Quantum Information Theory (WiSe 2014/21015)

M Wilkens & Carsten Henkel

Problem Set No 1 ($40 + 2\pi$ scores)[1]

emission: 15.10.2014; absorption: 29.10.2014; digestion 30.10.2014

▷ Aufgabe 1 (Queen on board) — 1 score

To localize a single Queen on a 8×8 board of chess you need Y/N replies to

- ☐ $64/2 = 32$ questions on average
- ☐ $\sqrt{64} = 8$ questions
- ☐ exactly $\log_2(64) = 6$ questions

Remark: This is a classic which you are hopefully familiar with from your school-days ...

▷ Aufgabe 2 (Data base search) — 3 scores

To identify a single item in an unstrucured database which contains N items you need on average

- ☐ $N/2$ queries
- ☐ $\sqrt{N}$ queries
- ☐ $\log_2 N$ queries

Remark: It is like looking up the name in the white pages[2] if you only have the number ...

▷ Aufgabe 3 (Two fair dice) — 2 scores

In rolling a fair dice twice, it is

- ☐ more likely
- ☐ equally likely
- ☐ less likely

that the sum of the face values is as prime number than it being divisible by three.

---

[1] Problems with transcendental scores are facultative nuts. Nuts have high nutrition value ...

[2] "White pages" is colloqial for "Telephone Directory" (which is the same as a telephone book)

▷ Aufgabe 4 (Is this sequence random?) (6 scores)

Consider the list of bits given below. Could this be a sample from a random 0/1-source? Is there a reason to doubt that?

```
11000100000001011010101011110001101100110111101001101100011000101111111000000011110101101111111100101011100001111100110000010010 1
0110111111001010101110001010000101010100101010101011101001010000001110110111010110001110111101100011110000000110011010000110 01
10101111011010011100000011011111110010111111100111010100100000101000000101111010100111010001001110011000001000000000110111001 1001
0001011010000111001110110000000101110001001011101101010011010000000011011100000010101110011111101001011110000111111100100110101
01111111110000100111110010101111000011000100011110001000110100111000010110010110001100001110010100100100011101000110010110001
10010101011000100010101111101111000101000100011101101000100111110101010011001101000100010110101110110101100100010001010001011
101110110000100111100100110010011000001110011010110000110000001101010111111011111111111101011000001110001010101000110101000111
10110000110000110100101111010110100111001110100000110110011100110110100011111000110001101001010111010010100000111101111110011
10100100101011010011110011011010110000000101000011111010101000100110100111000000000000011001010011110101111000000001100011001000
0111010000111111101000000010101100011001110011000010010011011111011011110001011000110010000000000000010101100001111010001000000
0111010011010100001111000011011110101110100100011110111000101011010011100100001100000101010100101000000101100001000000000110000
00010010001001001100001100010000100110001010011011000010001000101010000101101110011011001011010011011100000111010101100100001
1101000100100000010100100010101010101000111010111010011000111000010010001111000000010101110000100011000110001100010111000010110
101001010100111000111100100011110000000000010110001110000110111010001100101010110010010100110101100101111100100011101110010000
000100011101000001111101000010001101010001010010011001101101101111010000011111010000000100000100010010100101000101001101101010
110000000100010000000110001011001111101000010001000101001010001110011001000110101001001111000011011010001111010000001001010100
```

▷ Aufgabe 5 (Landauer's Principle) (8 scores)

In the lecture you learned of the Landauer's Principle which states that the erasure of one bit of information inevitably generates heat $Q = k_{\mathrm{B}} T \ln 2$, where T is the temperature of the computing enviroment.

(a) Can you find a simple proof which is based on the elementary thermodynamics of a single particle ideal gas?

Now introduce Maxwell's Demon – a small measurement device which can first measure the bit value, and then – at no cost of energy and with no increase of the gas entropy – erases the bit value by putting the gas into a pre-defined "initial state".

(b) At first sight, Maxwell's Demon seems to contradict Landauer's Principle. Why?

(c) Yet the Maxwell's Demon in fact does not contradict the Landauer's Principle. Why not?

Hint: You may want to read the article by M.B. Plenio and V. Vitalli *The physics of forgetting: Landauers erasure principle and information theory*, Cont. Phys. **42**, 25–60 (2001).

▷ Aufgabe 6 (Berlin or Potsdam) (π scores)

Imagine yourself in any of two cities B or P, not knowing which city you are in. You know however, that all citizens of B are consistent liers, and all citizens of P are consistent in telling the truth. Unfortunately, citizens can freely commute between B and P, so its hard to tell whom you are talking to.

(a) What is your initial level of ignorance about the city you are in?

(b) How can you find out which city you are in?

(c) How can you find out whom you are talking to?

Analyse the complexity of you interrogation in terms of Shannon entropies.

▷ Aufgabe 7 (A simple compressor) (2 scores)

Can you design a scheme to compress the file

```
001000000000000000000000000000000000000000
000000101111111111111111111111111111111111
111111111111111111111111111111111111111111
```

Now comes pretty dry a problem set, yet the inequalities you prove here are sufficiently important for the theoretical foundations of information theory to deserve some sweat.

The Shannon needs no further comment. The Jensen is at the heart of many variational principles in physics, in particular statistical physics, where it reigns under the notion "mean-field approximation" (german: Molekularfeldnäherung).

The Markov serves as a basis for the Chebyshev which in turn serves as a basis for the weak law of large numbers – and this law is of paramount importance for everything – in particular the Shannon coding theorems ...

▷ Aufgabe 8 (Shannon Entropy) (6 scores)

Let $H(\mathbf{p}) := -\sum_{i=1}^{A} \log_2 p_i$ be the Shannon entropy of a memoryless source of an alphabet of A symbols. Furthermore $H(\mathbf{p}\|\mathbf{q}) := \sum_{i=1}^{A} p_i \log_s(p_i/q_i)$ the *relative entropy* of two probability distributions $\mathbf{p} = \{p_1, \ldots, p_A\}$, $\mathbf{q} = \{q_1, \ldots, q_A\}$ (also called *Kullback-Leibler divergence*).

Prove the following theorems

(a) The Shannon entropy is bounded

$$0 \leq H(\mathbf{p}) \leq \log_2 A\,. \tag{1}$$

(b) The Kullback-Leibler divergence obeys the *Gibbs inequality*

$$H(\mathbf{p}\|\mathbf{q}) \leq 0\,. \tag{2}$$

with equality if and only if $\mathbf{p} = \mathbf{q}$.

(c) The Shannon entropy is *concave* – that is for two probability distributions $\mathbf{p}$, $\mathbf{q}$ we have

$$H(\lambda\mathbf{p} + (1-\lambda)\mathbf{q}) \geq \lambda H(\mathbf{p}) + (1-\lambda)H(\mathbf{q})\,, \qquad 0 \leq \lambda \leq 1\,. \tag{3}$$

▷ Aufgabe 9 (Jensen's inequality) (3 scores)

Let F be a convex function of a real random variable X with $p(x)$ its probability distribution. Prove the Jensen's inequality

$$\langle F \rangle \geq F(\langle X \rangle)\,. \tag{4}$$

▷ Aufgabe 10 (Markov's Inequality) (3 scores)

For any non-negative random variable X and any $\alpha > 0$, show that

$$\mathrm{Prob}(X \geq \alpha) \leq \frac{\langle X \rangle}{\alpha} \tag{5}$$

▷ **Aufgabe 11 (Chebyshev's Inequality)** (3 scores)

Let X be a real random variable with finite mean $\bar{X} := \langle X \rangle$ and variance σ_X^2, and let α be a positive real number. Prove the Chebyshev inequality

$$\mathrm{Prob}([X - \bar{X}]^2 \geq \alpha) \leq \frac{\sigma_X^2}{\alpha}\,. \tag{6}$$

▷ **Aufgabe 12 (Weak law of large numbers)** (3 scores)

Let $X := \frac{1}{N}\sum_i Y_i$, where the Y_i are N independent random variables $Y_1, \ldots, Y_N$, having common mean $\bar{Y}$ and common variance σ_Y^2, . Then

$$\mathrm{Prob}((X - \bar{Y})^2 \geq \alpha) \leq \frac{\sigma_Y^2}{\alpha N} \tag{7}$$

Describe in words where – for N sufficiently large – the distribution of the X is concentrated, and what is it's width.

▷ **Aufgabe 13 (Benford's Law)** (π scores)

Look at the numbers in any newspaper, more specifically at all the numbers anywhere in the text, which are larger than 1000, and are *not* years, prices of goods in advertisements, or telephone numbers (but, for example, statistical data, like number of citizen in town etc). Take a note of the first digit of each number, and count the relative frequencies of the digits.

"Benford's Law" claims that the digit "1" appears in such an ensemble with frequency $\approx 30\%$, whereas "9" appears only with frequency $\approx 5\%$. Confirm and explain.

<u>Hint:</u> If you have no newspaper at hand, make the following experiment: think of a large number N (like $N = 277465890$); write down all numbers between 0 and N; determine the relative frequency of those numbers, whose leading digit is 1; repeat the experiment a couple of times (say 100 times) in order to accumulate some statistics. This should confirm the Benford law. But still – you have to think of an explanation ...