Universität Leipzig
Institute of Computer Science
Winter term 2026/2027

Andreas Maletti

Exercises for the lecture

Cryptography

Solutions to Exercise Sheet 4

for the exercise on November 13th, 2026

Exercise 4.1

Decrypt this XOR of two ciphertexts from a one-time pad using the same key. Letters are encoded as alphabet positions as in Exercise 3.5. (will not be done during exercise)

```
AC_ZNXERMDL^22_78NCAYQ_^3_1AO^3_1EO^2_9TAUGPZCLTOFHRHO^2_9ZVF_E^2_9_ZB_LATCF^2_8MEND
WKBVKXQ_CIKTH^2_7ZSNNZYG^2_8ZDRLEPPTIBNA^2_7IQOWORAFA_GZDGTMMH^3_0__TQ_PEF
GAHNA__QMRMIICLSACEN^2_8CR_^3_0IRU_VELQUOE_RMIBCWZP^2_9MA_SAKMA^2_7DELFCOB
LEFK_^2_9-^2_8IA_^3_0MRHKOSAJCRT_DXPD_XMDWFORUBSHIQCDTC__O_GOMC^3_0NCTBTZD
IHA^2_9NCHCKEML_IJQ_HAJKGB^22_88G^2_7IGS_OTOTOSLVLKTAZK_XC_^2_8ET___GFZ^2_7L_K
KF^2_7Z__SZR_^2_8EPEOCMIGH_FMSAENCLFOQJ^3_1DMDNENQNDAVQLEBJELZ^2_8DL^3_1YECRA
^3_1TTXA^2_9CN_^2_7AYDFLLEHMSCTAJFFTB^2_7X^2_7YHVY^2_9GUOMBASIODFEWMEIERFWPOMJDA
JPGIY^3_0BABWATVLTPK^2_9GOHN^3_0_DTJGTDUQDMIT^3_1JLLERMOAPIRJRT^2_8ZNMYD_^22_78UU
FUKKT^2_9GJBRBLJQHTQNA_UR^2_8HPIUDMM_^3_0QABDT_LA_SZDOEAEMON^2_7LVEAOCAHBL
F^2_7OLMDKN_HSV^2_8I^2_9FWT_HY_UTZDQZLWGAGU__BWOD^2_7X^2_7CAYWD^2_9THREXHBQAHJVC
O^2_7TAZE_^2_7TTHO^2_9FFN^3_1OH^2_9HLE_Z_^2_7JXKESHFBQRBNPAEMHHXT^2_7MIYNAHDHVNLW__
IX^2_9FIZOEIDRH^3_0LS^2_9PV__SL^3_0__QJUS_TJQTW^2_8GI^3_1OCFAIAZOSG^2_9CB_U^2_8A^2_8EZA_B
_^2_9_VVQ^2_9SMCEDFOAFA_KSR_EE^23_90IGQLS
```

(Ciphertext available as bit sequence on my website)

Solution: The two original messages are excerpts from Lessing's "Nathan the Wise" and Salinger's "Catcher in the Rye".

Exercise 4.2

Which of the following functions are negligible? Justify your answer!

(a) $(2^{-n})_{n\in\mathbb{N}}$

(b) $(2^{-\sqrt{n}})_{n\in\mathbb{N}}$

(c) $(n^{-\log n})_{n\in\mathbb{N}}$

(d) $(n^{-2})_{n\in\mathbb{N}}$

(e) $(1.01^{-n})_{n\in\mathbb{N}}$

Solution: To prove that a function $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ is negligible we have to prove the following. Given any positive (univariate) polynomial p there exists $n_0 \in \mathbb{N}$ such that $f(n) < p(n)^{-1}$ for all $n \geq n_0$. In other words, (assuming that our function f is monotonically decreasing, which is usually the case) from a certain point n_0 onwards, our function needs to converge towards 0 faster than the inverse of any given polynomial p. The starting point n_0 may depend on the given polynomial p. This kind of definition should remind you of the big-O notation, so we use the same proof techniques here.

For all of the following cases, let p be any positive polynomial. To prove negligibility we demonstrate that

$$\lim_{n\to\infty} f(n) \cdot p(n) < 1 \ .$$

Indeed we must even have $\lim_{n\to\infty} f(n) \cdot p(n) = 0$. This can be seen as follows. Suppose that $\lim_{n\to\infty} f(n) \cdot p(n) = \epsilon$ with $0 < \epsilon < 1$. Then we consider the polynomial $p' = \epsilon^{-1} \cdot p$ (multiplication of the polynomial p by the scalar ϵ^{-1}) and compute

$$\lim_{n\to\infty} f(n) \cdot p'(n) = \lim_{n\to\infty} f(n) \cdot \epsilon^{-1} \cdot p(n) = \epsilon^{-1} \cdot \lim_{n\to\infty} f(n) \cdot p(n) = \epsilon^{-1} \cdot \epsilon = 1 \ ,$$

which would prove that f is <u>not</u> negligible. So we prove that

$$\lim_{n\to\infty} f(n) \cdot p(n) = 0$$

for any positive polynomial p to prove that f is negligible.

(a) In this case we need to prove

$$\lim_{n\to\infty} \frac{p(n)}{2^n} = 0$$

The easiest way to prove this are finitely many applications of l'Hôpital's rule (so formally we would need induction since we would need to prove it for any degree of the polynomial p). L'Hôpital's rule essentially states how to compute limits $\lim_{n\to a} \frac{f(n)}{g(n)}$ of fractions of functions that are differentiable (in an open interval I around a, except possibly at a). Moreover, we need to have $g(n) \neq 0$ for suitably many n around a (formally, for all $n \in I \setminus \{a\}$) and $\lim_{n\to a} f(n) = \lim_{n\to a} g(n) \in \{0, \infty\}$; i.e., both numerator and denominator individually diverge to ∞ or both converge to 0. Then

$$\text{if} \quad \lim_{n\to a} \frac{f'(n)}{g'(n)} \quad \text{exists, then} \quad \lim_{n\to a} \frac{f(n)}{g(n)} = \lim_{n\to a} \frac{f'(n)}{g'(n)} \ .$$

In other words, given these restrictions (which we typically fulfill) we can simply replace enumerator and denumerator by their respective derivative.

Returning to our actual limit, we obtain

$$\lim_{n\to\infty} \frac{p(n)}{2^n} = \lim_{n\to\infty} \frac{p'(n)}{2^n \cdot \ln 2} = \lim_{n\to\infty} \frac{p''(n)}{2^n \cdot (\ln 2)^2} \cdots = \lim_{n\to\infty} \frac{p^{(\deg p)}(n)}{2^n \cdot (\ln 2)^{\deg(p)}} = 0$$

as required because $p^{(\deg(p))}$ (the $\deg(p)$-th derivative of polynomial p) is a constant. Hence the function $(2^{-n})_{n\in\mathbb{N}}$ is negligible.

(b) In this case we prove that

$$\lim_{n\to\infty} \frac{p(n)}{2^{\sqrt{n}}} = 0 \ .$$

As before the numerator will be constant after $\deg(p)$ applications of l'Hôpital's rule. It remains to determine the derivative of $2^{\sqrt{n}}$. Recall that $\sqrt{n} = n^{\frac{1}{2}}$. Applying the chain rule we obtain the first derivative $2^{\sqrt{n}} \cdot \ln 2 \cdot \frac{1}{2} n^{-\frac{1}{2}} = \frac{2^{\sqrt{n}} \cdot \ln 2}{\sqrt{n}}$ and the second derivative also utilizing the product rule

$$2^{\sqrt{n}} \cdot (\ln 2)^2 \cdot \left(\frac{1}{2} n^{-\frac{1}{2}}\right)^2 + 2^{\sqrt{n}} \cdot \frac{1}{2} \cdot \left(-\frac{1}{2} n^{-\frac{3}{2}}\right) = \frac{2^{\sqrt{n}-2} \cdot \ln 2 \cdot (\sqrt{n} \cdot \ln 2 - 1)}{\sqrt{n^3}} \ .$$

Since the exponential will not vanish (no matter how many derivatives are taken) and all those derivatives tend to ∞ as $n \to \infty$ (another nice exercise), we obtain that $(2^{-\sqrt{n}})_{n\in\mathbb{N}}$ is negligible. A faster way to prove this would be

$$\lim_{n\to\infty} \frac{p(n)}{2^{\sqrt{n}}} = 0 \qquad \text{iff} \qquad \lim_{x\to\infty} \frac{p(x^2)}{2^x} = 0 \ ,$$

where $x = \sqrt{n}$. The right-hand side equation can be shown as in (a) since $p(x^2)$ is just another polynomial.

(c) Let us fix a base b for the logarithm. Then

$$\lim_{n\to\infty} \frac{p(n)}{n^{\log_b n}} = \lim_{n\to\infty} \frac{p(n)}{\left(\mathrm{e}^{\ln n}\right)^{\log_b n}} = \lim_{n\to\infty} \frac{p(n)}{\mathrm{e}^{(\ln n)^2/\ln b}} = 0$$

because the derivative of $\mathrm{e}^{(\ln n)^2/\ln b}$ is

$$\mathrm{e}^{(\ln n)^2/\ln b} \cdot \frac{2}{\ln b} \ln n \cdot \frac{1}{n} = 2\log_b n \cdot n^{\log_b n - 1}$$

and the second derivative is

$$\begin{aligned} & 2\log_b n \cdot \frac{1}{n} \cdot \left(2\log_b n \cdot n^{\log_b n - 1}\right) + n^{\log_b n}\left(\frac{2}{n \ln b} \cdot \frac{1}{n} - 2\log_b n \cdot \frac{1}{n^2}\right) \\ &= 4(\log_b n)^2 \cdot n^{\log_b n - 2} + \left(\frac{2 \cdot (\ln b)^{-1} - 2\log_b n}{n^2}\right) \cdot n^{\log_b n} \\ &= 2\Big(2(\log_b n)^2 + (\ln b)^{-1} - \log_b n\Big) \cdot n^{\log_b n - 2} \ . \end{aligned}$$

Continuing this we note that these derivatives will always tend to ∞ as $n \to \infty$, whereas, as usual, the enumerator $p(n)$ becomes constant in the $\deg(p)$-th derivative. Hence $(n^{-\log_b n})_{n\in\mathbb{N}}$ is negligible.

A faster method is available here as well.

$$\lim_{n\to\infty} \frac{p(n)}{n^{\log_b n}} = \lim_{n\to\infty} \frac{n^{-\deg(p)} \cdot p(n)}{n^{\log_b n - \deg(p)}} = 0$$

because the numerator now converges to a constant (namely the leading coefficient of p), whereas the denominator still diverges to ∞.

We note here that if we instead consider the function $(a^{-\log_b n})_{n\in\mathbb{N}}$, in which we replaced the base n by some constant $a \in \mathbb{N}$, then

$$a^{\log_b n} = a^{\log_a n / \log_a b} = \left(a^{\log_a n}\right)^{1/\log_a b} = n^{1/\log_a b} = \sqrt[(\log_a b)]{n}$$

so this function is clearly dominated by a polynomial, which proves that $(a^{-\log_b n})_{n\in\mathbb{N}}$ is <u>not</u> negligible.

(d) The function $(n^{-2})_{n\in\mathbb{N}}$ is clearly not negligible. We select the polynomial n^3 and compute

$$\lim_{n\to\infty} \frac{n^3}{n^2} = \lim_{n\to\infty} n = \infty \ ,$$

which proves that $(n^{-2})_{n\in\mathbb{N}}$ is <u>not</u> negligible.

(e) The function $(1.01^{-n})_{n\in\mathbb{N}}$ is negligible. The proof is analogous to the proof of (a) with each occurrence of base 2 replaced by the new base 1.01.

Exercise 4.3

Let $f, g\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be any negligible functions, $h\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be any function, and p be any positive polynomial. Prove or refute for each of the following functions that it is negligible:

(a) $f + g$ and $f \cdot g$
(b) $f + h$ and $f \cdot h$
(c) $f + p$ and $f \cdot p$

Solution:

(a) Let p' be any positive polynomial. The function $f + g$ is again negligible.

$$\begin{aligned}\lim_{n\to\infty} (f+g)(n)p'(n) &= \lim_{n\to\infty} \big(f(n)+g(n)\big)p'(n) = \lim_{n\to\infty} \big(f(n)p'(n) + g(n)p'(n)\big) \\ &= \Big(\lim_{n\to\infty} f(n)p'(n)\Big) + \Big(\lim_{n\to\infty} g(n)p'(n)\Big) = 0 + 0 = 0 \ ,\end{aligned}$$

where the individual limits follow from the negligibility of f and g. Similarly, the function $f \cdot g$ is again negligible.

$$\begin{aligned}\lim_{n\to\infty} (f\cdot g)(n)p'(n) &= \lim_{n\to\infty} f(n)g(n)p'(n) \\ &= \Big(\lim_{n\to\infty} f(n)p''(n)\Big) \cdot \Big(\lim_{n\to\infty} g(n)p'(n)\Big) = 0 \cdot 0 = 0 \ ,\end{aligned}$$

for the polynomial $p'' = 1$, where the individual limits follow from the negligibility of f and g.

(b) The functions $f + h$ and $f \cdot h$ need not be negligible. Select $f = (2^{-n})_{n \in \mathbb{N}}$ as negligible function and the constant function $h = 1$. Then we have $(f + h)(n) = f(n) + 1$ and thus $(f + h)(n) \geq 1$ for all $n \in \mathbb{N}$. Consequently $(f + h)$ is not negligible (is not eventually dominated by the inverse of the constant-1 polynomial). For the result on the product, we select the function $h = f^{-1}$. Then $(f \cdot h)(n) = f(n) \cdot h(n) = 2^{-n} \cdot 2^n = 1$ for all $n \in \mathbb{N}$, so $(f \cdot h)$ is not negligible (is not eventually dominated by the inverse of the constant-1 polynomial).

(c) The function $f + p$ need not be negligible. Select $f = (2^{-n})_{n \in \mathbb{N}}$ as negligible function and the constant function $p = 1$ (as before since it happens to be a positive polynomial). Then we have $(f + p)(n) = f(n) + 1$ and thus $(f + p)(n) \geq 1$ for all $n \in \mathbb{N}$. Consequently $(f + p)$ is not negligible (is not eventually dominated by the inverse of the constant-1 polynomial). However, $f \cdot p$ is again negligible, which we prove as follows. Let p' be any positive polynomial.

$$\lim_{n \to \infty} (f \cdot p)(n) p'(n) = \lim_{n \to \infty} f(n) p(n) p'(n) = \left(\lim_{n \to \infty} f(n) p''(n) \right) = 0 \ ,$$

where the last equality follows from the negligibility of f using the polynomial $p'' = p \cdot p'$.