ETH Zürich
Dept. Informatik

Prof. Markus Gross
WS 05/06

Informationstheorie

Lösung 2

2.1 Bedingte Wahrscheinlichkeiten

a) Wir definieren die Zufallsvariablen K und T: $K = 1$ falls Alice krank ist, sonst $K = 0$. $T = 1$ falls das Testergebnis von Alice positiv ist, sonst $T = 0$.
Gesucht ist die bedingte Wahrscheinlichkeit

$$\begin{aligned} P(K=0|T=1) &= \frac{P(K=0,T=1)}{P(T=1)} = \frac{P(K=0)\cdot P(T=1|K=0)}{0.99999\cdot 0.01 + 0.00001\cdot 0.99} \\ &= \frac{0.99999\cdot 0.01}{0.0100098} = \frac{99999}{100098} \approx 0.99901097. \end{aligned}$$

Die A-priori-Wahrscheinlichkeit liegt bei 0.99999. Ein positives Testergebnis braucht Alice also nicht stark zu beunruhigen.

b) K und T seien wie oben für Bob definiert.
Gesucht ist die bedingte Wahrscheinlichkeit

$$\begin{aligned} P(K=1|T=0) &= \frac{P(K=1,T=0)}{P(T=0)} = \frac{P(K=1)\cdot P(T=0|K=1)}{0.99999\cdot 0.99 + 0.00001\cdot 0.01} \\ &= \frac{0.00001\cdot 0.01}{0.9899902} = \frac{1}{9899902} \approx 0.0000001010111. \end{aligned}$$

Die A-priori-Wahrscheinlichkeit liegt bei 0.00001. Ein negatives Testergebnis erhöht Bobs Gelassenheit um etwas weniger als den Faktor 100.

2.2 Charakteristische Grössen für Wahrscheinlichkeitsverteilungen

a) Die optimale Strategie ist, die wahrscheinlichste PIN auszuprobieren. Die Grösse ist also gleich der maximalen Wahrscheinlichkeit:

$$OneTry(X) = \max_x P_X(x).$$

b) Die Menge der Elementarereignisse sind alle Paare (x_1, x_2) von PINs, wobei x_1 der PIN der gefundenen Karte und x_2 der PIN des Betrügers ist: $\mathcal{E} = \mathcal{X}^2$. Die Wahrscheinlichkeiten sind $P((x_1, x_2)) = P_X(x_1)P_X(x_2)$. Das Ereignis $\mathcal{A}$, dass der Betrüger Erfolg hat, ist $\mathcal{A} = \{(x_1, x_2)|x_1 = x_2\}$. Die Erfolgswahrscheinlichkeit ist die Summe der Wahrscheinlichkeiten der Elemente in $\mathcal{A}$. Folglich ist $P(\mathcal{A}) = \sum_x P_X(x)^2$. Dies ist die sogenannte *Kollisionswahrscheinlichkeit*.

c) Es müssen im schlimmsten Fall alle PINs mit einer positiven Wahrscheinlichkeit durchprobiert werden:

$$TryAll(X) = \#\{x|P_X(x) > 0\}.$$

Dies ist wohl kein sehr gutes Mass für die Sicherheit der Karte. Es ist nämlich möglich, dass es viele PINs mit sehr kleiner, und nur wenige mit grosser Wahscheinlichkeit gibt. Dann wäre obiges Mass zwar sehr gross, aber es wäre trotzdem möglich, die PIN in wenigen Versuchen mit grosser Wahrscheinlichkeit herauszufinden. Es gibt verschiedene Möglichkeiten, ein besseres Mass zu definieren. Sei im Folgenden $t(x)$ die Position, an welcher x mit der optimalen Strategie ausprobiert wird, das heisst x ist an der $t(x)$-ten Stelle, wenn die PINs ihrer Wahrscheinlichkeit nach sortiert werden.

- Die mittlere Anzahl Versuche, um die PIN zu erhalten:

$$MeanTrials(X) = \sum_x t(x)P_X(x).$$

- Die Anzahl Versuche, um mit einer Wahrscheinlichkeit p die PIN zu erlangen:

$$Trials_P(X) = \min\{t| \sum_{\{x|t(x)\leq t\}} P_X(x) \geq p\}.$$

- Vielfach werden Karte nach drei ungültigen Versuchen gesperrt. Deshalb kann man auch die Summe der Wahrscheinlichkeiten der drei wahrscheinlichsten PINs als Mass für die Sicherheit definieren:

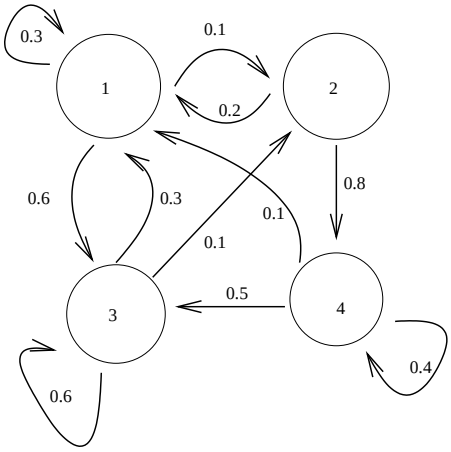
$$ThreeTrials(X) = \sum_{\{x|t(x)\leq 3\}} P_X(x)$$

2.3 Markov-Kette

Wir müssen Y so definieren, dass Z nicht mehr von X abhängt, wenn Y gegeben ist. Wenn X gerade ist, dann ist Z gleichverteilt über die ungeraden Werte. Wenn X ungerade ist, ist Z gleichverteilt über die geraden Werte. Die Abhängigkeit von Z von X steckt also in der Parität von X. Wenn wir nun $Y = X \pmod 2$ wählen, ist $P_{Z|XY} = P_{Z|Y}$.

2.4 Markov-Zustandsautomaten

a) Der Zustandsgraph sieht so aus:



b) Jeder Zustandsübergang kann betrachtet werden als eine Multiplikation mit M. Die Wahrscheinlichkeitsverteilung erhält man also am einfachsten durch

$$P_3(X) = M^3 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0.275 \\ 0.083 \\ 0.538 \\ 0.104 \end{bmatrix}$$

c) Die totalen Wahrscheinlichkeiten stehen im Eigenvektor v_1 zum Eigenwert 1, positiv und normiert nach der 1-norm ($\|v_1\|_1 = 1$, die Summe der Elemente ist 1), i.e. die Werte sind tatsaechlich eine Wahrscheinlichkeitsverteilung. Matlab sez:

$$P(X) = v_1 = \begin{bmatrix} 0.2703 \\ 0.0811 \\ 0.5405 \\ 0.1081 \end{bmatrix}$$

d) Ist der momentane Zustand der Automaten bekannt, so ist die totale Wahrscheinlichkeit im allgemeinen wenig Aussagekräftig. Die bedingten Wahrscheinlichkeiten in der Übergangsmatrix, insbesondere die zum aktuellen Zustand gehörige Spalte ist interassanter. Diese Spalte gibt die Verteilung des Zustands nach einem Zustandsübergang an.

Für die Wahrscheinlichkeitsverteilung $P_n(X|x_i)$, die die Wahrscheinlichkeiten der Zustände nach n Zustandsübergängen angibt (bei ursprünglichem Zustand x_i), gilt, dass

$$\lim_{n\to\infty} P_n(X|x_i) = P(X)$$

Egal, von welchem Zustand mal startet, sofern $P(x_i) \neq 0$. [Für einen Beweis siehe die Herleitung der Potenzmethode zur Eigenwertberechnung.]

Man kann also bei unserem kleinen Markov-Automaten erwarten, dass die Wahrscheinlichkeitsverteilung $P_{100}(X)$ recht nahe an $P(X)$ liegt.