Errata, Corrigenda et Addenda
Grundlegende Algorithmen

Volker Heun

Vieweg-Verlag, ISBN 3-528-03140-9

Stand: 19. Dezember 2002

Seite 9, Zeile 2 *(Korrektur):*
Ersetze: iterativ, rekursiv [im Bild 1.4]
durch: rekursiv, iterativ
[J. Gruber; 2001-12-19]

Seite 57, Zeile −13, −4 *(Korrektur):*
Ersetze: $V_{\text{Quick}}(1) = 0$
durch: $V_{\text{Quick}}(n) = 0$ für $n \in [0:1]$
[T. Bayer; 2002-12-10]

Seite 58, Zeile −16 *(Korrektur):*
Ersetze: $V_{\text{Quick}}(n) = 1$
durch: $V_{\text{Quick}}(n) = 0$ für $n \in [0:1]$
[T. Bayer; 2002-12-10]

Seite 85, Zeile 3 *(Korrektur):*
Ersetze: $\bar{V}_{\text{QSel}}(1) = 0$
durch: $\bar{V}_{\text{QSel}}(n) = 0$ für $n \in [0:1]$
[S. Kosub; 2002-12-06]

Seite 85, Zeile 7 *(Korrektur):*
Ersetze: Für $n = 1$ ist dies offensichtlich richtig und der Induktionsanfang ist damit gelegt. Für $n \geq 2$ gilt:
durch: Nachrechnen zeigt, dass dies für $n \in [0:2]$ richtig ist, und der Induktionsanfang ist damit gelegt. Für $n \geq 3$ gilt:
[S. Kosub; 2002-12-06]

Seite 108, Zeile −10 *(Korrektur):*
Ersetze: $\text{Ws}[k_2 \leq \frac{1}{2}n + 2n^{3/2}]$
durch: $\text{Ws}[k_2 \geq \frac{1}{2}n + 2n^{3/2}]$
[S. Gerke; 2000-12-01]

Seite 214, Zeile 6 *(Ergänzung):*
Für die Berechnung der Einträge der Shift-Tabelle haben wir nur zulässige Shifts verwendet, aber nicht alle. Formal muss auch noch bewiesen, werden, dass keine kürzeren Shifts vorkommen knnen. Die lässt sich jedoch recht einfach mit Hilfe eines Widerspruchsbeweises zeigen.
[V. Heun; 2001-11-2]

Seite 240, Zeile −7 *(Ergänzung):*

Es lässt sich sogar Folgendes beweisen:

Theorem 7.3 *Der Euklidische Algorithmus berechnet den größten gemeinsamen Teiler von zwei ganzen Zahlen a und b mit $O(\log^2(a+b))$ Bit-Operationen.*

[V. Heun; 2001-01-07]

Seite 241, Zeile −6 *(Ergänzung):*

Es lässt sich sogar Folgendes beweisen:

Theorem 7.5 *Der erweiterte Euklidische Algorithmus berechnet für $a, b \in \mathbb{N}_0$ den größten gemeinsamen Teiler und die dazugehörige Linearkombination aus a und b mit logarithmisch vielen arithmetischen Operationen. Die Komplexität in Bit-Operationen beträgt $O((\log(a+b))^2)$.*

[V. Heun; 2001-01-07]

Seite 256, Zeile −10 *(Ergänzung):*

Falls man die Nachricht N lieber aus $\mathbb{Z}_n$ statt $\mathbb{Z}_n^*$ wählen möchte, so kann man dies auch tun. Die Decodierung bleibt korrekt. Man benötigt dann für den Korrektheitsbeweis (d.h., um $(N^k)^{\varphi(n)} = 1$ zu beweisen) den Chinesischen Restsatz. Der kleine Satz von Fermat versagt hierbei für N mit $\mathrm{ggT}(N, n) > 1$ ist, d.h. wenn $N \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$.

[V. Heun; 2001-01-07]

Seite 276, Zeile +9 *(Korrektur):*

Ersetze: **for** (int $i = 1$; $i \leq n$; i++)

durch: **for** (int $i = 1$; $i \leq n - \ell$; i++)

[T. Bayer; 2000-12-01]