Diskrete Strukturen

Sommer 2019

Prof. Stefan Lucks, Jannis Bossert
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

January 21, 2020

Aufgabe 1: Bedingte Wahrscheinlichkeit

Angenommen, es gibt zwei äußerlich nicht voneinander unterscheidbare Urnen: Die erste Urne beinhaltet drei weiße und drei rote Kugeln; die zweite Urne drei weiße, eine rote und zwei blaue Kugeln. Sie können nicht sehen welche Kugeln wo enthalten sind. Ihre Aufgabe ist es zwei Kugeln ohne Zurücklegen zu ziehen. Sie gewinnen wenn Sie es schaffen zwei gleichfarbige Kugeln zu ziehen.

Aufgabe 1: Bedingte Wahrscheinlichkeit

Angenommen, es gibt zwei äußerlich nicht voneinander unterscheidbare Urnen: Die erste Urne beinhaltet drei weiße und drei rote Kugeln; die zweite Urne drei weiße, eine rote und zwei blaue Kugeln. Sie können nicht sehen welche Kugeln wo enthalten sind. Ihre Aufgabe ist es zwei Kugeln ohne Zurücklegen zu ziehen. Sie gewinnen wenn Sie es schaffen zwei gleichfarbige Kugeln zu ziehen.

Wir definieren folgende Zufallsvariablen:
u_i gibt an, aus welcher Urne wir im i-ten Zug gezogen haben. Mögliche Werte sind U_1 und U_2, für die erste oder zweite Urne.
k_i gibt an welche Farbe die im i-ten Zug gezogene Kugel hat. Mögliche Werte sind W, R, B.

Aufgabe 1: Bedingte Wahrscheinlichkeit

a) Sie ziehen zuerst eine weiße Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt?

Aufgabe 1: Bedingte Wahrscheinlichkeit

a) Sie ziehen zuerst eine weiße Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt? Gesucht: Wahrscheinlichkeit, dass wir aus der ersten Urne gezogen haben, unter der Bedingung, dass wir eine weiße Kugel gezogen haben:

$$\Pr[u_1 = U_1 | k_1 = W]$$

a) $\Pr[u_1 = U_1 | k_1 = W]$

Satz von Bayes:

$$\Pr[A|B] = \frac{\Pr[B|A] \cdot \Pr[A]}{\Pr[B]}$$

Also:

$$\Pr[u_1 = U_1 | k_1 = W] =$$

$$= \frac{\Pr[k_1 = W | u_1 = U_1] \cdot \Pr[u_1 = U_1]}{\Pr[k_1 = W]}$$

$$= \frac{\Pr[k_1 = W | u_1 = U_1] \cdot \Pr[u_1 = U_1]}{\Pr[k_1 = W | u_1 = U_1] \cdot \Pr[u_1 = U_1] + \Pr[k_1 = W | u_1 = U_2] \cdot \Pr[u_1 = U_2]}$$

$$= \frac{\frac{1}{2} \cdot \frac{1}{2}}{\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2}}$$

$$= \frac{1}{2}$$

Aufgabe 1: Bedingte Wahrscheinlichkeit

b) Sie ziehen zuerst eine rote Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt?

Aufgabe 1: Bedingte Wahrscheinlichkeit

b) Sie ziehen zuerst eine rote Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt?

Gesucht: Wahrscheinlichkeit, dass wir aus der ersten Urne gezogen haben, unter der Bedingung, dass wir eine rote Kugel gezogen haben:

$$\Pr[u_1 = U_1 | k_1 = R]$$

b) $\Pr[u_1 = U_1 | k_1 = R]$

Satz von Bayes:

$$\Pr[A|B] = \frac{\Pr[B|A] \cdot \Pr[A]}{\Pr[B]}$$

Also:

$$\Pr[u_1 = U_1 | k_1 = R] =$$

$$= \frac{\Pr[k_1 = R | u_1 = U_1] \cdot \Pr[u_1 = U_1]}{\Pr[k_1 = R]}$$

$$= \frac{\Pr[k_1 = R | u_1 = U_1] \cdot \Pr[u_1 = U_1]}{\Pr[k_1 = R | u_1 = U_1] \cdot \Pr[u_1 = U_1] + \Pr[k_1 = R | u_1 = U_2] \cdot \Pr[u_1 = U_2]}$$

$$= \frac{\frac{1}{2} \cdot \frac{1}{2}}{\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{6} \cdot \frac{1}{2}}$$

$$= \frac{3}{4}$$

Aufgabe 1: Bedingte Wahrscheinlichkeit

c) Ermitteln Sie in Abhängigkeit des Ergebnisses Ihres ersten Zuges eine für Sie optimale Strategie (aus derselben Urne nochmal ziehen oder wechseln) und ermitteln Sie Ihre maximale erwartete Gewinnwahrscheinlichkeit.

Aufgabe 1: Bedingte Wahrscheinlichkeit

c) Ermitteln Sie in Abhängigkeit des Ergebnisses Ihres ersten Zuges eine für Sie optimale Strategie (aus derselben Urne nochmal ziehen oder wechseln) und ermitteln Sie Ihre maximale erwartete Gewinnwahrscheinlichkeit.

Es gibt drei Fälle:

1. Wir ziehen zuerst eine weiße Kugel.
2. Wir ziehen zuerst eine rote Kugel.
3. Wir ziehen zuerst eine blaue Kugel.

Fall 1: $k_1 = W$

Wieder zwei Möglichkeiten: Entweder wir habe aus der ersten oder aus der zweiten Urne gezogen.

Es gilt:

$$\Pr\left[k_2 = W | u_2 = U_1 | u_1 = U_1 | k_1 = W\right] = \frac{2}{5} = Pr_{11}$$
$$\Pr\left[k_2 = W | u_2 = U_2 | u_1 = U_1 | k_1 = W\right] = \frac{1}{2} = Pr_{12}$$
$$\Pr\left[k_2 = W | u_2 = U_1 | u_1 = U_2 | k_1 = W\right] = \frac{1}{2} = Pr_{13}$$
$$\Pr\left[k_2 = W | u_2 = U_2 | u_1 = U_2 | k_1 = W\right] = \frac{2}{5} = Pr_{14}.$$

Bleiben wir bei der Urne des ersten Zugs, erhalten wir

$$\begin{aligned}\Pr\left[k_2 = W | u_2 = u_1 | k_1 = W\right] &= Pr_{11} \cdot \Pr\left[u_1 = U_1 | k_1 = W\right] \\ &\quad + Pr_{14} \cdot \Pr\left[u_1 = U_2 | k_1 = W\right] \\ &= \frac{2}{5} \cdot \frac{1}{2} + \frac{2}{5} \cdot \frac{1}{2} = \frac{2}{5}.\end{aligned}$$

Fall 1: $k_1 = W$

Wieder zwei Möglichkeiten: Entweder wir habe aus der ersten oder aus der zweiten Urne gezogen.

Es gilt:

$$\Pr\left[k_2 = W | u_2 = U_1 | u_1 = U_1 | k_1 = W\right] = \frac{2}{5} = Pr_{11}$$

$$\Pr\left[k_2 = W | u_2 = U_2 | u_1 = U_1 | k_1 = W\right] = \frac{1}{2} = Pr_{12}$$

$$\Pr\left[k_2 = W | u_2 = U_1 | u_1 = U_2 | k_1 = W\right] = \frac{1}{2} = Pr_{13}$$

$$\Pr\left[k_2 = W | u_2 = U_2 | u_1 = U_2 | k_1 = W\right] = \frac{2}{5} = Pr_{14}.$$

Wechseln wir die Urne, erhalten wir hingegen

$$\begin{aligned}\Pr\left[k_2 = W | u_2 \neq u_1 | k_1 = W\right] &= Pr_{12} \cdot \Pr\left[u_1 = U_1 | k_1 = W\right] \\ &\quad + Pr_{13} \cdot \Pr\left[u_1 = U_2 | k_1 = W\right] \\ &= \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}.\end{aligned}$$

Wir sollten demnach die Urne wechseln.

Fall 2: $k_1 = R$

Es gilt:

$$\Pr\left[k_2 = R | u_2 = U_1 | u_1 = U_1 | k_1 = R\right] = \frac{2}{5} = Pr_{21}$$
$$\Pr\left[k_2 = R | u_2 = U_2 | u_1 = U_1 | k_1 = R\right] = \frac{1}{6} = Pr_{22}$$
$$\Pr\left[k_2 = R | u_2 = U_1 | u_1 = U_2 | k_1 = R\right] = \frac{1}{2} = Pr_{23}$$
$$\Pr\left[k_2 = R | u_2 = U_2 | u_1 = U_2 | k_1 = R\right] = 0 = Pr_{24}.$$

Bleiben wir bei der Urne des ersten Zugs, erhalten wir

$$\begin{aligned}\Pr\left[k_2 = R | u_2 = u_1 | k_1 = R\right] &= Pr_{21} \cdot \Pr\left[u_1 = U_1 | k_1 = R\right] \\ &\quad + Pr_{24} \cdot \Pr\left[u_1 = U_2 | k_1 = R\right] \\ &= \frac{2}{5} \cdot \frac{3}{4} + 0 \cdot \frac{1}{4} = \frac{3}{10}.\end{aligned}$$

Fall 2: $k_1 = R$

Es gilt:

$$\Pr[k_2 = R | u_2 = U_1 | u_1 = U_1 | k_1 = R] = \frac{2}{5} = Pr_{21}$$
$$\Pr[k_2 = R | u_2 = U_2 | u_1 = U_1 | k_1 = R] = \frac{1}{6} = Pr_{22}$$
$$\Pr[k_2 = R | u_2 = U_1 | u_1 = U_2 | k_1 = R] = \frac{1}{2} = Pr_{23}$$
$$\Pr[k_2 = R | u_2 = U_2 | u_1 = U_2 | k_1 = R] = 0 = Pr_{24}.$$

Wechseln wir die Urne, erhalten wir hingegen

$$\begin{aligned}\Pr[k_2 = R | u_2 \neq u_1 | k_1 = R] &= Pr_{22} \cdot \Pr[u_1 = U_1 | k_1 = R] \\ &\quad + Pr_{23} \cdot \Pr[u_2 = U_2 | k_1 = R] \\ &= \frac{1}{6} \cdot \frac{3}{4} + \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{4}.\end{aligned}$$

Wir sollten in diesem Fall also lieber nochmal aus der gleichen Urne ziehen.

Fall 3: $k_1 = B$

Hier können wir nur aus Urne 2 gezogen haben, da es keine blaue Kugel in Urne eins gibt. Somit bleiben wir in diesem Fall bei der Urne und ziehen mit Wahrscheinlichkeit $\Pr = \frac{1}{5}$ die zweite blaue Kugel.

Fall 3: $k_1 = B$

Hier können wir nur aus Urne 2 gezogen haben, da es keine blaue Kugel in Urne eins gibt. Somit bleiben wir in diesem Fall bei der Urne und ziehen mit Wahrscheinlichkeit $\Pr = \frac{1}{5}$ die zweite blaue Kugel.

Unsere gesamte Gewinnwahrscheinlichkeit berechnet sich also wie folgt:

$$\begin{aligned}\Pr[k_2 = k_1] &= \Pr[k_2 = W | u_1 \neq u_2 | k_1 = W] \cdot Pr[k_1 = W] \\ &\quad + \Pr[k_2 = R | u_1 = u_2 | k_1 = R] \cdot Pr[k_1 = R] \\ &\quad + \Pr[k_2 = B | u_1 = u_2 | k_1 = B] \cdot Pr[k_1 = B] \\ &= \frac{1}{2} \cdot \frac{1}{2} + \frac{3}{10} \cdot \frac{1}{3} + \frac{1}{5} \cdot \frac{1}{6} \\ &= \frac{1}{4} + \frac{1}{10} + \frac{1}{30} = \frac{15}{60} + \frac{6}{60} + \frac{2}{60} = \frac{23}{60}\end{aligned}$$

Grundlagen der Statistik

Wiederholen Sie aus den Vorlesungsinhalten und selbständig die Bedeutung von Kombination, Permutation und Variation.

	Mit Wiederholung	Ohne Wiederholung	Reihenfolge
Permutation	–	$n!$	Ja
Variation	n^k	$\frac{n!}{(n-k)!}$	Ja
Kombination	$\binom{n+k-1}{k}$	$\binom{n}{k}$	Nein

Grundlagen der Statistik

Angenommen, Sie haben ein fair gemischtes Doppelkopfspiel mit 48 Karten (es gibt vier Farben und pro Farbe gibt es die folgenden Karten je zwei Mal: 9, 10, Bube, Dame, König und Ass).

a) Sie ziehen alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen der Karten gibt es?

b) Sie bekommen nacheinander eine Karte bis Sie 10 Karten haben. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wieviele mögliche Ergebnisse gibt es für Ihre 10 Karten (d. h. die Reihenfolge ist irrelevant)?

c) Sie erhalten 10 Karten aus dem Blatt nacheinander ohne Zurücklegen. Wie viele mögliche Reihenfolgen gibt es (die Reihenfolge ist relevant)?

d) Wir ignorieren für diese Teilaufgabe die Farbe der Karten und betrachten nur ihren Kartenwert. Sie ziehen abermals alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen gibt es?

e) Sie ziehen nacheinander eine Karte bis Sie eine Herz Zehn ziehen. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wie oft müssen Sie ziehen damit Ihre Wahrscheinlichkeit für eine Herz Zehn ≥ 0.5 ist?

a) Sie ziehen alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen der Karten gibt es?

a) Sie ziehen alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen der Karten gibt es?

Permutation mit Wiederholung $\rightarrow \frac{n!}{k_1!\cdot\ldots\cdot k_n!} = \frac{48!}{2!^{24}} = 7.4 \cdot 10^{53}$

b) Sie bekommen nacheinander eine Karte bis Sie 10 Karten haben. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wieviele mögliche Ergebnisse gibt es für Ihre 10 Karten (d. h. die Reihenfolge ist irrelevant)?

b) Sie bekommen nacheinander eine Karte bis Sie 10 Karten haben. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wieviele mögliche Ergebnisse gibt es für Ihre 10 Karten (d. h. die Reihenfolge ist irrelevant)?

Das ist eine Kombination mit Wiederholung. Es gibt

$$\binom{0.5 \cdot n + k - 1}{k} = \binom{33}{10} = 92561040$$

Möglichkeiten.

c) Sie erhalten 10 Karten aus dem Blatt nacheinander ohne Zurücklegen. Wie viele mögliche Reihenfolgen gibt es (die Reihenfolge ist relevant)?

c) Sie erhalten 10 Karten aus dem Blatt nacheinander ohne Zurücklegen. Wie viele mögliche Reihenfolgen gibt es (die Reihenfolge ist relevant)?

Gestrichen

d) Wir ignorieren für diese Teilaufgabe die Farbe der Karten und betrachten nur ihren Kartenwert. Sie ziehen abermals alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen gibt es?

d) Wir ignorieren für diese Teilaufgabe die Farbe der Karten und betrachten nur ihren Kartenwert. Sie ziehen abermals alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen gibt es?

Das ist eine Permutation mit Wiederholung. Für jeden der sechs möglichen Werte haben wir acht Karten, d.h. acht Asse, acht Könige, ... Wir bezeichnen mit $k_1, \ldots, k_6 = 8$ ihre jeweilige Anzahl.

$$\frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_6!} = \frac{48!}{(8!)^6} \approx 2.889 \cdot 10^{33}.$$

e) Sie ziehen nacheinander eine Karte bis Sie eine Herz Zehn ziehen. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wie oft müssen Sie ziehen damit Ihre Wahrscheinlichkeit für eine Herz Zehn ≥ 0.5 ist? Die Wahrscheinlichkeit dass wir nach q Ziehungen eines fair gezogenen Kartenspiels immer noch keine Herz Zehn gezogen haben ist

$$\prod_{i=1}^{q} \left(1 - \frac{2}{48}\right) = \left(\frac{23}{24}\right)^{q} = 0.5.$$

Dies können wir umformen zu

$$q \geq \log_{\frac{23}{24}}(0.5).$$

Wir erhalten $q \geq 16.29$, d.h. Sie müssen im Durchschnitt 17 mal ziehen.

Passwörter

Beurteilen Sie die Sicherheit der folgenden Verfahren zur Passworterzeugung. Begründen Sie bitte mathematisch, warum es in dem Ihrer Meinung nach sichereren System für einen Angreifer schwerer ist ein Passwort zu erraten. Gehen Sie hierbei davon aus, dass der Angreifer weiß, mit welchem System Sie das Passwort erzeugt haben.

System 1: Man wählt zufällig und gleichverteilt nacheinander 13 Zeichen aus dem Alphabet der Groß- und Kleinbuchstaben ohne Sonderzeichen und der Ziffern 0 - 9. ([a-zA-Z0-9])

System 2: Man wählt zufällig und gleichverteilt fünf Worte aus einem Wörterbuch mit 80000 Einträgen.

Zufällig und gleichverteilt bedeutet, dass bei System 1 jedes Zeichen mit der gleichen Wahrscheinlichkeit gewählt wird wie die anderen Zeichen und bei System 2, dass jedes Wort mit der gleichen Wahrscheinlichkeit gewählt wird wie jedes andere Wort. Das Ziehen erfolgt bei beiden Systemen mit Zurücklegen.

Passwörter

Anzahl möglicher Paswörter in System 1:

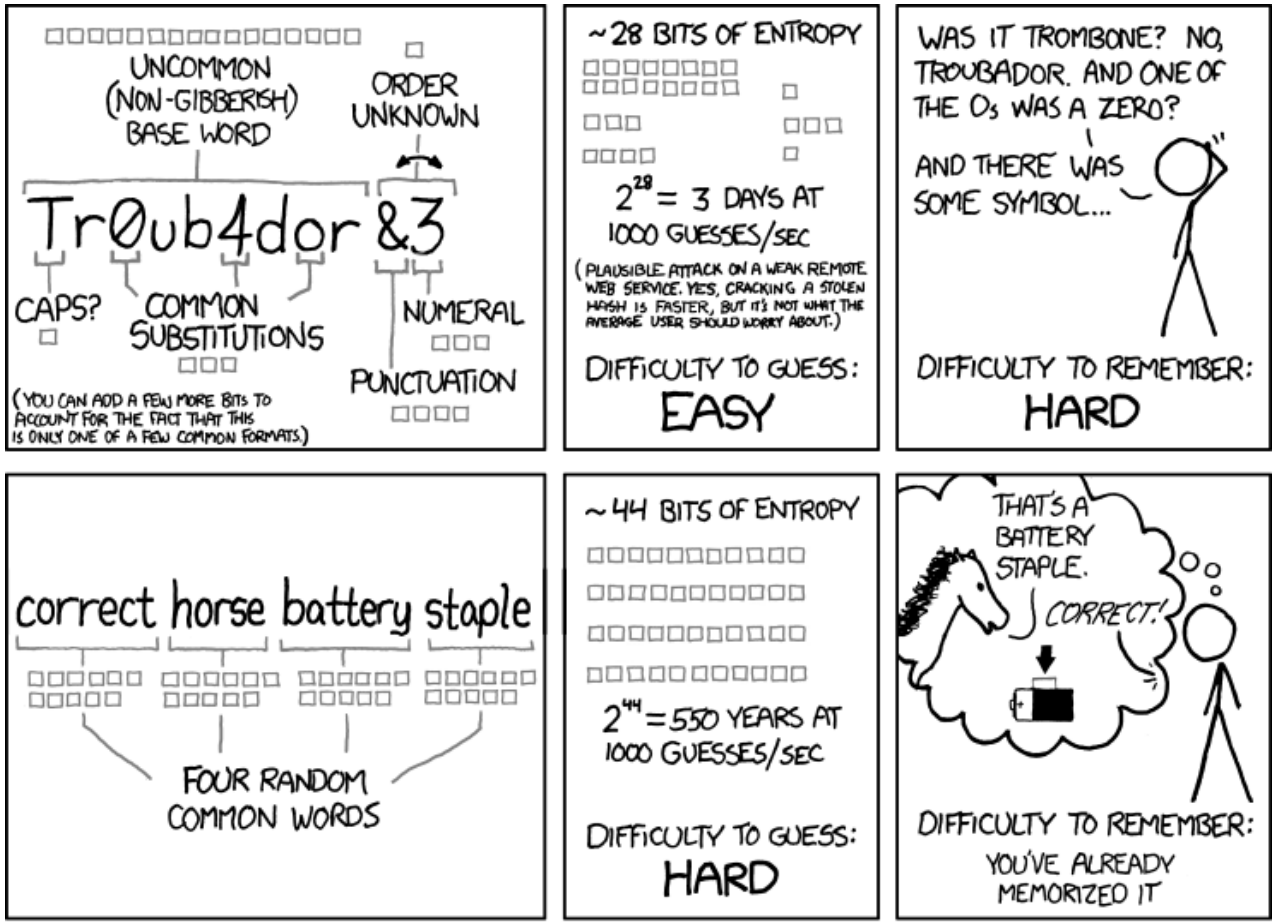
$$62^{13} = 2000285392686697889054 72$$

Anzahl möglicher Paswörter in System 2:

$$80000^5 = 32768000000000000000000000$$

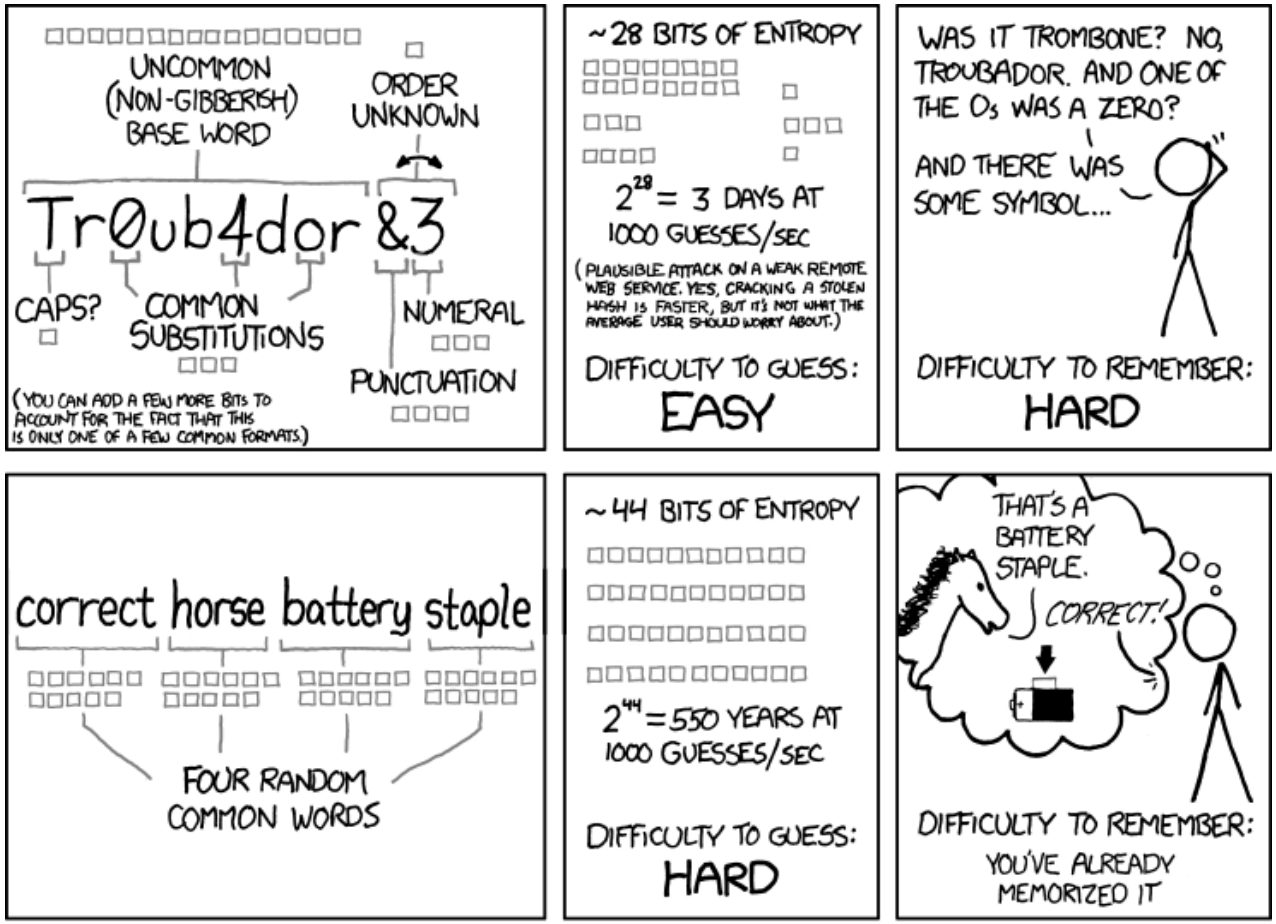
Somit gibt es in System 2 $307677146073133021109452 8$ mehr mögliche passwörter als in System 1. Die Wahrscheinlichkeit, dass ein Angreifer unser Passwort errät ist unter System 2 also geringer als unter System 1, er braucht im Schnitt also wesentlich länger um das Passwort zu erraten.

Passwörter



https://imgs.xkcd.com/comics/password_strength.png, abgerufen 10.01.2020, 15:20 Uhr

Passwörter



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

`https://imgs.xkcd.com/comics/password_strength.png`, abgerufen 10.01.2020, 15:20 Uhr

Nutzt Passwortmanager!

Fragen?