Chair of Network Architectures and Services
School of Computation, Information, and Technology
Technical University of Munich

Note:

- During the attendance check a sticker containing a unique code will be put on this exam.
- This code contains a unique number that associates this exam with your registration number.
- This number is printed both next to the code and to the signature field in the attendance check list.

Basics of TUMexam

Exam:	IN0000 / Endterm	**Date:**	Saturday 1st January, 2022
Examiner:	Prof. Dr.-Ing. Georg Carle	**Time:**	13:00 – 14:00

P 1	P 2	P 3	P 4	P 5	P 6	P 7	P 8	P 9	P 10

Working instructions

- This exam consists of **20 pages** with a total of **10 problems**.
  Please make sure now that you received a complete copy of the exam.

- The total amount of achievable credits in this exam is 92 credits.

- Detaching pages from the exam is prohibited.

- Allowed resources:

  - one **non-programmable pocket calculator**

  - one **analog dictionary** English ↔ native language

- Subproblems marked by * can be solved without results of previous subproblems.

- **Answers are only accepted if the solution approach is documented.** Give a reason for each answer unless explicitly stated otherwise in the respective subproblem.

- Do not write with red or green colors nor use pencils.

- Physically turn off all electronic devices, put them into your bag and close the bag.

Left room from _____	to _____	/	Early submission at _____	

Problems

Problem 1   Changelog (0 credits)

WiSe 2022

- Data Matrix generation now relies von `dmtxwrite` and `imagemagick`. If not installed, placeholders will be generated.

- The template now checks for invalid calculation functions in MC problems and invalid decimal seperators for credits.

SoSe 2022

- As the template is now available under LPPL, the possibility to include custom organization names and logos has been added. See `conf/organization.tex` for details.

- New macros for randomization have been added, which also workaround some bugs with `pgfmath`. See Section 8 for details.
  You may, however, still use `pgfmath` directly provided that you do not re-initialize its pseudo random number generator. The template ensures that randomization is deterministic accross builds.

WiSe 2021

- **Important:** Older versions of the template are **incompatible** with `2021ws` instances due to changes in `conf/examconf.sty`. Please make sure to use this version of the template with instances created for `2021ws`.

- Removal of `tumlang.tex`

  - So far, we had to include your organization in the template upon request. Afterwards, you were able to choose your organization by calling `\organization` with the correct parameter.

  - From now on you may set your department, chair, and examiner explicitly in `conf/examconf.sty` (or preferably using the web interface). The web interface will also offer autocompletion based on previously entered values.

- Moved `examconf.tex` to `conf/generated/examconf.tex` as it is considered read only. Do not change this file anymore directly but use the web interface to update an exam's settings. Manual changes will be ignored by the web interface.

- Working instructions on the title page can now be fully customized by editing `conf/examnotes.tex` and `conf/toolsallowed.tex` – the latter being also included in examination protocols. Web users may edit those file in the web editor.

- Removed department logos since the new schools do not have logos anymore.

- Added macro `\textboxinput[width]{height}{solution}` to place an invisible text box with optional solution text. Default width is `\textwidth`. Primarily meant for remote exams with keyboard input outside of regular solution boxes, e. g. within figures or tables.

- Fixed a bug that did not show the ERID of a printable exam in the student sticker box.

Problem 2 General Configuration (9 credits)

The general configuration for an exam is made in the file conf/generated/examconf.tex. **You should never change this file by hand.** Set the options in the webinterface instead and clone or download the template.

a) Specify the title of your exam. That commonly refers to the lecture to which the exam belongs.

```
\title{Basics of TUMexam}
```

b) Specify the type of your exam, e. g. Endterm, Retake, Modulprüfung.

```
\type{Endterm}
```

c) Set your module number, normally a code consisting of two letters and four to five digits.

```
\module{IN0000}
```

d) Specify the date of your exam (day, month, year).

```
\date{1}{2}{2016}
```

e) Specify the begin and end times of your exam.

```
\starttime{13:00}
\stoptime{14:00}
```

f) Choose the language (english or german).

```
\lang{english}
```

g) Set the department.

```
\examiner{\department}
```

h) Set the chair.

```
\examiner{\chair}
```

i) Set the examiner.

```
\examiner{\chairhead}
```

Problem 3 Advanced Configuration (18 credits)

There are a lot more configuration options provided in `conf/generated/examconf.tex`. **You should never change this file by hand.** Set the options in the webinterface instead and clone or download the template.

a) Specify whether this exam is a submission, i. e., an exam written remotely and submitted online.
Note: This option cannot be changed after an exam has been created in the webinterface, which is why this option will be overwritten when pushing or uploading the template.

☐ `\submissiontrue`

☒ `\submissionfalse`

b) State if you want to have one or two correction passes.
Note: The second pass is obligatory because otherwise TUMexam could not differentiate between an intentionally omitted and by accident not detected second pass.
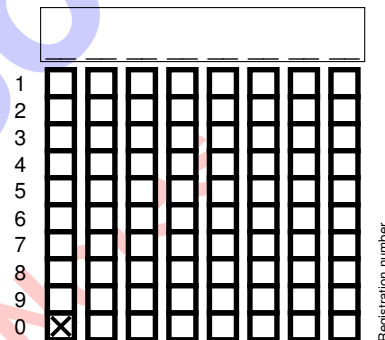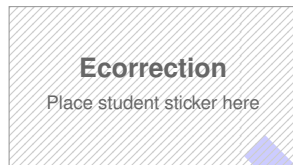
☒ `\singlepassfalse` (two correction passes)

☐ `\singlepasstrue` (one correction pass)

c) State if you want to give half credits.

☐ `\halfcreditsfalse`

☒ `\halfcreditstrue`

d) Registration stickers vs. registration boxes:

☐ `\registrationstickerfalse` (no stickers but boxes)

☒ `\registrationstickertrue` (stickers)

Of course, TUmexam also supports registration boxes as alternative to registration stickers. However, we urge you to use the registration stickers whenever possible. The reasons are:

1. With the sticker sheets we provide there is no additional overhead compared to printing ordinary attendee lists without stickers.

2. It seems to be a tough task for our students to correctly mark their registration number in the box (in particular whether to start counting at 0 or 1).

3. If 5 % of your students do not get their registration number correctly marked, and you have 1000 participants, do the math of manually fixing registration numbers.

4. Of course, that is only a hassle, provided that students follow requests and write their registration number as digits in the headline of the box (and if they do, given that you can read it . . .).

5. However, most important, a student might accidentally hit the registration number of another student that is registered to the exam but does not show up. That case cannot be detected and the the exam is assigned to the wrong student!

In contrast, registration stickers are virtually fail-proof.

e) If you want to create your problem sheet separate from the answer sheet, then you may need this option. Seperate answer sheets may ease your decision regarding the online exam review as the problems are not made available to students after the exam, only their answers. Please contact us for details.

☒ \externalproblemsfalse

☐ \externalproblemstrue

f) State if you want an additional cover sheet. We discourage the use as it increases the print times due to the additional envelope per exam.

☒ \coversheetfalse

☐ \coversheettrue

g) Specify how your exam should be printed and stapled.

☐ \onestaple (one staple at the top left corner)

☐ \nostaple (only useful if there is only one sheet)

☒ \booklet (a booklet)

h) Specify if you want serif font or the TUM corporate design font Helvetica.

☐ \seriftrue

☒ \seriffalse

i) Specify if you want arabic numbering of subproblems.

☐ \subproblemarabictrue

☒ \subproblemarabicfalse

j) Do not show the amount of credits per problem.

☐ \noproblemcreditstrue

☒ \noproblemcreditsfalse

k) Remove the problem heading. This option is useful only if your exam consists of a single problem with multiple subproblems, e.g. quizze and surveys.

☐ \noproblemtrue

☒ \noproblemfalse

l) Remove the title section from the first page. This option is useful for very compact exams, quizze, or surveys.

☐ \notitletrue

☒ \notitlefalse

m) The title page of an exam has a rectangular corrector box per problem and per correction pass. It is meant solely as a signature field for correctors to indicate whether or not and by whom a specific problem has been corrected. If you do not want those boxes for some reason, e.g. you have so many problems that the boxes do not fit into a single line, you may remove them using this option.

☐ \nocorrectorboxtrue

☒ \nocorrectorboxfalse

n) Enable if you want to print single-sided exams. This may be usefull if in combination with the \onestaple option. The backsides will still have pagecodes, which is important for scanning as we cannot prevent students from writing something on the backsides. Do **not** use this option together with \coversheettrue.

☐ \singlesidetrue

☒ \singlesidefalse

Some texts can be modified as follows.

o) Allowed tools

0
1

The allowed tools can be modified in conf/toolsallowed.tex.
If no tools are allowed, you should explicitly state that.

p) Announcement of tools

0
1

In conf/toolsannouncement.tex you can state where you announced the allowed tools.

q) Notes on the exam title page

0
1

Additional notes on the exam title page can be configured in conf/examnotes.tex.

r) Notes on the binder (PDF for archiving / online review)

0
1

Additional notes on the binder can be configured in conf/bindernotes.tex.

Problem 4 Building (11 credits)

The template depends on an up to date version of texlive-full and GNU make to build everything you need for your exam. Please note that using an IDE for LaTeX documents such as TeXstudio is not explicitly supported, but possible for the most part if you correctly setup the directories from which class and style files are loaded.

The first part of make commands is used during exam creation, i. e., before building the final exam copies, attendee lists, seatplans, and protocols.

Hint: For answers to the following questions, build a solution with correction notes of this exam using `make correction`.

a) How is the exam itself built?

```
make  or  make exam
created documents: exam.pdf
```

b) How is the solution built? (See Subproblem h) for individual solutions)

```
make solution
created documents: exam-solution.pdf
```

c) How is the annotated solution containing all correction notes built?

```
make correction
created documents: exam-correction.pdf, exam-correction-book.pdf
```

d) How is an example exam with page codes as it is printed built?

```
make example
created documents: exam-example.pdf, exam-example-book.pdf
```

e) How is a side by side version of the exam and the annotated solution built?

```
make hud
created documents: hud.pdf
```

f) How are all of the above documents built?

```
make all
```

The second part of make commands is used to create the documents for printing. Note that some of the documents need additional data that is usually not available on your local computer, such as a list of rooms, distribution of students to rooms etc.

g) How are all of the individual exams built?
Hint: EXAMCOUNT is set to the number of copies required.

```
make EXAMCOUNT=10 examids
created documents: exam-out/Exxxx.pdf, exam-out/Exxxx-book.pdf
created metadata: exam-out/Exxxx-pages.csv, exam-out/Exxxx-boxes.csv
```

h) How are all of the individual solutions built?
Hint: EXAMCOUNT is set to the number of copies required.

```
make EXAMCOUNT=10 solutionids
created documents: solution-out/Exxxx-solution.pdf
```

i) How are all of protocol, attendeelist, etc. built?
Note: these targets can only be built if the respective metadata is available, which is commonly not the case on your local machine. The targets are built on the server and can be downloaded from there.

```
make print
created documents: print/attendeelist.pdf,
print/protocol.pdf, print/protocol-signature.pdf,
print/seatplan.pdf, print/seatplan-a3.pdf,
print/roomplan.pdf, print/packing.pdf
```

j) How is all the remaining metadata that is needed for scanning built?

```
make scan
created metadata: scan/scanconf.yml,
scan/srids.csv, scan/problems.csv, scan/boxes.csv,
scan/problemboxes.csv, scan/registrationboxes.csv,
scan/attendeelistpages.csv, scan/protocolpages.csv
```

k) How can we speed up the building of exams?

Specify the number of threads to use, e.g. make -j 16. Note that our Makefile also builds external TikZ figures in the subfolder "figures" in parallel.

Problem 5 Some background on how TUMexam works (14 credits)

In the following we discuss some more background regarding the TUMexam LaTeX template. This understanding will prevent you from some pitfalls that users sometimes encounter.

a)* The instruction box below contains a page code which is typeset three times on every page of a printable exam copy. Which information is contained in such a code?

IN-BT-1-20200101-E0001-01

<department>-<instance>-<exam_id>-<date>-<ERID>-<page>

- department: short name of department, e.g. IN for Informatics; defined by by \organization
- instance: short name of your instance, chosen when creating an instance and also part of the URL of your instance
- exam_id: integer value representing the exam (primary key in database)
- date: date of your exam in the format yyyymmdd
- erid: ERID (Exam Relative Identifier) representing a specific exam copy, unique to each printed copy
- page: page number within an ERID

b)* Is it neccessary that all page codes can be read.

No.
A single page code is sufficient such that a scanned page can be associated with an exam. However, TUMexam aligns scanned pages (deskews the scan) to perfectly detect cross boxes. This step is vital and works best if one of the codes at the bottom and the code at the top of a page is detected. Depending on which codes are detected, alignment may be suboptimal.

c)* What happens if an ERID is printed twice?

We end up with duplicate page codes, which cannot be processed.
The only possible recovery is to remove all page codes from one exam and note an unused ERID on each page by hand. This results in error pages during processing for which we can manually enter valid, unique page codes.

d)* Can additional pages, e.g. scratch paper, be added to an exam?

Yes, but it is not recommended: we can note the ERID to which the paper belongs and a sequential page number on each *side* (front and back). Those pages will be reported as error pages during processing and can then be added to the correct ERID.

e)* The first page of a printable exam copy (one with page codes) contains a box named "Exam empty" in the footline, all other pages have a box named "Page empty". What are these boxes used for?

Marking one of those boxes declares the whole exam or the respective page as being empty, i.e., credit boxes are set to zero without needing to cross all boxes.
Be carefull when using the "Page empty" box as it may happen that you accidentally set the credits for a subproblem to zero if the solution for that subproblem is not on the same page as the credit box, e.g. subproblems of the form "mark somehting in Figure ..." with the figure being on a different page.

Problem 6   Creating problems (8 credits)

This section describes how the problems of an exam are created. It is advisable to not only read this document, but also have a look at the source code of the sample problems.

Hint: Problems that can be solved without solving previous subproblems first are marked by *. (It is up to you whether or not you want to tell that your students, but if you do, please do it carefully.)

0
1

a)* First, we need to declare a problem.

```
\problem{The problem title}
Here afterwards, we can insert arbitrary material like text or pictures.
```

0
1

b) Then, we need to declare the subproblems.

```
\subproblem{1}   or   \subproblem*{1}
The argument (number) is the amount of credits for the subproblem.
The star-version just creates a star next to the subproblem number. This could e. g. indicate
subproblems wich are solvable independently.
```

There are different environments to create solutionboxes.

0
1

c) How can we define a normal solutionbox of 3 cm in height?

```
\begin{solutionbox}[3cm]
This is the solution.
\end{solutionbox}

The optional argument specifies the height of the solutionbox.
```

0
1

d) How can we annotate the solution with correction notes?

```
\credit  ✓

\hcredit ✓

\correction{ This is a correction note. }
```

0
1

e) How can we define a solutionbox with instructions?

```
\begin{instructionbox}
This is instructiontext, e.\g. a table preprint
\solution{

This is the solution.

}
\end{instructionbox}

Note: instructionboxes allow no text input in the PDF as it would interfere with instructions
```

f) How can we define a solutionbox with gridlines?

```
\begin{gridsolutionbox}
This is the solution.
\end{gridsolutionbox}
```

g) How can we define a solutionbox with grid and instructions?

```
\begin{gridinstructionbox}
This is instructiontext, e.\g. a table preprint
\solution{

This is the solution.

}
\end{gridinstructionbox}
```

Note: instructionboxes allow no text input in the PDF as it would interfere with instructions

h)* „Ich bitte Sie, das neue Corporate Design konsequent umzusetzen. Sehen Sie darin eine Loyalitätspflicht der Hochschulmitglieder, damit sich der Hinweis auf die Rechtsverbindlichkeit erübrigen kann."[1]

For that reason, TUMexam is based on Helvetica, and we do our best to convince you of Helvetica–even in math mode:

mathnormal	$abcdefghhjkklmnopqrstuvwxyz$
	$ABCDEFGHJKLMNOPQRSTUVWXYZ$
	1234567890
	$\alpha\beta\gamma\delta\epsilon\zeta\eta\theta\kappa\lambda\mu\nu\xi\pi\rho\sigma\tau\phi\chi\psi\omega$
	$\Delta\Theta\Lambda\Pi\Phi\Psi\Omega$
mathbit	$\boldsymbol{abcdefghjklmnopqrstuvwxyz}$
	$\boldsymbol{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$
	$\boldsymbol{01234567890}$
	$\boldsymbol{\alpha\beta\gamma\epsilon\zeta\eta\theta\kappa\lambda\mu\nu\xi\pi\rho\sigma\tau\phi\chi\psi\omega}$
	$\boldsymbol{\Delta\Theta\Lambda\Pi\Phi\Psi\Omega}$
mathcal	$\mathcal{ABCDEFGHIJKLMNOPQRSTUVXYZ}$
symbols	$\sum_{n=1}^{N}\frac{N(N-1)}{2}, \quad \frac{1}{2\pi}\int_{-\infty}^{\infty}f(x)e^{-j\omega t}\,\mathrm{d}t$
addons	$\Pr\left[X=x\mid Y=y\right], \mathrm{Var}\left[x\right], \mathrm{E}\left[X\right]$

If you plan to disobey this request, you may use computer modern instead by setting \seriftrue in examconf.tex.

---

[1]Wolfgang A. Herrmann, Corporate Design Handbuch 2016

Problem 7   Multiple choice problems with TUMexam (7 credits)

TUMexam supports the automatic evaluation of multiple choice problems (both single and multiple answer) through so called *calculation functions* that are supplied as optional argument to the \subproblem macro.

a) How can we define a multiple choice question?

☐ \subproblem{<max_credit>} This does not work as it would be a normal subproblem.

☒ \subproblem[<calculation_function>]{<max_credit>}
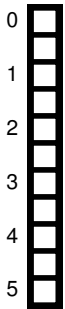
b) What are the available calculation functions?

0
1
2
3
4
5

- mc
  Every correct cross gives +1 credit, every incorrect cross gives -1 credit. Missing crosses do not count. The lowest possible amount of credits is 0. If the specified maximum credits do not equal the number of correct answers, credits are scaled by the factor max_credit/correct_options. You **must** ensure that this fraction is a multiple of 0.5 credits.

- strict_mc
  Works the same way as mc, but a missing cross also gives -1 credit.

- binary_mc
  Gives the specified maximum amount of credits if everything is correct and 0 credits otherwise.

- ternary_mc
  The subproblem gives the specified amount of credits if everything is answered correctly. If there is exactly one cross missing *or* one wrong answer crossed, the resulting amount of credits is max_credit/2. Otherwise, the amount of credits is 0.

  Note that in a problem with two correct options, crossing one correct and one incorrect answer gives 0 credits since aside from the incorrect answer there is also one correct answer missing.

- per_option_mc
  In this case, each answer option is graded individually depending on whether its state (crossed or not crossed) is correct. You **must** set the maxmimum number of credits to be a multiple of the total number of options, e. g. having 5 options leaves you with 5, 10, 15, . . . as possible values. Each option with correct state is than awarded 1, 2, 3, . . . credits.

  Example: A question with 2 correct options out of 5 options in total and a max_credit of 5 would give 3 credits (!) if a student simply crosses nothing since in that case 3 options are "correctly not crossed". If max_credit is set to 10, the result would be 6 credits in this example.

c) What is the command to typeset instructions on how to mark correct answers?

Mark correct answers with a cross ☒

To undo a cross, completely fill out the answer option ■

To re-mark an option, use a human-readable marking ✕■

☐ \makenotes{}

☐ \notesmc{}

☒ \mcnotes{}

☐ \makemc{}

Problem 8   Randomization of problems (8 credits)

The TUMexam LaTeX template offers a broad range of options to randomize problems. There are only two limitations to what is allowed: each random version of a (sub)problem must

- have the same number of credits and
- be located on the same page.

Virtually all functionality for randomization is provided through pgfmath. The TUMexam LaTeX template adds a few convenience macros to extend pgfmaths functionality and passes a seed value to pgfmaths pseudo random number generator. This seed is either the ERID (exam number) or the magic number 42 in case of example builds – which is very important to allow for deterministic builds of exams.

Now, let's see how that works . . .

a)* This is only an example of a multiple choice subproblem . . .

☐ Option 4   ☒ Option 1   ☐ Option 3   ☐ Option 2

b)* How to create different permutations of Subproblem a)?

☐ 0
☐ 1

Please see Subproblems 3g) and h) to learn how to build variants of exams and solutions. See Subproblem a) in the resulting PDFs. The answer options are permuted by default. If you do not want to permute MC answer options, use the starred environment of `multiplechoice`.

c)* How to get a random integer from the range {0,1,...,42}?
Hint: TUMexam defines `\randinteger`.

☐ 0
☐ 1

`\randinteger{\myrandomint}{0}{42}` randomly assigns the value 12 to the macro `\myrandomint`.

d)* How to define a list of elements and retrieve a random element from that list?
Hint: TUMexam defines `\randitem`.

☐ 0
☐ 1

```
\pgfmathdeclarerandomlist{myrandomlist}{{item 1}{item 2}{item 3}{item 4}}
\randitem{\myrandomitem}{myrandomlist}
\myrandomitem
```

`\myrandomitem` evaluates to "item 2".

e)* When multiple lists are in use at the same time, `\randitem` creates all possible combinations. How do you link the selection of two items from two lists?
Hint: TUMexam defines `\randitemsameindex`.

☐ 0
☐ 1

```
\pgfmathdeclarerandomlist{myfirstrandomlist}{{A}{B}{C}{D}{E}}
\pgfmathdeclarerandomlist{mysecondrandomlist}{{a}{b}{c}{d}{e}}
\randitem{\myfirstrandomitem}{myfirstrandomlist}
\randitemsameindex{\mysecondrandomitem}{mysecondrandomlist}
```

`\randitemsameindex` chooses the item with the same index as the previous `\randitem`. If, for example, `\myfirstrandomitem` evaluates to "C", `\mysecondrandomitem` would have to evaluate to "c". This could be useful if you have a list of values and another list with the corresponding solutions, for example.

0
1

f)* All random values generated with the above macros are placed into the LaTeX logfile so that the corrector can search for an exam another student may have copied from. How can you extract this data into a CSV?

```
grep -h 'Randomized values CSV row' build/exam.tex/*/*.log |
    cut --bytes=28- | iconv -f LATIN1 >values.csv
```

If you want to explicitly log any additional (e. g. dynamically calculated) values, you can use \randitemlog{}.

Note: The macros generated are printed in red in the correction notes so that the correctors immediately know what to look for. This has the drawback that they may contain a \color{red}, which may be unsuitable if you need the raw value, e.g. for \pgfmathparse, \SI, or \ifnum.
For those cases, all aforementioned randomization macros also define a second macro (which simply has uncolored appended to its name) that contains the raw value.

And here comes an example of a problem with randomized values:

0
1
2

g)* Given a channel with a bandwith of 30 MHz. Derive the signal-to-noise ratio in dB such that a rate of 11 Mbit/s is possible.

$$r = B \log_2(1 + \text{SNR}) \Rightarrow \text{SNR} = 2^{(r/B)} - 1 \approx -5.39\,\text{dB}$$

Important: be very carefull with such random inputs for calculations due to limited value range and precision!

Problem 9 Single stream point-to-point MIMO on multiple carriers (4 credits)

We consider the communication scenario in Figure 9.1 where multiple data streams s_k are transmitted on K subcarriers, one stream per carrier. The signals s_k are mutually independent and Gaussian distributed with zero mean and unit variance, i.e., $s_k \sim \mathcal{N}_\mathbb{C}(0,1)$. The transmitter and receiver have N and M antennas, respectively. The signal s_k denotes the data stream transmitted on carrier k which is precoded with $\boldsymbol{p}_k \in \mathbb{C}^N$
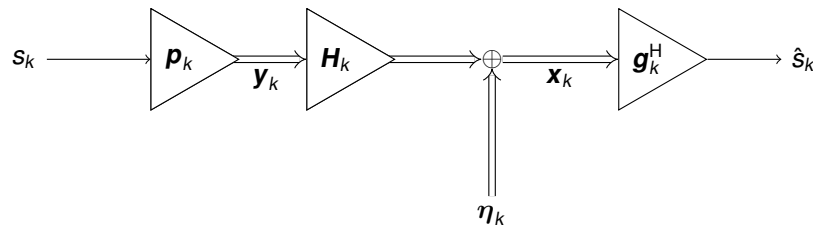

Figure 9.1: Single-stream point-to-point MIMO

and transmitted via the channel $\boldsymbol{H}_k \in \mathbb{C}^{M \times N}$.
The received signal $\boldsymbol{x}_k \in \mathbb{C}^M$ is perturbed with Gaussian noise $\boldsymbol{\eta}_k \sim \mathcal{N}_\mathbb{C}(\boldsymbol{0}_M, \boldsymbol{C}_k)$ with noise covariance $\boldsymbol{C}_k \in \mathbb{C}^{M \times M}$. Filtering with the receive filter $\boldsymbol{g}_k \in \mathbb{C}^M$ yields the received signal $\hat{s}_k$. The sum transmit power across all carriers is bounded by

$$\sum_{k=1}^{K} \mathsf{E}\left[\|\boldsymbol{y}_k\|_2^2\right] \leq E_{\text{Tx}}. \tag{9.1}$$

In the first part of this problem we will consider above system without equalizer.

a)* Give an expression for $\boldsymbol{x}_k$ as a function of s_k and $\boldsymbol{\eta}_k$.

$$\boldsymbol{x}_k = \boldsymbol{H}_k \boldsymbol{p}_k s_k + \boldsymbol{\eta}_k \ \checkmark$$

b)* Rewrite the power constraint (9.1) as a function of $\boldsymbol{p}_k$.

$$\sum_{k=1}^{K} \mathsf{E}\left[\|\boldsymbol{y}_k\|_2^2\right] = \sum_{k=1}^{K} \mathsf{E}\left[s_k^* s_k \boldsymbol{p}_k^{\mathsf{H}} \boldsymbol{p}_k\right] = \sum_{k=1}^{K} \boldsymbol{p}_k^{\mathsf{H}} \boldsymbol{p}_k \leq E_{\text{Tx}} \ \checkmark$$

c) Calculate the covariance matrix $\boldsymbol{C}_{\boldsymbol{x}_k}$ of the received signal $\boldsymbol{x}_k$.

$$\boldsymbol{C}_{\boldsymbol{x}_k} = \mathsf{E}\left[\boldsymbol{x}_k \boldsymbol{x}_k^{\mathsf{H}}\right] \ \checkmark \ = \boldsymbol{H}_k \boldsymbol{p}_k \boldsymbol{p}_k^{\mathsf{H}} \boldsymbol{H}_k^{\mathsf{H}} + \boldsymbol{C}_k \ \checkmark$$

Problem 10   Finite extension fields (13 credits)

Given the finite filed $\mathbb{F}_p$, we consider finite extension fields

$$F_q[x] = \left\{ \sum_{i=0}^{n-1} a_i x^i \,\middle|\, a_i \in \mathbb{F}_p \right\}. \tag{10.1}$$

a)* State the conditions on p, q, and n such that a finite extension field $F_q[x]$ exists.

> If $p \in \mathbb{N}$ is prime ✓ , $F_q[x]$ exists for any $q = p^n$ with $n \in \mathbb{N}$. ✓

b)* What is a *generator* of $\mathbb{F}_p$?

> Some $g \in \mathbb{F}_p$ is called *generator* if $\bigcup \left\{ g^i : i = 0, 1, \ldots, n-1 \right\} = \mathbb{F}_p \backslash \{0\}$. ✓

We now consider the finite extension field $F_{16}[x]$ built upon $\mathbb{F}_2 = \{0, 1\}$.

c)* State two reasons why this extensions field is of particular interest with respect to network coding.

> - The probability of two random vector $\boldsymbol{x}, \boldsymbol{y} \in F_q^N[x]$ is low for $N \geq 4$. ✓
>
> - The field allows for very efficient implementations. ✓
>
> - Symbols are represented by a nibble, i. e., two symbols make up an octet.

d)* List all elements of $F_{16}[x]$.

> $F_8[x] = \{0, 1,$
> $x, x+1,$
> $x^2, x^2+1, x^2+x, x^2+x+1$
> $x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}$

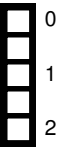e)* Explain why a reduction polynomial $r(x)$ is needed for the multiplicative group of $F_q[x]$.

Multiplication of $c = a \cdot b$ of $a, b \in F_q[x]$ may result in $c \notin F_q[x]$. ✓
Therefore, multiplication is defined as

$$c = a \cdot b \bmod r \quad \forall a, b \in F_q[x].$$ ✓

□ 0
□ 1
□ 2

f) State the conditions a polyomial $r(x)$ has to fulfill to be a suitable reduction polyomial.
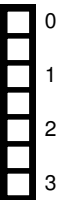
- $r \neq a \cdot b \ \forall a, b \in F_q[x]$ ✓

- $\deg(r) = n + 1$ for $q = 2^n$ ✓

□ 0
□ 1
□ 2

g) Find a reduction polynomial $r(x) \neq x^4 + 1$ for $F_q[x]$.

$x^4 + 1$
[Rechenweg fehlt ($\leftarrow$ this is a \fixme, not a comment for correctors)]

□ 0
□ 1
□ 2
□ 3

Additional space for solutions–clearly mark the (sub)problem your answers are related to and strike out invalid solutions.