Quantum Information Theory (SS'06)

Problem Set No 1 ($20 + \pi$ scores)[1]

emission: 20.04.06; absorption: 11.05.06

▷ Aufgabe 1 (Berlin or Potsdam) (4 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 2 (Landauer's Principle) (6 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 3 (Shannon Entropy) (10 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

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

(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 4 (Decrypt this!)** (π scores)

As an inofficial employee of your countrie's special service you are of course well aware of the relative frequencies of the letters in English language documents (see Fig 1 for a reminder). Hence for you it is a piece of cake to decrypt the following cryptogram

```
,(flphjmkcfj,kslg-zdsfclzplvzcchj8vk,8zjl8
il,(k,lzpl-fg-zmhv8jalk,lzjflgz8j,lf8,(f-l
fnkv,selz-lkgg-zn8ck,fselklcfiikaflifsfv,f
mlk,lkjz,(f-lgz8j,qluvskhmfli(kjjzj.lwrt4o
```

which is known to be the result of a simple substitution cipher executed on an English text. What message did the sender of this cryptogram try to conceal?

Letter	Percentage	Letter	Percentage	Letter	Percentage	Letter	Percentage
a	5.75	h	3.13	o	6.89	v	0.69
b	1.28	i	5.99	p	1.92	w	1.19
c	2.63	j	0.06	q	0.08	x	0.73
d	2.85	k	0.84	r	5.08	y	1.64
e	9.13	l	3.35	s	5.67	z	0.07
f	1.73	m	2.35	t	7.06	-	19.28
g	1.33	n	5.96	u	3.34		

Abbildung 1: Distribution (percentage) over the 27 outcomes for a randomly selected letter in an English language document *The Frequently Asked Questions Manual for Linux*. Quoted after: David J.C. MacKay, Cambridge, UK.