Cryptography --- Prof Jeroen --- 2021/1

Problem Set Module 1

Necessary reading for this assignment:

1. Slide-set of Module 1 -- Probability, Information Theory and Complexity
2. Mao Standard Notation (pg 57-60)
3. Mao § 3.1--3.5; 3.7-3.8 (everything, except Birthday Paradox)
4. Mao § 4.1--4.3;
5. **[Extra]** Mao § 4.4; except § 4.4.5.1

Note: Material labeled as [Extra] is considered an interesting, optional topic, but is outside the scope of the material to be studied for the exams.

Review questions R1 - R11

1. Is cryptography possible without some probabilistic process? Explain your answer.
2. What is the restricted version of Bayes' Theorem? And the extended version?
3. List difficulties with the frequentist interpretation of probabilities.
4. What is the definition of (Shannon) entropy? Conditional entropy? Mutual Information?
5. What is the definition of redundancy of a natural language? What does it say about compressibility?
6. Why is the theory of NP-Completeness of little relevance to crypto?
7. What is a sub-exponential algorithm?
8. What is a trapdoor one-way function? Give an example.
9. Present 3 different ways to model a probabilistic Turing machine.
10. **[Extra]** The classes $\mathcal{ZPP}$, Monte Carlo, Las Vegas, and $\mathcal{BPP}$ an example of a computational problem for each different from the examples given in Mao, Chapter 4.
11. **[Extra]** (Mao question 4.6) The definition of $\mathcal{BPP}$ use the fixed values $\epsilon = \frac{2}{3}$ and $\delta = \frac{1}{3}$, and not some arbitrary values greater then and less then $\frac{1}{2}$. Explain why this is not a problem, i.e. why both definitions are equivalent. See Mao 4.4.1.2.

Exercises E1 -- E10

<u>Probability</u>

1. **[Easy]** Which is more secure? A 6-digit password or a 4-letter password? If the password allows upper and lowercase letters, all digits, and two addition symbols, what is the size of the set of possibilities? This corresponds to how many bits?
2. **[Hard]** At the end of a show, the winning participant is offered to choose between 3 doors, say A, B and C. Behind 1 door is the big prize, behind 2 doors there is nothing. The following steps take place:
    1. P chooses one door, say A.
    2. The show's presenter, Sílvio Santos, opens one of the other 2 doors, say B, and shows that there is no prize behind Door B. Now SS asks P whether P wants to chance to door C, or wants to stick to door B.

    Question Should P switch or not? Justify your answer.

3. **Medium** From the point of view of the participant's strategy, does it matter if the show's presenter actually *knows* behind which door the prize is? Explain.
4. **[Easy]** Approximate how many binary strings of length 128 exist? And of length 256?
5. **[Medium]** Consider the example of Bayes theorem in the slides. Recompute the probability of having illness XYX after having tested positive, if it is known that 1% of the population is affected by XYZ. And what is the answer if 0.01% of the population is affected by it.
6. **[Medium]** (continuation) It is known that the illness XYZ is hereditary: a father has a 30% chance of given the illness to its offspring. If it is known that the father of the patient testes has XYZ, how does this additional information affect the probability computed in the previous question?
7. **[Medium]** Consider an ordinary set of 52 playing cards, with 13 cards of each of four kinds (port.: naipe). See https://pt.wikipedia.org/wiki/Baralho.
    - **Experiment A:** The dealer shuffles the deck, then spreads out all 52 playing cards on the table. Alice chooses one arbitrarily. What is the probability that this card is a spade (♠)?. Answer: Since 13 out of 52 cards are spades, the probability is 1/4.
    - **Experiment B:** The dealer shuffles the deck, then opens the first 2 cards on top. One is a spades, one is not. Compute the probability that the next (third) card is a spades.
    - **Experiment C:** The dealer shuffles the deck, then removes the first 2 cards on top, putting them aside without opening them. Compute the probability that the next (third) card is a spades by conditioning on the 4 possible options of the two unopened cards.
    - Is the answer to Experiment C different from Experiment A? Explain.
    - **Experiment D:** The dealer shuffles the deck, then spreads out all 52 playing cards on the table. Alice chooses one arbitrarily. The dealer then separates 13 cards from the remaining 51 cards and says "these 13 cards are all hearts (♡)". Assuming that the dealer tells the truth, what is the probability that the card chosen by Alice is a spade? Justify your answer.
    - **Experiment E:** The dealer shuffles the deck, then spreads out all 52 playing cards on the table. Alice chooses one arbitrarily. The dealer then separates 13 cards from the remaining 51 cards and says "these 13 cards are all of the same kind". Assuming that the dealer tells the truth, what is the probability that the card chosen by Alice is a spade? Justify your answer.
8. **Medium** the binomial distribution $Bin(n = 10, p = 0.5)$, what is the probability that $k \notin \{\lfloor \frac{n}{3} \rfloor \dots \lceil \frac{2n}{3} \rceil\}$? Same question for $n = 100, 1000, 10000$. What happens for $n \to \infty$?

Entropy

9. [**Easy**] What is the entropy of the uniform distribution of size N, i.e. what is $H(\mathcal{U}_N)$?
10. **[Easy]** Let $n = pq$ be the product of two prime numbers p, q of 1024 bits each. (a) How many bits has n? (b) What is $H(p|n)$?
11. **[Medium]** In Monty's Hall, what is the participant's uncertainty before the show presenter opens one door? And afterwards? So how much information is communicated by opening the door?

Probabilistic complexity

12. **[Extra]** Find at least 3 different examples of a probabilistic algorithm. Try to find examples not mentioned in the book.