Bayes und der Primzahltest von Rabin und Miller

Ist *n* keine Primzahl, so kann man (relativ leicht) zeigen, dass *n* für höchstens 25 % der Basen *a* den Rabin-Miller-Test besteht. Daher ist die Wahrscheinlichkeit dafür, dass eine Zahl, die nicht prim ist, dennoch als prim getestet wird kleiner $\frac{1}{4^k}$ (falls der Test mit *k* Zufallszahlen als Basen durchgeführt wird). Da der Test andererseits nie „false“ antwortet, wenn *n* prim ist (Satz von Fermat!), gilt insgesamt:

Rabin-Miller sagt → *n* ist ↓	true	false
prim	*richtig positiv* $p(\text{true} \mid \text{prim}) = 1$	*falsch negativ* $p(\text{false} \mid \text{prim}) = 0$
nicht prim	*falsch positiv* $p_k(\text{true} \mid \text{nicht prim}) \le \frac{1}{4^k}$	*richtig negativ* $p_k(\text{false} \mid \text{nicht prim}) \ge 1-\frac{1}{4^k}$

Interessanter ist es aber die Wahrscheinlichkeit dafür zu kennen, dass eine Zahl, die als prim getestet wurde, tatsächlich nicht prim ist. Zur Ermittlung dieser Wahrscheinlichkeit berechnen wir zunächst die Wahrscheinlichkeit p_n für eine *n*-bit-Zahl prim zu sein.

Es gibt etwa $\pi(2^n)-\pi(2^{n-1})$ *n*-bit-Primzahlen, also ist

$$p_n \approx \frac{\frac{2^n}{n\ln(2)}-\frac{2^{n-1}}{(n-1)\ln(2)}}{2^{n-1}} = \frac{2}{n\ln(2)}-\frac{1}{(n-1)\ln(2)} = \frac{n-2}{(n-1)n\ln(2)}.$$

Für $n = 512$ gilt $p_n \approx \frac{510}{511\cdot 512\cdot \ln(2)} \approx \frac{1}{355{,}6}$.

Die bedingte Wahrscheinlichkeit für eine *n*-bit-Zahl nicht prim zu sein, unter der Vorausset zung, dass der Rabin-Miller-Test bestanden wird, ist daher bei *k* Tests

$$
\begin{aligned}
p_{n,k}(\textit{nicht prim} \mid \textit{true}) &\overset{(*)}{=} \frac{p_n(\textit{nicht prim})\, p_k(\textit{true} \mid \textit{nicht prim})}{p_n(\textit{nicht prim})\, p_k(\textit{true} \mid \textit{nicht prim}) + p_n(\textit{prim})\, p(\textit{true} \mid \textit{prim})} \\
&\le \frac{(1-p_n)\frac{1}{4^k}}{(1-p_n)\frac{1}{4^k} + p_n \cdot 1} \\
&= \frac{1}{4^k} \cdot \frac{(1-p_n)4^k}{1-p_n+p_n 4^k} \\
&= p_k(\textit{true} \mid \textit{nicht prim}) \cdot \frac{(1-p_n)4^k}{1-p_n+p_n 4^k}. \\
&\le p_k(\textit{true} \mid \textit{nicht prim}) \cdot \frac{1-p_n}{p_n},
\end{aligned}
$$

also:

$$p_{512,k}(\textit{nicht prim} \mid \textit{true}) \le p_k(\textit{true} \mid \textit{nicht prim}) \cdot 354{,}6$$

(Für *k* = 10 ist $p_{512,10}(\textit{nicht prim} \mid \textit{true}) \le p_{10}(\textit{true} \mid \textit{nicht prim}) \cdot 354{,}5$ nur geringfügig kleiner)

Die Gleichung (*) folgt aus dem Satz von Bayes, der im Folgenden für endliche Mengen bewiesen wird.

Hat die Menge *Ω* genau *n* Elemente und die Teilmenge $E \subseteq \Omega$ genau *m* Elemente, so sagt man: Die *relative Häufigkeit* der Elemente von *E* in *Ω* ist $\frac{m}{n}$ bzw. die *Wahrscheinlichkeit* dafür, dass ein Element aus *Ω* auch in *E* ist, beträgt $p(E) = \frac{m}{n}$.

Bedingte Wahrscheinlichkeiten:

Enthält *Ω* eine weitere Teilmenge E_1 mit genau n_1 Elementen und enthält $E_1 \cap E$ genau m_1 Elemente, so ist die relative Häufigkeit der Elemente von *E* in E_1 gleich $\frac{m_1}{n_1}$. In diesem Fall sagt man auch: Die Wahrscheinlichkeit dafür, dass ein Element in *E* ist, unter der Voraussetzung, dass es in E_1 ist, beträgt $p(E \mid E_1) = \frac{m_1}{n_1}$. $p(E \mid E_1)$ heißt auch *bedingte Wahrscheinlichkeit* (für *E* unter der Voraussetzung E_1). Dabei gilt:

(1) $$p(E \mid E_1) = \frac{p(E_1 \cap E)}{p(E_1)}.$$

(Beweis: $p(E \mid E_1) = \frac{m_1}{n_1} = \frac{\frac{m_1}{n}}{\frac{n_1}{n}} = \frac{p(E_1 \cap E)}{p(E_1)}$.) Daraus folgt nun auch der

Satz von der totalen Wahrscheinlichkeit:

Sind E, E_1 und E_2 Teilmengen der endlichen Menge Ω mit $E_1 \cap E_2 = \varnothing$ und $E_1 \cup E_2 = \Omega$ (d. h. Ω ist die disjunkte Vereinigung von E_1 und E_2), so gilt

(2) $\quad p(E) = p(E_1) \cdot p(E \mid E_1) + p(E_2) \cdot p(E \mid E_2)$.

Beweis: Mit den Bezeichnungen von oben, $|E_2| = n_2$ und $|E_2 \cap E| = m_2$ gilt

$$p(E_1) \cdot p(E \mid E_1) + p(E_2) \cdot p(E \mid E_2) = \frac{n_1}{n} \cdot \frac{m_1}{n_1} + \frac{n_2}{n} \cdot \frac{m_2}{n_2} = \frac{m_1}{n} + \frac{m_2}{n} = \frac{m}{n} = p(E).$$

Bemerkung. Diese Aussage sowie der Satz von Bayes gelten auch für unendliche Wahrscheinlichkeitsräume.

Aus (1) und (2) folgt der

Satz von Bayes: Sind E, E_1 und E_2 Teilmengen der endlichen Menge Ω mit $E_1 \cap E_2 = \varnothing$ und $E_1 \cup E_2 = \Omega$ (d. h. Ω ist die disjunkte Vereinigung von E_1 und E_2), so gilt

$$p(E_1 \mid E) = \frac{p(E_1) \cdot p(E \mid E_1)}{p(E_1) \cdot p(E \mid E_1) + p(E_2) \cdot p(E \mid E_2)}.$$

Beweis: Aus (1) folgt $p(E_1) \cdot p(E \mid E_1) = p(E \cap E_1) = p(E) \cdot p(E_1 \mid E)$, also auch $p(E_1 \mid E) = \dfrac{p(E_1) \cdot p(E \mid E_1)}{p(E)}$ und mit (2) die Behauptung.