Aktueller Überblick

§0 Einführende Worte (✓)

§1 Geschichtlicher Überblick (✓)

§2 Zufall

§3 Perfekte Sicherheit und ihre Grenzen

§4 Angriffsszenarien

§5 Der komplexitätstheoretische Ansatz

§6 Pseudozufallsgeneratoren und Stromchiffren

§7 Pseudozufallsfunktionen und Blockchiffren

§2 Zufall

Zufall

Eine intuitive Einführung
mit Variablen im klassischen Sinne.

Achtung. Die Darstellung ist teilweise substantiell anders als der
aktuelle "Standard".

Das betrifft auch den Begriff der Zufallsvariablen.

Aber: Für Anwendungen passt das Folgende sogar besser.

Mit der "aktuellen Sichtweise" muss man de facto oftmals in
Anwendungen "schummeln", weil die Definitionen nicht ganz
passen, bei uns ist das besser.

Variablen

Klassische Idee von Variablen:

Beispiel.

Wir betrachten einen sich auf einer Bahn bewegenden Gegenstand.

Wir haben die **Variablen**

Ort. x

Zeit. t

Die Variablen können konkrete **Werte** annehmen.

$$x = x^{(0)}, t = t^{(0)}, \dots$$

(“ $x = x^{(0)}$ ” bedeutet nicht “Identität”, denn eine Variable und ein Wert sind immer verschieden, es ist nur eine Symbolik für “Die Variable nimmt / nehme den Wert an.”. Besser wäre vielleicht so etwas wie $x \rightsquigarrow x^{(0)}$.)

Variablen

In einem mathematischen Modell wird dies beschrieben durch einen *funktionalen Zusammenhang*:

$$x = f(t) .$$

(Der Begriff ist vielleicht von mir (weiß nicht); “funktional” ist hier das Adjektiv zu “Funktion”. Es gibt auch den Begriff eines “Funktional”; dies ist etwas anderes.)

In Bezug auf diesen Zusammenhang heißt t **unabhängige Variable** und x **abhängige Variable**.

Für das Folgende besser: x ist von t **funktional abhängig** / wird so betrachtet.

Das kann sich aber immer ändern:

Man könnte in einer Anwendung auch den funktionalen Zusammenhang vergessen ,

einfach x als unabhängige Variable betrachten.

Variablen

Vergleiche “moderne Sichtweise”:

“Was sollen ‘Variablen’ überhaupt sein?

Ich kenne nur Elemente und Abbildungen.

Wir haben hier eine Abbildung

$$[t_0, t_1] \longrightarrow \mathbf{R}, t \mapsto x(t)$$

‘ t ’ ist aber keine Variable, sondern immer ein konkretes Element aus dem Definitionsbereich.”

So gehen wir hier **nicht** vor.

Wahrscheinlichkeitsräume

Ein mathematischer Zugang zur Idee der Wahrscheinlichkeiten mit echten Variablen

(Was Wahrscheinlichkeit "ist", wird nicht behandelt, es wird einfach Mathe gemacht ...)

Es sei $\mathcal{Z}$ eine endliche oder abzählbare Menge.

Elemente von $\mathcal{Z}$ heißen (normalerweise) **Ergebnisse** (werden entsprechend interpretiert).

(Bei uns diverse Namen wie z.B. Klartext, Chiffriertext, Schlüssel ...)

Typische Notation. $z^{(0)}, z^{(1)}, \dots \in \mathcal{Z}$

Mengen von Ergebnissen heißen **Ereignisse**.

Typische Notation. $\mathcal{A}, \mathcal{B}, \dots \subseteq \mathcal{Z}$

Die Menge selbst heißt (normalerweise) **Ergebnismenge** (Intuition: eines Zufallsexperiments). (Bei uns Klartextraum oder -menge etc.)

Wahrscheinlichkeitsräume

Wir stellen uns ein zufälliges Element / zufälliges Ergebnis aus $\mathcal{Z}$ vor: z .

Wir kennen nur Wahrscheinlichkeiten: $\mathbf{P}[z = z^{(0)}] = \mathbf{P}_z(z^{(0)})$.

(Verwendung eckiger Klammern hat keine Bedeutung.)

Diese müssen (natürlich) erfüllen:

$$\sum_{z^{(0)} \in \mathcal{Z}} \mathbf{P}_z(z^{(0)}) = 1$$

(Bei abzählbar vielen Elementen ist dies der Wert einer konvergenten Reihe.)

Eine Zuordnung $\mathbf{P} : \mathcal{Z} \rightarrow [0, 1]$ mit dieser Summen-Eigenschaft heißt auch **Wahrscheinlichkeitsverteilung** oder **Wahrscheinlichkeitsmaß** auf $\mathcal{Z}$.

Dann: Für $\mathcal{A} \subseteq \mathcal{Z}$: $\mathbf{P}[z \in \mathcal{A}] = \mathbf{P}_z[\mathcal{A}] := \sum_{z^{(0)} \in \mathcal{A}} \mathbf{P}_z(z^{(0)})$.

Wahrscheinlichkeitsräume

Unsere (intuitive) Definition und Sprachgebrauch

Eine **Zufallsvariable mit Werten in $\mathcal{Z}$** und ein **zufälliges Element von $\mathcal{Z}$** sind dasselbe.

Dies ist gegeben durch Wahrscheinlichkeiten wie beschrieben.

Man erhält hiermit eine Wahrscheinlichkeitsverteilung auf $\mathcal{Z}$ und dann einen **Wahrscheinlichkeitsraum**. Dies ist $\mathcal{Z}$ mit einer Wahrscheinlichkeitsverteilung.

Wahrscheinlichkeitsräume

Notation

Wenn z eine Zufallsvariable mit Werten in $\mathcal{Z}$ ist, haben wir die Wahrscheinlichkeiten $\mathbf{P}[z = z^{(0)}] = \mathbf{P}_z(z^{(0)})$ für $z^{(0)} \in \mathcal{Z}$ und die Wahrscheinlichkeitsverteilung $\mathbf{P}_z$.

Wir schreiben in der Regel einfach $\mathbf{P}$ hierfür.

Für $\mathcal{A} \subseteq \mathcal{Z}$ (ein Ereignis) haben wir dann auch

$$\mathbf{P}[z \in \mathcal{A}] = \mathbf{P}_z[\mathcal{A}] = \mathbf{P}[\mathcal{A}] .$$

Wahrscheinlichkeitsverteilungen

Wichtige Eigenschaften einer Wahrscheinlichkeitsverteilung $\mathbf{P}[-]$:

- ▶ Für $\mathcal{A} \subseteq \mathcal{Z}$: $\mathbf{P}[\mathcal{A}] \geq 0$
- ▶ $\mathbf{P}[\mathcal{Z}] = 1$
- ▶ Für $\mathcal{A}, \mathcal{B} \subseteq \mathcal{Z}$ mit $\mathcal{A} \cap \mathcal{B} = \emptyset$: $\mathbf{P}[\mathcal{A} \dot{\cup} \mathcal{B}] = \mathbf{P}[\mathcal{A}] + \mathbf{P}[\mathcal{B}]$
- ▶ Für $\mathcal{A}_1, \mathcal{A}_2, \dots \subseteq \mathcal{Z}$ (abzählbar viele) mit $\mathcal{A}_i \cap \mathcal{A}_j = \emptyset$ für $i \neq j$:

$$\mathbf{P}\left[\bigcup_{n \geq 1} \mathcal{A}_n\right] = \sum_{n=1}^{\infty} \mathbf{P}[\mathcal{A}_n]$$

(Wert einer konvergenten Reihe)

(Axiome von Kolmogorov)

Bedingte Wahrscheinlichkeit

Seien $\mathcal{A}, \mathcal{B} \subseteq \mathcal{Z}$.

Definition. $\mathcal{A}$ und $\mathcal{B}$ sind (zueinander) (stochastisch) unabhängig, falls

$$\mathbf{P}[\mathcal{A} \cap \mathcal{B}] = \mathbf{P}[\mathcal{A}] \cdot \mathbf{P}[\mathcal{B}] .$$

Für festes $\mathcal{B}$ mit $\mathbf{P}[\mathcal{B}] > 0$:

Die bedingte Wahrscheinlichkeit von des Ereignisses $\mathcal{A}$ gegeben das Ereignis $\mathcal{B}$ ist

$$\mathbf{P}[\mathcal{A}|\mathcal{B}] := \frac{\mathbf{P}[\mathcal{A} \cap \mathcal{B}]}{\mathbf{P}[\mathcal{B}]} .$$

Es ist $\mathbf{P}[\mathcal{B}|\mathcal{B}] = 1$.

Wir erhalten eine Wahrscheinlichkeitsverteilung auf $\mathcal{B}$.

Zufallsvariablen

Es sei z eine Zufallsvariable mit Werten in einer endlichen / abzählbaren Menge $\mathcal{Z}$ (= ein zufälliges Element von $\mathcal{Z}$).

Es sei $\mathcal{U}$ eine weitere endliche / abzählbare Menge.

Es sei nun u eine Variable auf $\mathcal{U}$ und es sei ein funktionaler Zusammenhang

$$u = f(z)$$

gegeben.

Die Variable u hängt also mittels f **deterministisch** von der Zufallsvariablen (dem zufälligen Element) z **ab**.

Der Zufall ist also in z , wird deterministisch übertragen.

Induzierter Zufall

$$u = f(z)$$

Die Verteilung von z auf $\mathcal{Z}$ induziert eine von u auf $\mathcal{U}$:

$$\begin{aligned}\mathbf{P}[u = u^{(0)}] &= \mathbf{P}[f(z) = u^{(0)}] = \\ \mathbf{P}[z \in f^{-1}(\{u^{(0)}\})] .\end{aligned}$$

(Ganz genau ist es so: Wir starten mit der Verteilung $\mathbf{P}_z$ auf $\mathcal{Z}$ und definieren mit

$$\mathbf{P}_u(u^{(0)}) := \mathbf{P}_z(f^{-1}(\{u^{(0)}\}))$$

eine Verteilung auf $\mathcal{U}$.)

Wenn wir die Verteilung auf $\mathcal{U}$ eingeführt haben, können wir f “vergessen”. (Jedenfalls, wenn wir nur u betrachten wollen.)

Ein Beispiel

Einmal würfeln mit “fairem Würfel”:

Modell mit z mit Werten in $\mathcal{Z} = \{1, \dots, 6\}$,

$$\mathbf{P}[z = 1] = \dots = \mathbf{P}[z = 6] = \frac{1}{6}.$$

Ein Beispiel

Zweimal würfeln:

$z = (z_1, z_2)$ mit Werten in $\mathcal{Z} = \{1, \dots, 6\} \times \{1, \dots, 6\}$

$$\mathbf{P}[z = z^{(0)}] = \frac{1}{36}.$$

Von z determinierte Zufallsvariablen:

- ▶ z_1
- ▶ z_2
- ▶ $z_1 + z_2$
- ▶ $z_1 - z_2$

Ein Beispiel

▶ $\mathbf{P}[z_1 = z_1^{(0)}] = \frac{1}{6}$.

▶ $\mathbf{P}[z_2 = z_2^{(0)}] = \frac{1}{6}$.

▶ $\mathbf{P}[z_1 + z_2 = z^{(0)}]$:

$z^{(0)}$	2	3	4	5	6	7	8	9	10	11	12
p	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

▶ $\mathbf{P}[z_1 - z_2 = z^{(0)}]$:

$z^{(0)}$	-5	-4	-3	-2	-1	0	1	2	3	4	5
p	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Zufallsvariablen

Es seien zwei Zufallsvariablen gegeben, die deterministisch von derselben Zufallsvariablen abhängen:

$$u = f(z) , v = g(z)$$

Die Zufallsvariable u habe Werte in der endlichen oder abzählbaren Menge $\mathcal{U}$, v in $\mathcal{V}$.

Zufallsvariablen

Wir können nun für $u^{(0)} \in \mathcal{U}, v^{(0)} \in \mathcal{V}$ die **verbundene Wahrscheinlichkeit**

$$\mathbf{P}[u = u^{(0)}, v = v^{(0)}]$$

betrachten mit:

$$\mathbf{P}[u = u^{(0)}, v = v^{(0)}] = \mathbf{P}[f(z) = u^{(0)}, g(z) = v^{(0)}] =$$

$$\mathbf{P}[z \in f^{-1}(\{u^{(0)}\}), z \in g^{-1}(\{v^{(0)}\})] =$$

$$\mathbf{P}[z \in f^{-1}(\{u^{(0)}\}) \cap g^{-1}(\{v^{(0)}\})]$$

(Das ist eigentlich ein Spezialfall des schon behandelten "induzierten Zufall": Es ist $(u, v) = (f(z), g(z))$ mit Zufallsvariable z . Damit können wir aus (u, v) eine Zufallsvariable machen. Es ist:

$$\mathbf{P}_{(u,v)}((u^{(0)}, v^{(0)})) = \mathbf{P}_z[(f, g)^{-1}(\{(u^{(0)}, v^{(0)})\})] = \mathbf{P}_z[f^{-1}(\{u^{(0)}\}) \cap g^{-1}(\{v^{(0)}\})].)$$

Zufallsvariablen

Weiter mit $u, v \dots$

Definition. Dann sind u und v (zueinander) (stochastisch) unabhängig, falls für alle festen Elemente $u^{(0)}$ von $\mathcal{U}$, $v^{(0)}$ von $\mathcal{V}$ gilt:

$$\mathbf{P}[u = u^{(0)}, v = v^{(0)}] = \mathbf{P}[u = u^{(0)}] \cdot \mathbf{P}[v = v^{(0)}]$$

Zufallsvariablen

Es ist stets

$$\mathbf{P}[u = u^{(0)}] = \sum_{v^{(0)}} \mathbf{P}[u = u^{(0)} \mid v = v^{(0)}] \cdot \mathbf{P}[v = v^{(0)}].$$

Hierbei läuft die Summe über alle $v^{(0)} \in \mathcal{V}$ mit $\mathbf{P}[v = v^{(0)}] > 0$.

(Diese Bedingung brauchen wir, damit die bedingte Wahrscheinlichkeit überhaupt definiert ist.)

Begründung

Es ist $\mathbf{P}[u = u^{(0)} \mid v = v^{(0)}] \cdot \mathbf{P}[v = v^{(0)}] = \mathbf{P}[u = u^{(0)}, v = v^{(0)}]$.

Für verschiedene $v^{(1)}, v^{(2)} \in \mathcal{V}$ sind die Bedingungen “ $u = u^{(0)}, v = v^{(1)}$ ” und “ $u = u^{(0)}, v = v^{(2)}$ ” disjunkt (sie können nicht gleichzeitig eintreten).

Deshalb kann man die Wahrscheinlichkeiten addieren, um $\mathbf{P}[u = u^{(0)}]$ zu erhalten.

Wichtige Prinzipien

Zufallsvariablen mit Werten in $\mathcal{Z}$ sind zufällige Elemente in $\mathcal{Z}$.

Eine Zufallsvariable kann (in einem bestimmten Kontext) von einer anderen Zufallsvariablen deterministisch abhängen.

Zufallsvariablen sind wichtig.

Genauer: Bei einer Zufallsvariablen u mit Werten in $\mathcal{U}$ sind die Wahrscheinlichkeiten $\mathbf{P}[u = u^{(0)}]$ wichtig.

D.h. die von u definierte Verteilung auf $\mathcal{U}$ ist wichtig.

Oftmals betrachtet man mehrere Zufallsvariablen, sagen wir u_1 mit Werten in $\mathcal{U}_1, \dots, u_n$ mit Werten in $\mathcal{U}_n$, abhängig von derselben Zufallsvariablen:

$$u_i = f_i(z) .$$

Dann sind die **verbundenen Wahrscheinlichkeiten**

$$\mathbf{P}[u_1 = u^{(1)}, \dots, u_n = u^{(n)}] = \mathbf{P}[f_1(z_1) = u^{(1)}, \dots, f_n(z_n) = u^{(n)}]$$

wichtig.

Zufallsvariablen

Der “zugrundeliegenden Wahrscheinlichkeitsraum” $\mathcal{Z}$ und die funktionalen Zusammenhänge $u_i = f(z_i)$ sind in der Regel nicht wichtig.

(Es ist nicht wichtig, von welcher Zufallsvariablen die u_i nun deterministisch abhängen.)

Gegeben eine Zufallsvariable u_0 mit Werten in $\mathcal{U}$, gibt es eine zweite Zufallsvariable u_1 mit Werten in $\mathcal{U}$ mit

- ▶ derselben Verteilung,
- ▶ funktionalen Zusammenhängen / deterministische Abhängigkeiten

$$u_0 = f_0(z), u_1 = f_1(z)$$

mit einer Zufallsvariable z ,

- ▶ wobei u_0 und u_1 zueinander stochastisch unabhängig sind.

(Denke an Würfeln, betrachte das Beispiel mit den zwei Würfeln!)

Das kann man iterieren, man erhält unabhängige identische verteilte Zufallsvariablen $u_0, u_1, \dots, u_n, \dots$

Laufen lassen bis zum Erfolg ...

Aufgabe

Es sei ein algorithmisches Problem gegeben und ein randomisierter Algorithmus, der immer terminiert, aber nicht immer mit dem richtigen Ergebnis.

Das Ergebnis sei aber überprüfbar.

Wir betrachten eine konkrete Eingabe. Für diese Eingabe ist dann die Ausgabe eine Zufallsvariable. Es sei p die Wahrscheinlichkeit für "richtig".

Wie oft muss man den Algorithmus nun "im Durchschnitt" laufen lassen?

Hinweis

Wie oft muss man im Durchschnitt würfeln, bis man eine 6 erhält?

Laufen lassen bis zum Erfolg ...

Zur Antwort

Wir haben hier (irgendwie) eine Zufallsvariable a für die Anzahl der Versuche.

Wir fragen nach dem Erwartungswert:

$$\mathbf{E}[a] = \sum_{a^{(0)}} \mathbf{P}[a = a^{(0)}] \cdot a^{(0)}$$

Wie ist a verteilt?

Laufen lassen bis zum Erfolg ...

Formaler Ansatz

Sei $p > 0$ die Wahrscheinlichkeit für “richtig” bei einem Lauf.

Wir betrachten unabhängige Zufallsvariablen $e_1, e_2, \dots$ mit Werten in $\{0, 1\}$ mit $\mathbf{P}[e_i = 1] = p$ (1 entspricht “richtig”)

und setzen hiermit $a := \min\{i \mid e_i = 1\}$.

Wir haben

$$\mathbf{P}[a = a^{(0)}] = \mathbf{P}[e_1 = \dots = e_{a^{(0)}-1} = 0, e_{a^{(0)}} = 1] = (1-p)^{a^{(0)}-1} \cdot p .$$

Somit ist a eine **geometrisch verteilte Zufallsvariable**.

Laufen lassen bis zum Erfolg ...

$$\mathbf{P}[a = a^{(0)}] = \mathbf{P}[e_1 = \dots = e_{a^{(0)}-1} = 0, e_{a^{(0)}} = 1] = (p-1)^{a^{(0)}-1} \cdot p.$$

Ist a wirklich eine Zufallsvariable?

Es ist

$$\sum_{a^{(0)}} \mathbf{P}[a = a^{(0)}] = \sum_{i \geq 1} (p-1)^{i-1} \cdot p = \sum_{i \geq 0} (p-1)^i \cdot p = \frac{1}{1 - (1-p)} \cdot p = 1.$$

Ja!

Laufen lassen bis zum Erfolg ...

$$\mathbf{P}[a = a^{(0)}] = \mathbf{P}[e_1 = \dots = e_{a^{(0)}-1} = 0, e_{a^{(0)}} = 1] = (p-1)^{a^{(0)}-1} \cdot p.$$

Der Erwartungswert ist:

$$\begin{aligned} \mathbf{E}[a] &= \sum_{a^{(0)} \geq 1} \mathbf{P}[a = a^{(0)}] \cdot a^{(0)} = \sum_{i \geq 1} (1-p)^{i-1} \cdot p \cdot i = \\ p \cdot \frac{d}{dp} \left(- \sum_{i \geq 1} (1-p)^i \right) &= p \cdot \frac{d}{dp} \left(- \left(\frac{1}{p} - 1 \right) \right) = p \cdot \frac{1}{p^2} = \frac{1}{p} \end{aligned}$$

OK!

Laufen lassen bis zum Erfolg ...

Aufgabe

Es sei ein algorithmisches Problem gegeben und ein randomisierter Algorithmus, der immer terminiert, aber nicht immer mit dem richtigen Ergebnis.

Das Ergebnis sei aber überprüfbar.

Wir betrachten eine konkrete Eingabe. Für diese Eingabe ist dann die Ausgabe eine Zufallsvariable. Es sei p die Wahrscheinlichkeit für "richtig".

Wie oft muss man den Algorithmus dann "im Durchschnitt" laufen lassen?

Antwort

$$\frac{1}{p}$$

Ein Zitat

Wikipedia: Variable

Arten von Variablen

- ▶ *Unabhängige Variable*
- ▶ *Abhängige Variable*

Abgrenzung

Eine Zufallsvariable – auch Zufallsgröße, Zufallsveränderliche oder stochastische Variable – ist keine Variable, sondern eine Funktion, deren Funktionswerte von den Zufallsergebnissen des zugehörigen Zufallsversuchs abhängen.

Meine Frage

Und was sind dann x und y in $y = f(x)$?

Konkrete Werte? Oder ist $y = f$?

Was bedeutet dann “unabhängige Variable” / “abhängige Variable”?

Umgekehrt: Wenn “Variable” ein sinnvolles Konzept ist, dann kann man auch Zufallsvariablen als Variablen betrachten ...