{R}$ $n \mapsto c$, $c \in \mathbb{R}$

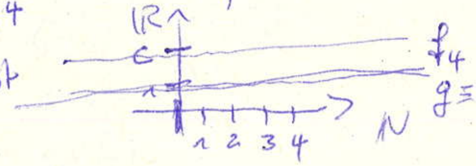
Es ist $f \in \mathcal{O}(g)$ (Schreibweise auch $f = \mathcal{O}(g)$, sprich f ist $\mathcal{O}(g)$),

falls es $n_0 \in \mathbb{N}$ und $c \in \mathbb{R}_{>0}$ gibt so, dass

für alle $n_1, \dots, n_k$ mit $n_i \geq n_0$ $(1 \leq i \leq k)$ $f(n_1, \dots, n_k) \leq c\, g(n_1, \dots, n_k)$.

Bsp: (1) $f_4 \in \mathcal{O}(1)$, wobei 1 die Funktion $g : \mathbb{N} \to \mathbb{R}$, $a \mapsto 1$ $(g \equiv 1)$

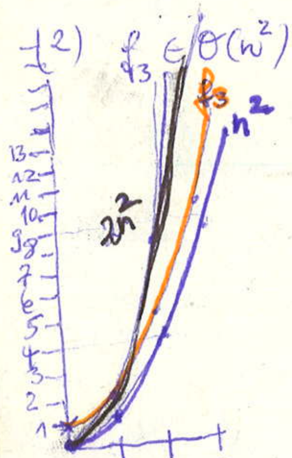
ist



$\Rightarrow$ Setze $n_0 = 0$. Dann ist $f_4(n_1) \leq c\,1$

für alle $n_1 \geq n_0$. (es gilt sogar Gleichheit).

(2) $f_3 \in \mathcal{O}(n^2)$, wobei n^2 für die Fkt. $g : \mathbb{N} \to \mathbb{R}$ $n \mapsto n^2$ steht.



Es ist $n_0 = 1$ und $c = 2$: für $n_1 \geq 1$ gilt $f_3(n_1) = n_1^2 + 1$
$\leq 2 n_1^2$

Also $f \in \mathcal{O}(g)$ bedeutet: für groß genuge n_i, genauer für $n_i \geq n_0$ $(1 \leq i \leq 2)$ ist f kleiner gleich dem c-Vielfachen von g für eine positive Konstante $c \in \mathbb{R}$.

~~Wir wollen~~ Weitere Bsp.:

- ges $r \in \mathbb{N}$ $f : \mathbb{N} \to \mathbb{R}$ $a \mapsto \log_r a$ $\Rightarrow f \in \mathcal{O}(\log a)$, wobei $\log a$ der Logarithmus zur Basis 10 ist: Es ist $\log_r a = \frac{\log a}{\log r} = \frac{1}{\log r} \cdot \log a$

und $c := \frac{1}{\log r} \in \mathbb{R}_{>0}$

K2

- $f: \mathbb{N} \to \mathbb{R}$ $n \mapsto$ # Bits der Binärdarstellung von n

  ~~$f(n)$~~ $f \in \mathcal{O}(\log n)$

  Es ist $f(n) = \lfloor \log_2 n \rfloor + 1$ und daher $f \in \mathcal{O}(\log n)$

- ~~f~~ Seien $a, b \in \mathbb{N}$ in Binärdarstellung gegeben. Die Länge von a sei m und die von b n.

  Sei $f: \mathbb{N}^2 \to \mathbb{R}$ f: Laufzeit der Berechnung von $f(a,b) \mapsto a+b$. $\Rightarrow f \in \mathcal{O}(\max\{n,m\})$

  $= \mathcal{O}(\max\{\log a, \log b\})$. Dabei nehmen wir an, dass das Addieren von zwei ~~Zahlen~~ Bits $\mathcal{O}(1)$ kostet, das Lesen/Schreiben einer Zahl gar nichts.

  Bsp: $a = 10101$, $b = 111$

$$\begin{array}{r} 10101 \\ 111 \\ \hline \end{array}$$

Sei oBdA $a \geq b$. Dann führen wir max. $\ell(a) + 1 = m+1$ - viele Additionen durch. Also ist die Laufzeit höchstens $(m+1)\,\mathcal{O}(1)$, d.h. $f(a,b) \leq (m+1)\,c \cdot 1 = c \cdot (m+1) \leq 2c \cdot m$

Also $f \in \mathcal{O}(\max\{n,m\})$.

Perfekte Sicherheit

Sei $S \neq \emptyset$ eine Menge. Ele in S sind die Elementarereignisse, die Teilmengen von S die Ereignisse. Sei Pr eine Wahrscheinlichkeitsverteilung auf S ($Pr: \mathcal{P}(S) \to \mathbb{R}$ (1.) $Pr(A) \geq 0$ $A \in S$, (2.) $Pr(S) = 1$ (3.) $Pr(A \cup B) = Pr(A) + Pr(B)$ für $A \cap B = \emptyset$

Bedingte Wahrscheinlichkeit: $Pr(A|B) = \frac{Pr(A \cap B)}{Pr(B)}$ (Wahrscheinlichkeit, dass A eintritt, falls B bereits eingetreten ist [$Pr(B|B) = 1$]

A und B unabhängig, falls $Pr(A \cap B) = Pr(A)\,Pr(B)$ ($\Leftrightarrow Pr(A|B) = Pr(A)$)

A tritt also mit derselben Wahrscheinlichkeit ein, ob B gilt oder auch nicht.

Sei $\mathbb{K} = (\mathcal{P}, \mathcal{C}, \mathcal{K}, e_k, d_k)$ ein Kryptosystem.

Es sei $Pr_{\mathcal{P}}$, $Pr_{\mathcal{K}}$ ~~eine~~ W-Verteilungen auf $\mathcal{P}$ bzw. $\mathcal{K}$. Wir erhalten W-Verteilung auf $\mathcal{P} \times \mathcal{K}$: $Pr(p, k) := Pr_{\mathcal{P}}(p)\,Pr_{\mathcal{K}}(k)$

Identifiziere p mit $\{(p, k) \mid k \in \mathcal{K}\}$ und k mit $\{(p, k) \mid p \in \mathcal{P}\}$.

Dann gilt $Pr(p) = Pr_{\mathcal{P}}(p)$ und $Pr(k) = Pr_{\mathcal{K}}(k)$

Für $c \in \mathcal{C}$ identifiziere c mit dem Ereignis: $\{(p, k) \mid p \in \mathcal{P}, k \in \mathcal{K}, e_k(p) = c\}$

Dadurch haben wir den Chiffren auch eine Wahrscheinlichkeit zugeordnet.

$\mathbb{K}$ heißt perfekt sicher, falls für alle $p \in \mathcal{P}$ und $c \in \mathcal{C}$ die Ereignisse p und c unabhängig voneinander sind, d.h. falls $Pr(p|c) = Pr(p)$, d.h. falls c von Eve abgefangen wird, sie keinerlei Rückschlüsse auf p machen kann.

Falls $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}| < \infty$, dann gibt der Satz von Shannon Auskunft über die perfekte Sicherheit.

Satz (Shannon): Sei $|\mathcal{C}| = |\mathcal{K}| = |\mathcal{P}| < \infty$ und sei $Pr(x) > 0$ für jedes $x \in \mathcal{P}$. $\mathbb{K}$ ist genau dann perfekt sicher, falls die Wahrscheinlichkeitsverteilung auf $\mathcal{K}$ die Gleichverteilung ist und falls es zu jedem $x \in \mathcal{P}$ und jedem $y \in \mathcal{C}$ genau ein $k \in \mathcal{K}$ mit $e_k(x) = y$ gibt.

Das One-Time-Pad (Einmal-Block) (Vernam-Chiffre 1917)

$\mathcal{P} = \mathcal{K} = \mathcal{C} = K^n$, $K = \mathbb{Z}_2$ (also $\mathcal{P}$ besteht aus n-Tupeln von 0'en und 1'en.

Wir haben eine Verknüpfung auf $\mathbb{Z}_2^n$: $(a_1,\dots,a_n) \oplus (b_1,\dots,b_n) := (a_1+b_1,\dots,a_n+b_n)$, wobei $a_1,\dots,a_n,b_1,\dots,b_n \in \mathbb{Z}_2$ und a_i+b_i in $\mathbb{Z}_2$ gerechnet wird $(1 \le i \le n)$

Die Verschlüsselung ist $e_k(p) = p \oplus k$, wobei $p = (p_1,\dots,p_n)$ und $k = (k_1,\dots,k_n)$

Das One-Time-Pad ist g.d. perfekt sicher, wenn die Schlüssel $k \in \mathcal{K}$ gleichverteilt gewählt werden.

Ein anderes Bsp eines perfekt sicheren Kryptosystems:

$\mathcal{P} = \{0,1\}$, $\mathcal{K} = \{u,v,w,z\}$, $\mathcal{C} = \{U,V,W,Z\}$

$e_k(x)$, $k \rightarrow$ / $x \downarrow$	u	v	w	z
0	U	V	W	Z
1	V	U	Z	W

$Pr_{\mathcal{P}}(0) = \alpha$, $Pr_{\mathcal{P}}(1) = \beta$, $\alpha + \beta = 1$

$Pr_{\mathcal{K}}(u) = Pr_{\mathcal{K}}(v) = \sigma$, $Pr_{\mathcal{K}}(w) = Pr_{\mathcal{K}}(z) = \tau$, $\sigma + \tau = 1/2$

Beh. K ist mit dieser W-Verteilung perfekt sicher.

Dazu müssen wir für alle $p \in \mathcal{P}$ und $c \in \mathcal{C}$ $Pr_{\mathcal{P}\times\mathcal{K}}(p|c) = Pr_{\mathcal{P}\times\mathcal{K}}(p)$ zeigen.

Bsp. $c = U$, $p = 0$ $\quad Pr_{\mathcal{P}\times\mathcal{K}}(p|c) = \dfrac{Pr_{\mathcal{P}\times\mathcal{K}}(p \cap U)}{Pr_{\mathcal{P}\times\mathcal{K}}(U)} = \dfrac{Pr_{\mathcal{P}\times\mathcal{K}}((0,u))}{\sigma} = \dfrac{\alpha \cdot \sigma}{\sigma}$

$= \alpha = Pr_{\mathcal{P}}(p)$

$Pr_{\mathcal{P}\times\mathcal{K}}(U) = Pr_{\mathcal{P}\times\mathcal{K}}(\{(0,u),(1,v)\})$

$= Pr_{\mathcal{P}}(0) Pr_{\mathcal{K}}(u) + Pr_{\mathcal{P}}(1) Pr_{\mathcal{K}}(v)$

$= \alpha\sigma + \beta\sigma = (\alpha+\beta)\sigma = \sigma$

ZP: abends → 28