Universität des Saarlandes
FR Informatik

Kurt Mehlhorn **WiSe 2018/19**

Übungen zu Ideen der Informatik

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter18/ideen/

Blatt 8 Abgabeschluss: 17.12.2018

Aufgabe 1 (*5 Punkte*) Teilnehmer bei dem Bitcoin/Blockchain Protokoll die versuchen die mathematischen Rätsel zu lösen, und damit den nächsten Block an der Blockchain bestimmen zu dürfen, nennt man auch *Miner*. Wie in der Vorlesung besprochen, darf ein Miner auch eine Transaktion in den Block setzen bei der er zur Belohnung einen festen Betrag an Bitcoins bekommt. Am Anfang, in 2008, waren das jeweils 50 Bitcoins. Jedes mal wenn die Blockchain um 210000 Blocks gewachsen ist, was circa alle 4 Jahre passiert, wird dieser Betrag halbiert. So liegt dieser gerade bei 12.5. Da die kleinste Denomination des Bitcoins $1/10^8$ beträgt (ein Satoshi), wird man irgendwann den Betrag nicht mehr halbieren können und der Betrag der Belohnung wird dann auf Null gesetzt. Wann wird das etwa passieren? Wie viele Bitcoins werden dann im Umlauf sein?

Lösung: Circa 2110-2140 wird der Betrag auf 0 fallen. Die menge der Bitcoins in Zirkulation wird dann circa 21 Millionen sein.

Aufgabe 2 (*10 Punkte*) Die Wahrscheinlichkeit, dass wenn Alice alleine an einer anderen Abzweigung der Blockchain arbeitet als alle anderen Teilnehmern und trotzdem überholt, errinert an den von der Spieltheorie bekannte „Ruin des Spielers“. Dieser steht für den stets sinkenden Erwartungswert des Spielkapitals im Laufe des Spieles, wenn die Gewinne wieder investiert werden.
Besitze Alice 9 und Bob 1 Euro. Alice und Bob werfen wiederholt eine faire Münze, die bei jedem Wurf mit einer Wahrscheinlichkeit von $p = 0.5$ auf Kopf und $q = 0.5$ auf Zahl landet. Nach jedem Wurf: Sollte Kopf kommen, gibt Alice einen Cent an Bob, sollte Zahl kommen, bekommt Alice einen Cent von Bob. Aufgehört wird wenn einer der zwei Spieler verliert in dem er kein Geld mehr hat.

a) Was ist die Wahrscheinlichkeit, dass Bob gewinnt? (Das Ergebnis ist ausreichend)

b) Erläutern Sie den Rechenweg von Aufgabenteil a).

c) Was ist die Wahrscheinlichkeit, dass das Spiel für immer weitergeht und nie endet?

Hinweis: Versuchen Sie es zuerst mit ein Paar anderen Aufteilungen der 10 Euro. Was, wenn Bob 0 *Cent hat, und Alice* 1000*? Was, wenn Bob* 1 *Cent hat und Alice* 999*, usw.*

Lösung:

- $\frac{1}{10}$. Sei R_n das Ereignis, dass Bob von einer Situation mit n Cents gewinnt. Dann gilt,

$$P(R_n) = P(R_n|\overline{W})P(\overline{W}) + P(R_n|W)P(W)$$
$$= 0.5P(R_{n-1}) + 0.5P(R_{n+1}) \Rightarrow P(R_{n+1}) - P(R_n) = P(R_n) - P(R_{n-1}).$$

  Hier ist W die Wahrscheinlichkeit, dass Bob diese Runde gewinnt. Da $P(R_0) = 0$ und $P(R_{1000}) = 1$

- 0 früher oder später werden 1000 mal Kopf (oder 1000 mal Zahl) hintereinander geworfen.

Aufgabe 3 (*10 Punkte*) Digitale und dezentrale Währungen sind eine relativ neue und revolutionäre Entwicklung. Dabei ist es noch weit offen wie diese sich entwickeln werden. Wie schätzen sie die Wahrscheinlichkeit ein, dass Bitcoin oder eine ähnliche digitale Währung zu einer etablierten Währung wird? Könnten Sie sich vorstellen in fünf oder in zehn Jahren im Supermarkt mit Bitcoins einkaufen zu gehen? Was wären Vor- und Nachteile davon? Diskutieren Sie auf circa einer halben Seite.

Bitcoins und Blockchains war spannend ☐ okay ☐ langweilig ☐
schwierig ☐ okay ☐ einfach ☐