Algorithmen, Wahrscheinlichkeit und Information

Kapitel 01: Ereignisse und Wahrscheinlichkeit (WSK)

Def.: Wahrscheinlichkeitsraum
1) Ergebnisraum Ω
= Menge aller möglichen Ereignisse
$\omega \in \Omega$: Elementarereignis
2) Ereignissystem Σ
= Menge von Testmengen aus Ω
= Z^{Ω}
3) WSK-Maß P:
P: $\Sigma \rightarrow [0,1]$

Def.: WSK-Maß P: $\Sigma \rightarrow [0,1]$
$P[\Omega] = 1$
$P[\emptyset] = 0$
Für alle paarweise disjunkten Ereignisse E_1, E_2, ...
$P[\bigcup E_i] = \Sigma(P[E_i])$

Ereignisse sind Mengen
$E_1 \cap E_2$: E_1 und E_2 treten gleichzeitig auf
$E_1 \cup E_2$: mindestens eines von E_1 und E_2 tritt auf
$\overline{E}$: Komplement von E

Lem.: $P[E_1 \cup E_2] = P[E_1] + P[E_2] - P[E_1 \cap E_2]$
Bew.:
$P[E_1] = P[E_1 \setminus (E_1 \cap E_2)] + P[E_1 \cap E_2]$
$P[E_2] = P[E_2 \setminus (E_1 \cap E_2)] + P[E_1 \cap E_2]$
$P[E_1 \cup E_2] = P[E_1 \setminus (E_1 \cap E_2)] + P[E_2 \setminus (E_1 \cap E_2)] + P[E_1 \cap E_2]$
Lem.: Union Bound
Für alle Ereignisse E_1, E_2, ...
$P[\bigcup E_i] \leq \Sigma(P[E_i])$

Lem.: Inklusion und Exklusion
Für Ereignisse E_1, E_2, ...
$P[\bigcup E_i] = \Sigma(P[E_i]) - \Sigma(P[E_i \cap E_j]) + \Sigma(P[E_i \cap E_j \cap E_k]) + ... + (-1)^{l+1} \Sigma(P[E_i \cap E_j \cap \ldots \cap E_l])$

Algorithmus: Äquivalenz von Polynomen
(x-1)(x+2)(x-3)(x+4)(x-5)(x+6)
$\stackrel{?}{=}$
$x^6 + 3x^5 - 14x^4 - 78x^3 + 400x^2 + 444x - 720$
F(x) als Produkt: Ausmultiplizieren $\rightarrow \theta(d^2)$ Operationen
G(x) als Normalform

Allg. $F(x) \stackrel{?}{\equiv} G(x)$

PolyEq(F(x), G(x)))
$r \stackrel{R}{\leftarrow} \{1, \ldots, 1000d\}$
<u>if</u> $F(x) \neq G(x)$ <u>then</u>
return "different"
<u>else</u>
return "maybe equal"

falls:
$F(x) = G(x) \wedge$ "maybe equal": die Antwort ist korrekt
$F(x) \neq G(x) \wedge$ "different": die Antwort ist korrekt
$F(x) \neq G(x) \wedge$ "maybe equal": die Antwort ist falsch!

Wahrscheinlichkeit, dass Antwort falsch ist:
$D(x) = F(x) - G(x) \Leftrightarrow$ falls r Nullstelle von D(x)
Grad d $\Leftrightarrow$ höchstens d Nullstellen
WSK $= \frac{d}{1000 \cdot d} = \frac{1}{1000}$

<u>Randomisierte Algorithmen</u>

Las Vegas Algorithmus:
terminiert eventuell nicht
Ergebnis immer korrekt

Monte Carlo Algorithmus:
terminiert immer
Ergebnis eventuell falsch
$\rightarrow$ Für Entscheidungsprobleme (YES/NO)
Einseitige Fehler
Eine Antwort (YES/NO) ist immer korrekt
Zweiseitige Fehler
...

<u>Unabhängigkeit</u>
<u>Def.:</u> Ereignisse E und F sind unabhängig $\leftrightarrow P[E \cap F] = P(E) \cdot P(F)$

<u>bedingte Wahrscheinlichkeit</u>
$P[E|F] = \frac{P[E \cap F]}{P(F)}$

Algorithmus MultiPolyEq(...)
<u>for</u> j = 1, ..., k <u>do</u>
<u>if</u> PolyEq(...) = "different" <u>then</u>
return "different"

end
return "maybe equal"

Wahrscheinlichkeiten sind unabhängig
P[eine Runde falsch] = $\frac{1}{1000}$
P[alle k Runden falsch] = $(\frac{1}{1000})^k$

Theorem
$E_1, E_2, ..., E_k$ paarweise disjunkte Ereignisse
$\Omega = \bigcup E_i$
$P[A] = \Sigma\, P[A|E_j] \cdot P[E_j]$

Theorem von Bayes
$E_1, E_2, ..., E_k$ paarweise disjunkte Ereignisse
$\Omega = \bigcup E_i$
Für alle A, E_j: $P[E_j|A] = \frac{P[E_j \cap A]}{P(A)} = \frac{P[A|E_j] \cdot P[E_j]}{\Sigma P[A|E_j] \cdot P[E_j]}$

Intrusive-Prevention-System
Soll Alarm (A) geben, falls eine Intrusion (I) vorliegt
$P[A|I] = 0.95$
$P[A|T] = 0.01$
$P[I] = 0.02$

WSK dafür, dass bei Alarm (A) tatsächlich eine Inklusion passiert:
$P[I|A] = 0.66$