Theoretische Grundlagen der Informatik II
Blatt 10

Markus Vieth Marvin Becker

25. Januar 2016

Markus Vieth, Marvin Becker

Aufgabe 1

Pseudocode Sei `E` das Ergebnis des Monte Carlo Algorithmus, `I` die Eingabe und `boolean test(Ergebnis E)` der Algorithmus, welcher das Ergebnis überprüft.

```
Ergebnis E;
do {
        E = MonteCarloAlgorithmus(I);
}while(!test(E));
return E;
```

Laufzeit Sei $q(n) = 1 - p(n)$ und $P(X = i) := q(n)^{i-1} \cdot p(n)$ die Wahrscheinlichkeit, dass der Monte Carlo Algorithmus nach i Durchläufen das richtige Ergebnis liefert (also zuerst $i - 1$ falsche und dann ein richtiges). Dann beträgt die zu erwartende Anzahl an Durchläufen:

$$E(X) = \sum_{i=1}^{\infty} i \cdot q(n)^{i-1} \cdot p(n) =^{1} p(n) \cdot \sum_{i=1}^{\infty} i \cdot q(n)^{i-1} =^{2} p(n) \cdot \frac{1}{(1-q(n))^2} = \frac{p(n)}{(1-1+p(n))^2} = \frac{1}{p(n)}$$

Sei $T_{LV}(n)$ die Laufzeit des oben beschriebenen Algorithmus:

$$\Rightarrow T_{LV}(n) = E(X) \cdot (T(n) + t(n)) = \frac{T(n) + t(n)}{p(n)}$$

q.e.d.

Sei X die Anzahl der Durchläufe $X \sim geom_p \Rightarrow E[X] = \frac{1}{p(n)}$ P(X=k)=(1-p)$^{k-1} \cdot p$ E[X] $= \sum_{k=1}^{\infty} = \sum_{k=1}^{\infty}(1 - p$

Aufgabe 2

a)

Behauptung Wenn f und g vernachlässigbar sind, dann ist $f + g$ vernachlässigbar.

Beweis Sei $\mathcal{P}$ die Menge aller Polynome,

$$f, g \text{ vernachlässigbar } \Rightarrow \forall p(x) \in \mathcal{P} \exists N \in \mathbb{N} | f(n) < \frac{1}{2p(n)} \wedge g(n) < \frac{1}{2p(n)} \forall n > N$$

$$\Rightarrow f(n) + g(n) < \frac{1}{2p} + \frac{1}{2p} = \frac{2}{2p} = \frac{1}{p} \frac{1}{2p(n)} + \frac{1}{2p(n)} = \frac{2}{2p(n)} = \frac{1}{p(n)} \forall n > N$$

q.e.d.

b)

Behauptung Wenn f und g vernachlässigbar sind, dann ist fg vernachlässigbar.

[1] $\sum_{i=1}^{\infty} i \cdot q(n)^{i-1} \cdot p(n)$ ist absolut konvergent, wenn $0 < p(n) < 1$, kann per Quotientenkriterium gezeigt werden

[2] Ableitung der geometrischen Reihe

Beweis

f, g vernachlässigbar $\Rightarrow$[3] $\underline{f < 1 f(n) < 1} \wedge \underline{g < 1 g(n) < 1} \Rightarrow \underline{fg < g < p(n)} \underline{f(n)g(n) < g(n) < \frac{1}{p(n)}} \Rightarrow \underline{fg f(n)g(n)}$ ist

q.e.d.

c)

Behauptung Wenn f vernachlässigbar und g eine beliebige positive Funktion ist, dann ist $f + g$ vernachlässigbar.

Gegenbeispiel

Anmerkung: Im folgenden wird davon ausgegangen, dass vernachlässigbare Funktionen stets größer oder gleich 0 sind.
Sei f eine beliebige vernachlässigbare Funktion und $g = 1$

$$\nexists N \in \mathbb{N} \mid f(n) + 1 < 1 \; \forall \; n > N$$

q.e.d.

d)

Behauptung Wenn f vernachlässigbar und c eine positive Konstante ist, dann ist cf vernachlässigbar.

Beweis

$$f \text{ vernachlässigbar } \Rightarrow \forall p(x) \in \mathcal{P} \exists N \in \mathbb{N} | f(n) < \frac{1}{c \cdot p(n)} \forall n > N \Rightarrow c \cdot f(n) < \frac{c}{c \cdot p(n)} = \frac{1}{p(n)}$$
$$\Rightarrow cf \text{ ist vernachlässigbar.}$$

q.e.d.

e)

Behauptung $f(n) = \frac{1}{n^{10}}$. f ist vernachlässigbar.

Gegenbeispiel

$$\nexists N \in \mathbb{N} | \frac{1}{n^{10}} < \frac{1}{n^{42}} \Rightarrow f \text{ ist nicht vernachlässigbar.}$$

q.e.d.

Aufgabe 3

a)

Behauptung Sei $H_1(s) = G_2(\overline{s})$. Zeige, dass H_1 ein PZG ist.

Beweis

[3] da 1 ein Polynom vom Grad 0 ist

Zu zeigen:$\ell_{H_1}(n) > n$

$$H_1(s) = G_2(\overline{s}) \wedge \ell_{G_2}(n) = 2n \Rightarrow \ell_{H_1}(n) = 2n$$

Zu zeigen:$|Pr\left[D(H_1(s)) = 1\right] - Pr\left[D(r) = 1\right]| \leq negl(n)$ Sei $s \in_R \{0,1\}^n$ und $r \in_R \{0,1\}^{2n}$ $\_ : \{0,1\}^n \to \{0,$

$$s \text{ zufällig gleichverteilt} \Rightarrow Pr\left[D(G_2(\overline{s})) = 1\right] = Pr\left[D(G_2(s)) = 1\right]$$

$$\Rightarrow Pr\left[D(G_2(\overline{s})) = 1\right] = Pr\left[D(G_2(s)) = 1\right] = Pr\left[D(H_1(s)) = 1\right]$$

$\Rightarrow H_1$ ist ein PZG.

b)

Behauptung Sei $H_2(s) = G_1(s)|G_2(\overline{s})$. Zeige, dass H_2 nicht notwendig ein PZG ist, indem du G_1 und G_2 so wählst, dass H_2 nicht wirklich randomisiert ist.

Gegenbeispiel Sei $G_1(s)$ ein PZG und $G_2(s) := G_1(\overline{s})$ und somit auch ein PZG. Und $negl(n)$ die Menge aller vernachlässigbaren Funktionen.

$$\Rightarrow H_1(s) = G_1(s)|G_2(\overline{s}) = G_1(s)|G_1(s)$$

$\Rightarrow$ Für einen Unterscheider $\mathfrak{D}$, welcher in eine Bitfolge s der Länge $4n$ überprüft, ob die ersten $\frac{4n}{2}$ den letzten $\frac{4n}{2}$ Bits entsprechen gilt:

$$Pr\left[D(H_2(s)) = 1\right] = 1 \wedge = Pr\left[D(r) = 1\right] = \frac{2^{2n}}{2^{4n}} = \frac{1}{2^{2n}}$$

$$\Rightarrow |Pr\left[D(H_2(s)) = 1\right] - Pr\left[D(r) = 1\right]| = \frac{2^{2n} - 1}{2^{2n}} \notin negl(4n)$$

$\Rightarrow H_2(s)$ ist kein PZG.

q.e.d.