Improving the LaTeX Sources of the Ct Book

20+ Years of CrypTool

Doris Behrendt
@dantetante

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

2019 Nov 01

How I got involved . . .

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from bibtex zu biblatex

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

How I got involved . . .

- I'm a board member of Dante e. V., the *German Speaking TEX User Group*, in German Deutschsprachige Anwendervereinigung TeX e. V., see `www.dante.de`
- Dante is organising 2 conferences per year
- I met Bernhard Esslinger at our spring conference in 2018
- in 2018 I started improving the LATEX sources of the CrypTool Book (CTB)

tasks

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

tasks

- change the LaTeX sources such that besides PDF there are also other output formats possible, e.g. HTML and ePub, but also PDF with smaller pagesize optimised for mobile phones
  - there are two LaTeX packages that can transform LaTeX to HTML or ePub: `lwarp` or `tex4ht`
  - both have restrictions, e.g. not every included LaTeX package is supported
  - the more plain vanilla the LaTeX code, the better
- test all SageMath examples
- eliminate typos, go through math
- take a critical look at everything
- feedback to BE

Inventory taking (May 2018)

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

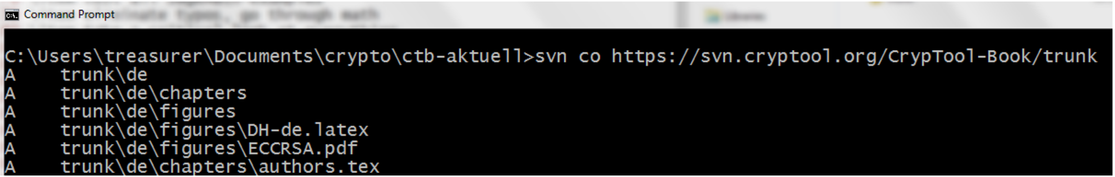
to-do-list

Inventory taking (May 2018)

- fetch project via `svn`

Inventory taking (May 2018)

- fetch project via `svn` screenshot of actual 2019 version



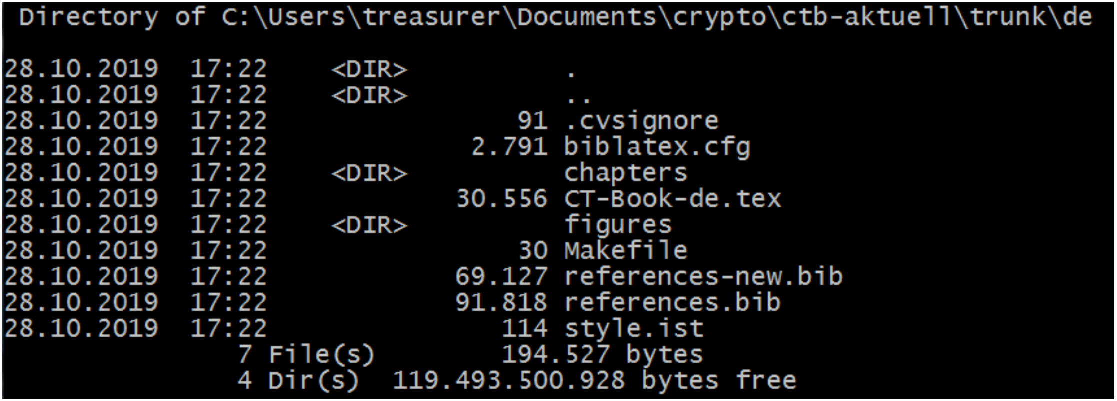
```
C:\Users\treasurer\Documents\crypto\ctb-aktuell>svn co https://svn.cryptool.org/CrypTool-Book/trunk
A     trunk\de
A     trunk\de\chapters
A     trunk\de\figures
A     trunk\de\figures\DH-de.latex
A     trunk\de\figures\ECCRSA.pdf
A     trunk\de\chapters\authors.tex
```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de (“deutsch”)

Inventory taking (May 2018)

- fetch project via svn
- files in folder de (“deutsch”) screenshot of actual 2019 version



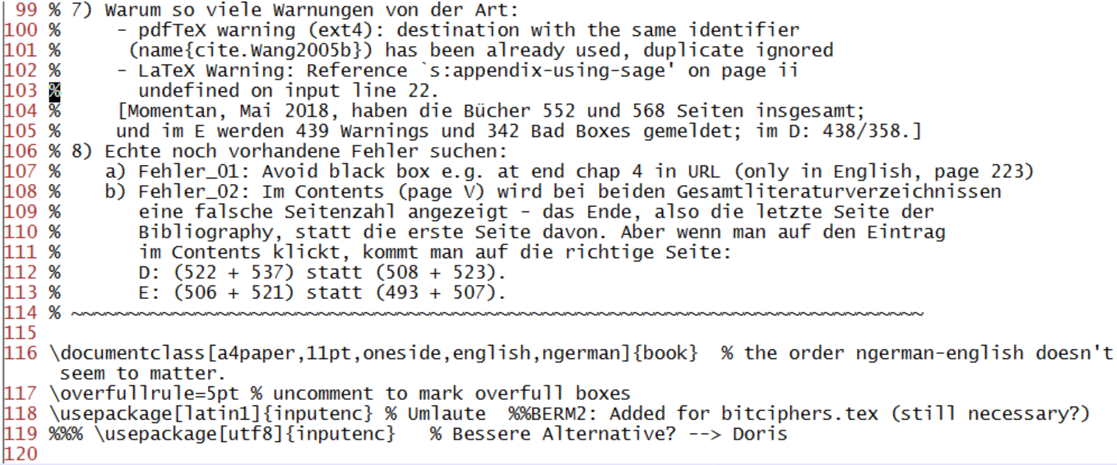
```
 Directory of C:\Users\treasurer\Documents\crypto\ctb-aktuell\trunk\de

28.10.2019  17:22    <DIR>          .
28.10.2019  17:22    <DIR>          ..
28.10.2019  17:22                91 .cvsignore
28.10.2019  17:22             2.791 biblatex.cfg
28.10.2019  17:22    <DIR>          chapters
28.10.2019  17:22            30.556 CT-Book-de.tex
28.10.2019  17:22    <DIR>          figures
28.10.2019  17:22                30 Makefile
28.10.2019  17:22            69.127 references-new.bib
28.10.2019  17:22            91.818 references.bib
28.10.2019  17:22               114 style.ist
               7 File(s)        194.527 bytes
               4 Dir(s)  119.493.500.928 bytes free
```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de (“deutsch”)
- main header file: `CT-Book-de.tex`

Inventory taking (May 2018)

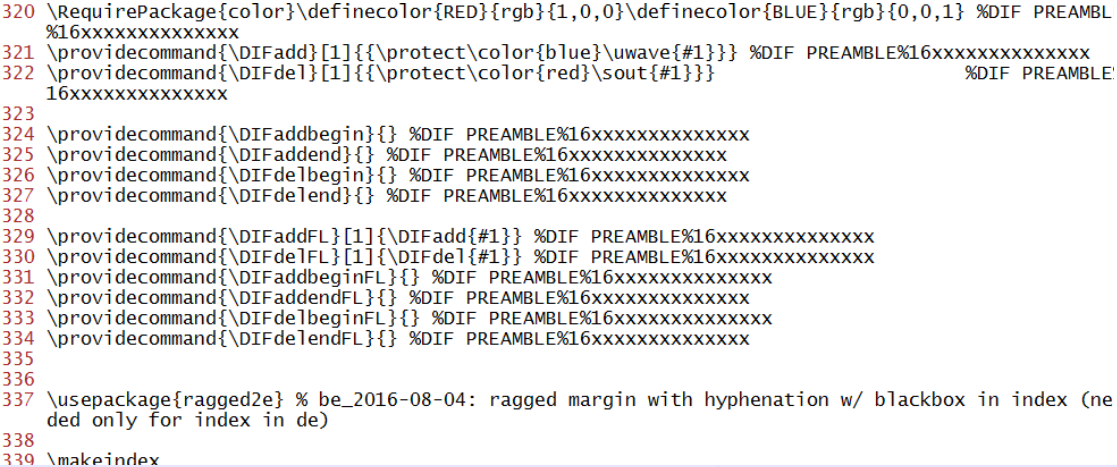
- fetch project via `svn`
- files in folder de ("deutsch")
- main header file: `CT-Book-de.tex`



```
% 7) Warum so viele Warnungen von der Art:
%     - pdfTeX warning (ext4): destination with the same identifier
%      (name{cite.Wang2005b}) has been already used, duplicate ignored
%     - LaTeX Warning: Reference `s:appendix-using-sage' on page ii
%       undefined on input line 22.
%     [Momentan, Mai 2018, haben die Bücher 552 und 568 Seiten insgesamt;
%     und im E werden 439 Warnings und 342 Bad Boxes gemeldet; im D: 438/358.]
% 8) Echte noch vorhandene Fehler suchen:
%    a) Fehler_01: Avoid black box e.g. at end chap 4 in URL (only in English, page 223)
%    b) Fehler_02: Im Contents (page V) wird bei beiden Gesamtliteraturverzeichnissen
%       eine falsche Seitenzahl angezeigt - das Ende, also die letzte Seite der
%       Bibliography, statt die erste Seite davon. Aber wenn man auf den Eintrag
%       im Contents klickt, kommt man auf die richtige Seite:
%       D: (522 + 537) statt (508 + 523).
%       E: (506 + 521) statt (493 + 507).
% ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

\documentclass[a4paper,11pt,oneside,english,ngerman]{book}  % the order ngerman-english doesn't seem to matter.
\overfullrule=5pt % uncomment to mark overfull boxes
\usepackage[latin1]{inputenc} % Umlaute  %%BERM2: Added for bitciphers.tex (still necessary?)
%%% \usepackage[utf8]{inputenc}   % Bessere Alternative? --> Doris

```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de ("deutsch")
- main header file: `CT-Book-de.tex`



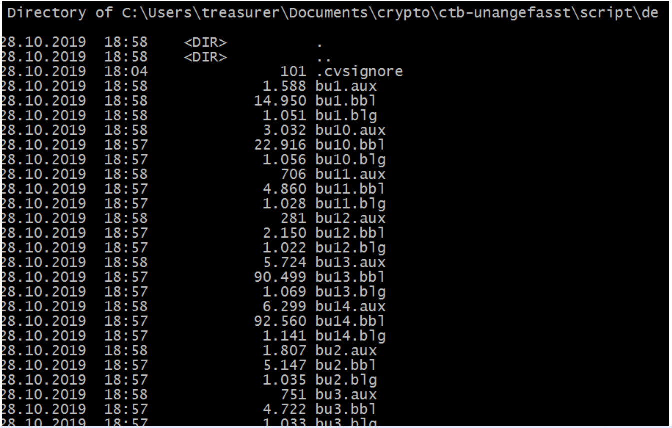
```
\RequirePackage{color}\definecolor{RED}{rgb}{1,0,0}\definecolor{BLUE}{rgb}{0,0,1} %DIF PREAMBL
%16xxxxxxxxxxxxxx
\providecommand{\DIFadd}[1]{{\protect\color{blue}\uwave{#1}}} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdel}[1]{{\protect\color{red}\sout{#1}}}                      %DIF PREAMBLE
16xxxxxxxxxxxxxx

\providecommand{\DIFaddbegin}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFaddend}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdelbegin}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdelend}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx

\providecommand{\DIFaddFL}[1]{\DIFadd{#1}} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdelFL}[1]{\DIFdel{#1}} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFaddbeginFL}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFaddendFL}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdelbeginFL}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx
\providecommand{\DIFdelendFL}{} %DIF PREAMBLE%16xxxxxxxxxxxxxx


\usepackage{ragged2e} % be_2016-08-04: ragged margin with hyphenation w/ blackbox in index (ne
ded only for index in de)

\makeindex
```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de (“deutsch”)
- main header file: `CT-Book-de.tex`
- aux-files after typesetting in folder `de`

Inventory taking (May 2018)

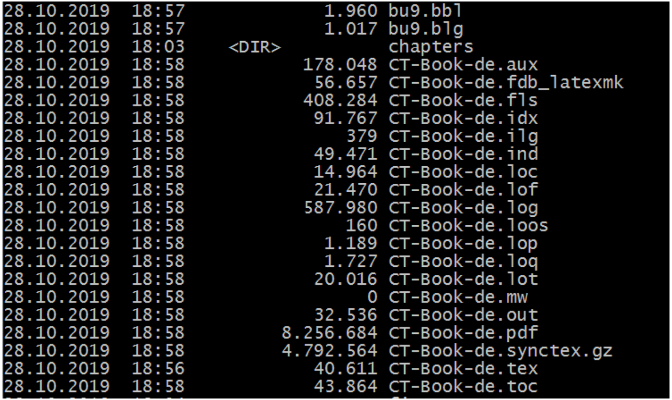
- fetch project via `svn`
- files in folder de ("deutsch")
- main header file: `CT-Book-de.tex`
- aux-files after typesetting in folder `de`



```
 Directory of C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de

28.10.2019  18:58    <DIR>          .
28.10.2019  18:58    <DIR>          ..
28.10.2019  18:04               101 .cvsignore
28.10.2019  18:58             1.588 bu1.aux
28.10.2019  18:58            14.950 bu1.bbl
28.10.2019  18:58             1.051 bu1.blg
28.10.2019  18:58             3.032 bu10.aux
28.10.2019  18:57            22.916 bu10.bbl
28.10.2019  18:57             1.056 bu10.blg
28.10.2019  18:58               706 bu11.aux
28.10.2019  18:57             4.860 bu11.bbl
28.10.2019  18:57             1.028 bu11.blg
28.10.2019  18:58               281 bu12.aux
28.10.2019  18:57             2.150 bu12.bbl
28.10.2019  18:57             1.022 bu12.blg
28.10.2019  18:58             5.724 bu13.aux
28.10.2019  18:57            90.499 bu13.bbl
28.10.2019  18:57             1.069 bu13.blg
28.10.2019  18:58             6.299 bu14.aux
28.10.2019  18:57            92.560 bu14.bbl
28.10.2019  18:57             1.141 bu14.blg
28.10.2019  18:58             1.807 bu2.aux
28.10.2019  18:57             5.147 bu2.bbl
28.10.2019  18:57             1.035 bu2.blg
28.10.2019  18:58               751 bu3.aux
28.10.2019  18:57             4.722 bu3.bbl
28.10.2019  18:57             1.033 bu3.blg
```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de ("deutsch")
- main header file: `CT-Book-de.tex`
- aux-files after typesetting in folder `de`



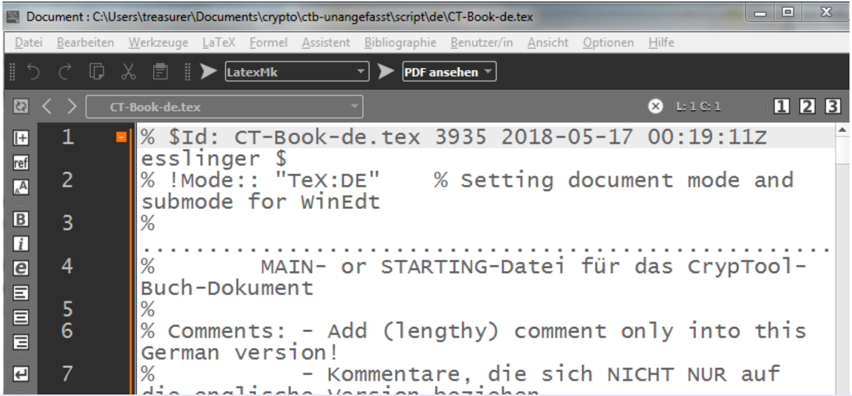
```
28.10.2019  18:57             1.960 bu9.bbl
28.10.2019  18:57             1.017 bu9.blg
28.10.2019  18:03    <DIR>          chapters
28.10.2019  18:58           178.048 CT-Book-de.aux
28.10.2019  18:58            56.657 CT-Book-de.fdb_latexmk
28.10.2019  18:58           408.284 CT-Book-de.fls
28.10.2019  18:58            91.767 CT-Book-de.idx
28.10.2019  18:58               379 CT-Book-de.ilg
28.10.2019  18:58            49.471 CT-Book-de.ind
28.10.2019  18:58            14.964 CT-Book-de.loc
28.10.2019  18:58            21.470 CT-Book-de.lof
28.10.2019  18:58           587.980 CT-Book-de.log
28.10.2019  18:58               160 CT-Book-de.loos
28.10.2019  18:58             1.189 CT-Book-de.lop
28.10.2019  18:58             1.727 CT-Book-de.loq
28.10.2019  18:58            20.016 CT-Book-de.lot
28.10.2019  18:58                 0 CT-Book-de.mw
28.10.2019  18:58            32.536 CT-Book-de.out
28.10.2019  18:58         8.256.684 CT-Book-de.pdf
28.10.2019  18:58         4.792.564 CT-Book-de.synctex.gz
28.10.2019  18:56            40.611 CT-Book-de.tex
28.10.2019  18:58            43.864 CT-Book-de.toc
```

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de (“deutsch”)
- main header file: `CT-Book-de.tex`
- aux-files after typesetting in folder `de`
- how typeset? ⟶ it has to be a frontend with `latexmk`, e.g. `TeXMaker`:

Inventory taking (May 2018)

- fetch project via `svn`
- files in folder de (“deutsch”)
- main header file: `CT-Book-de.tex`
- aux-files after typesetting in folder `de`
- how typeset? ⟶ it has to be a frontend with `latexmk`, e.g. `TeXMaker`:


Document : C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\CT-Book-de.tex
Datei Bearbeiten Werkzeuge LaTeX Formel Assistent Bibliographie Benutzer/in Ansicht Optionen Hilfe
LatexMk
PDF ansehen
CT-Book-de.tex
L: 1 C: 1
1 2 3

```
% $Id: CT-Book-de.tex 3935 2018-05-17 00:19:11Z esslinger $
% !Mode:: "TeX:DE"     % Setting document mode and submode for WinEdt
%
%.......................................................
%         MAIN- or STARTING-Datei für das CrypTool-Buch-Dokument
%
% Comments: - Add (lengthy) comment only into this German version!
%             - Kommentare, die sich NICHT NUR auf die englische Version beziehen
```

Arara

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

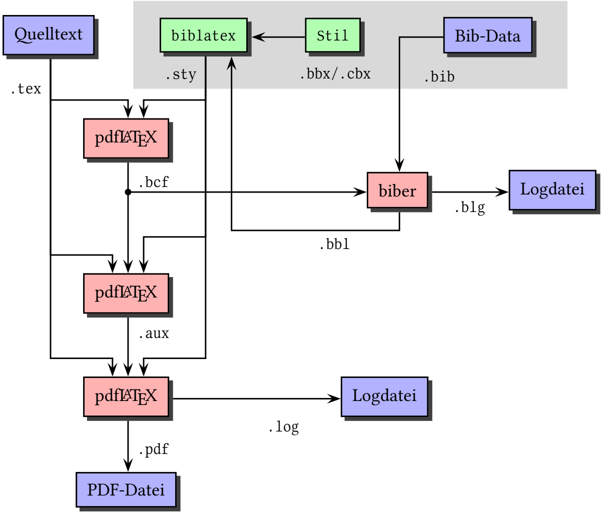
to-do-list

Arara

- just typeset with `pdflatex` is not enough

Arara

- just typeset with `pdflatex` is not enough



graphic by Herbert Voß

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don’t have it at all

Arara

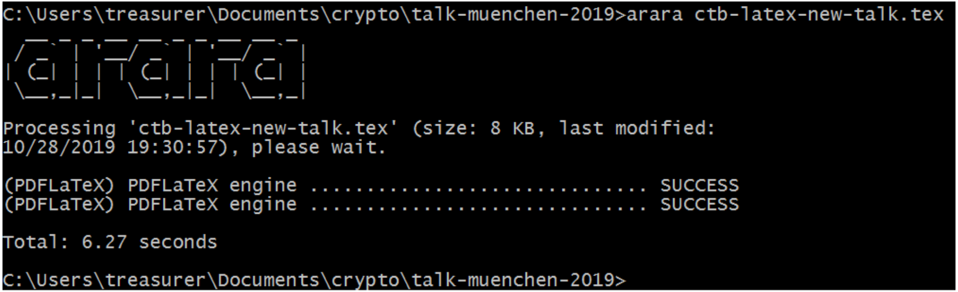
- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TEX distribution; with it, typesetting gets faster

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TeX distribution; with it, typesetting gets faster
- call it via the command line

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TEX distribution; with it, typesetting gets faster
- call it via the command line



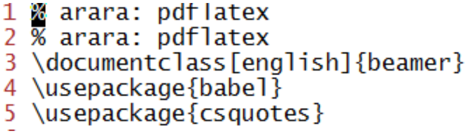
```
C:\Users\treasurer\Documents\crypto\talk-muenchen-2019>arara ctb-latex-new-talk.tex
  __ _ _ __ __ _ _ __ __ _
 / _` | '__/ _` | '__/ _` |
| (_| | | | (_| | | | (_| |
 \__,_|_|  \__,_|_|  \__,_|

Processing 'ctb-latex-new-talk.tex' (size: 8 KB, last modified:
10/28/2019 19:30:57), please wait.

(PDFLaTeX) PDFLaTeX engine .............................. SUCCESS
(PDFLaTeX) PDFLaTeX engine .............................. SUCCESS

Total: 6.27 seconds

C:\Users\treasurer\Documents\crypto\talk-muenchen-2019>
```

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TEX distribution; with it, typesetting gets faster
- call it via the command line
- include lines into your header

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TeX distribution; with it, typesetting gets faster
- call it via the command line
- include lines into your header



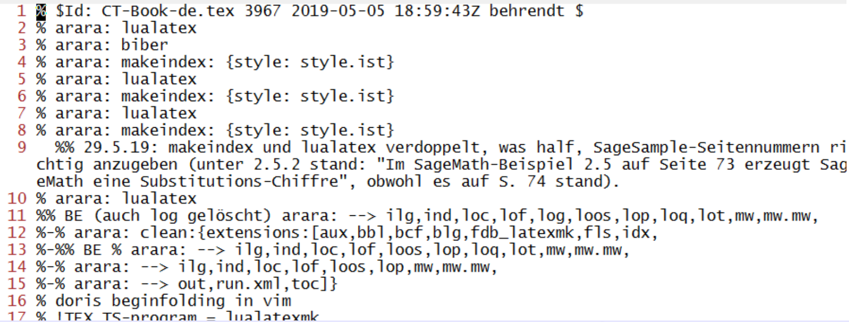
```
% arara: pdflatex
% arara: pdflatex
\documentclass[english]{beamer}
\usepackage{babel}
\usepackage{csquotes}
```

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TEX distribution; with it, typesetting gets faster
- call it via the command line
- include lines into your header
- this is what we use for the CTB now:

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TEX distribution; with it, typesetting gets faster
- call it via the command line
- include lines into your header
- this is what we use for the CTB now:



```
% $Id: CT-Book-de.tex 3967 2019-05-05 18:59:43Z behrendt $
% arara: lualatex
% arara: biber
% arara: makeindex: {style: style.ist}
% arara: lualatex
% arara: makeindex: {style: style.ist}
% arara: lualatex
% arara: makeindex: {style: style.ist}
  %% 29.5.19: makeindex und lualatex verdoppelt, was half, SageSample-Seitennummern ri
chtig anzugeben (unter 2.5.2 stand: "Im SageMath-Beispiel 2.5 auf Seite 73 erzeugt Sag
eMath eine Substitutions-Chiffre", obwohl es auf S. 74 stand).
% arara: lualatex
%% BE (auch log gelöscht) arara: --> ilg,ind,loc,lof,log,loos,lop,loq,lot,mw,mw.mw,
%-% arara: clean:{extensions:[aux,bbl,bcf,blg,fdb_latexmk,fls,idx,
%-%% BE % arara: --> ilg,ind,loc,lof,loos,lop,loq,lot,mw,mw.mw,
%-% arara: --> ilg,ind,loc,lof,loos,lop,mw,mw.mw,
%-% arara: --> out,run.xml,toc]}
% doris beginfolding in vim
% !TEX TS-program = lualatexmk
```

Arara

- just typeset with `pdflatex` is not enough
- not all frontends have `(pdf)latexmk` activated, some don't have it at all
- better use `arara` by Paulo Cereda, it's a part of every actual TeX distribution; with it, typesetting gets faster
- call it via the command line
- include lines into your header
- this is what we use for the CTB now:
- `arara` is quite powerful and actively developed, see https://www.ctan.org/pkg/arara

transision from bibtex zu biblatex

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from bibtex zu biblatex

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

transision from bibtex zu biblatex

- bibtex is older than biblatex and still widely used

transision from bibtex zu biblatex

- biblatex has more capabilities, e. g. it can handle utf8/unicode

transision from bibtex zu biblatex

- easily create multiple bibliographies

transision from bibtex zu biblatex

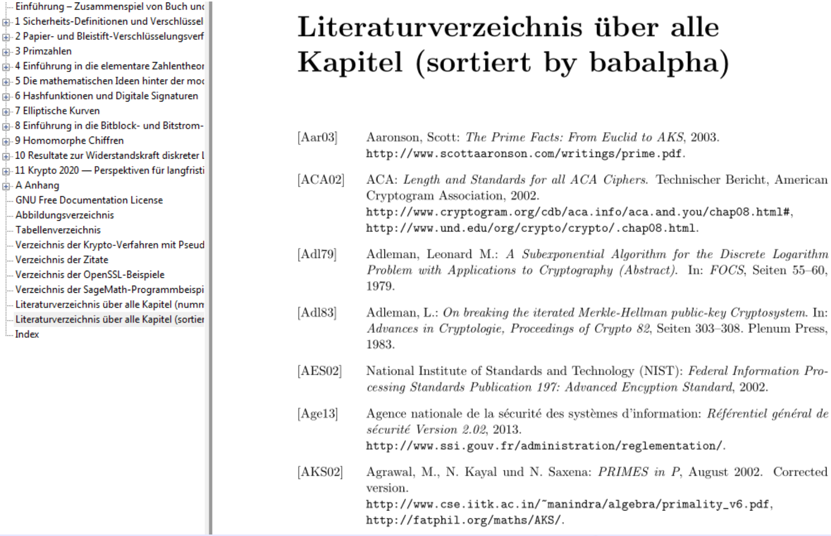
- better sorting

transision from bibtex zu biblatex

- Philip Kime's talk at the last Dante conference, see `https://www.dante.de/veranstaltungen/herbst2019/programm/`

transision from bibtex zu biblatex

- ctb bibliography before changes



Literaturverzeichnis über alle Kapitel (sortiert by babalpha)

[Aar03] Aaronson, Scott: *The Prime Facts: From Euclid to AKS*, 2003. `http://www.scottaaronson.com/writings/prime.pdf`.

[ACA02] ACA: *Length and Standards for all ACA Ciphers*. Technischer Bericht, American Cryptogram Association, 2002. `http://www.cryptogram.org/cdb/aca.info/aca.and.you/chap08.html#`, `http://www.und.edu/org/crypto/crypto/.chap08.html`.

[Adl79] Adleman, Leonard M.: *A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography (Abstract)*. In: *FOCS*, Seiten 55–60, 1979.

[Adl83] Adleman, L.: *On breaking the iterated Merkle-Hellman public-key Cryptosystem*. In: *Advances in Cryptologie, Proceedings of Crypto 82*, Seiten 303–308. Plenum Press, 1983.

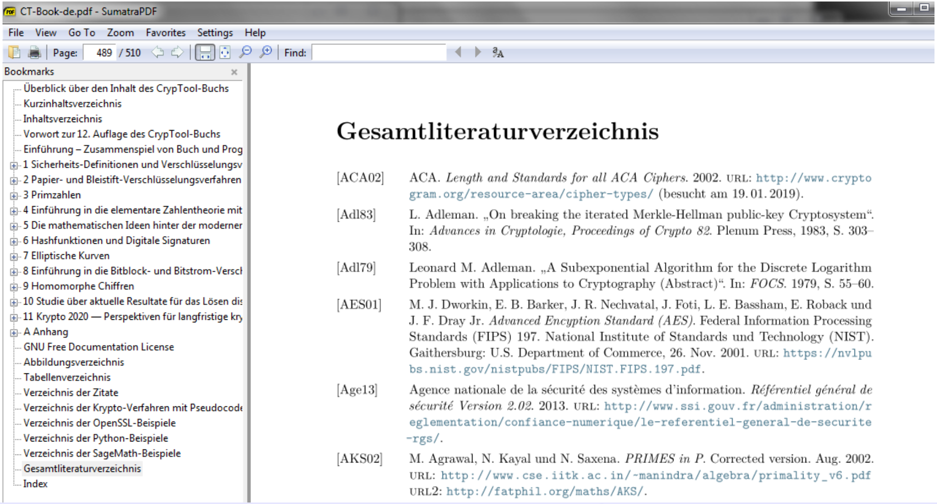
[AES02] National Institute of Standards and Technology (NIST): *Federal Information Processing Standards Publication 197: Advanced Encyption Standard*, 2002.

[Age13] Agence nationale de la sécurité des systèmes d'information: *Référentiel général de sécurité Version 2.02*, 2013. `http://www.ssi.gouv.fr/administration/reglementation/`.

[AKS02] Agrawal, M., N. Kayal und N. Saxena: *PRIMES in P*, August 2002. Corrected version. `http://www.cse.iitk.ac.in/~manindra/algebra/primality_v6.pdf`, `http://fatphil.org/maths/AKS/`.

transision from bibtex zu biblatex

- ctb bibliography before changes
- bibliography now


CT-Book-de.pdf - SumatraPDF
File View Go To Zoom Favorites Settings Help
Page: 489 / 510
Find:
Bookmarks

Gesamtliteraturverzeichnis

[ACA02] ACA. *Length and Standards for all ACA Ciphers*. 2002. URL: http://www.cryptogram.org/resource-area/cipher-types/ (besucht am 19. 01. 2019).

[Adl83] L. Adleman. „On breaking the iterated Merkle-Hellman public-key Cryptosystem“. In: *Advances in Cryptologie, Proceedings of Crypto 82*. Plenum Press, 1983, S. 303–308.

[Adl79] Leonard M. Adleman. „A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography (Abstract)“. In: *FOCS*. 1979, S. 55–60.

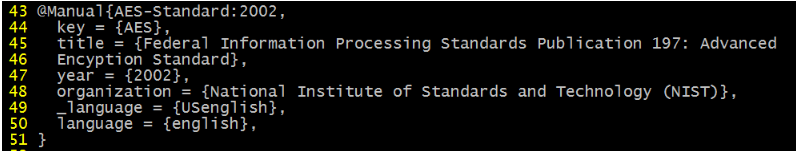
[AES01] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, E. Roback und J. F. Dray Jr. *Advanced Encyption Standard (AES)*. Federal Information Processing Standards (FIPS) 197. National Institute of Standards und Technology (NIST). Gaithersburg: U.S. Department of Commerce, 26. Nov. 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[Age13] Agence nationale de la sécurité des systèmes d'information. *Référentiel général de sécurité Version 2.02*. 2013. URL: http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

[AKS02] M. Agrawal, N. Kayal und N. Saxena. *PRIMES in P*. Corrected version. Aug. 2002. URL: http://www.cse.iitk.ac.in/~manindra/algebra/primality_v6.pdf URL2: http://fatphil.org/maths/AKS/.

transision from bibtex zu biblatex

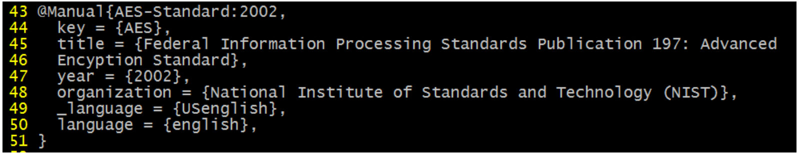
- ctb bibliography before changes
- bibliography now
- `references.bib` (example before changes)



```
@Manual{AES-Standard:2002,
  key = {AES},
  title = {Federal Information Processing Standards Publication 197: Advanced
  Encyption Standard},
  year = {2002},
  organization = {National Institute of Standards and Technology (NIST)},
  _language = {USenglish},
  language = {english},
}
```

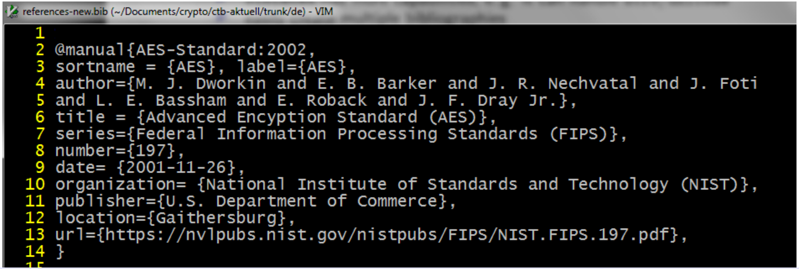
transision from bibtex zu biblatex

- ctb bibliography before changes
- bibliography now
- `references.bib` (example before changes)



```
@Manual{AES-Standard:2002,
  key = {AES},
  title = {Federal Information Processing Standards Publication 197: Advanced
  Encyption Standard},
  year = {2002},
  organization = {National Institute of Standards and Technology (NIST)},
  _language = {USenglish},
  language = {english},
}
```

- `references-new.bib` (example now, for german version)



references-new.bib (~/Documents/crypto/ctb-aktuell/trunk/de) - VIM

```

@manual{AES-Standard:2002,
sortname = {AES}, label={AES},
author={M. J. Dworkin and E. B. Barker and J. R. Nechvatal and J. Foti
and L. E. Bassham and E. Roback and J. F. Dray Jr.},
title = {Advanced Encyption Standard (AES)},
series={Federal Information Processing Standards (FIPS)},
number={197},
date= {2001-11-26},
organization= {National Institute of Standards and Technology (NIST)},
publisher={U.S. Department of Commerce},
location={Gaithersburg},
url={https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf},
}
```

transition from pdflatex to lualatex

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

transition from pdflatex to lualatex

- what is `lualatex`?
  Both `LuaTeX` and `XeTeX` are UTF-8 engines for processing TEX documents. This means that the input (.tex files) can contain characters that with pdfTeX are difficult to use directly. Both can also use system fonts, again in contrast to pdfTeX.

  ...

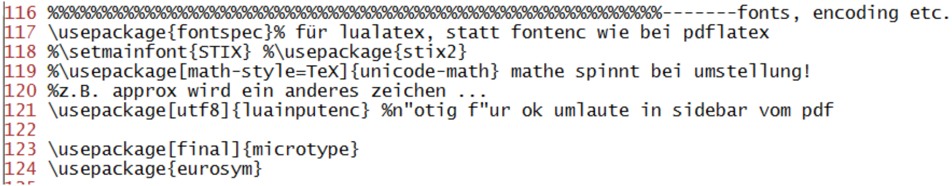
  LuaTeX has bigger aims. The idea is to add a scripting language (Lua) to TEX, and to open up the internals of TeX to this language. (see `https://tex.stackexchange.com/questions/36/differences-between-luatex-context-and-xetex` or also in german `https://texfragen.de/was_ist_luatex_und_kann_ich_es_anstelle_von_latex_benutzen` and `https://texwelt.de/fragen/70/was-ist-luatex`)

transition from pdflatex to lualatex

- what is `lualatex`?
- why change to `lualatex`?
  - get rid of some packages, e.g. morewrites, ae
  - easier handling of fonts, nonascii characters, computations
  - later: try other fonts

transition from pdflatex to lualatex

- what is `lualatex`?
- why change to `lualatex`?
  - get rid of some packages, e.g. morewrites, ae
  - easier handling of fonts, nonascii characters, computations
  - later: try other fonts
- some changes in header necessary



```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%-------fonts, encoding etc.
\usepackage{fontspec}% für lualatex, statt fontenc wie bei pdflatex
%\setmainfont{STIX} %\usepackage{stix2}
%\usepackage[math-style=TeX]{unicode-math} mathe spinnt bei umstellung!
%z.B. approx wird ein anderes zeichen ...
\usepackage[utf8]{luainputenc} %n"otig f"ur ok umlaute in sidebar vom pdf

\usepackage[final]{microtype}
\usepackage{eurosym}
```

transition from pdflatex to lualatex

- what is `lualatex`?
- why change to `lualatex`?
  - get rid of some packages, e.g. morewrites, ae
  - easier handling of fonts, nonascii characters, computations
  - later: try other fonts
- some changes in header necessary
- check encoding of `.tex` file and `.bib` file, should be `utf8` instead of (default?) `latin1`

transition from pdflatex to lualatex

- what is `lualatex`?
- why change to `lualatex`?
  - get rid of some packages, e.g. morewrites, ae
  - easier handling of fonts, nonascii characters, computations
  - later: try other fonts
- some changes in header necessary
- check encoding of `.tex` file and `.bib` file, should be `utf8` instead of (default?) `latin1`
- encoding dependent on frontend/editor/system defaults/file

lengths, pagebreaks, indents etc.

How I got involved ...

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

lengths, pagebreaks, indents etc.

- when using the same LaTeX source for e.g. PDF output of A4 as well as A5, better don't include images like this:

  ```
  \includegraphics[width=7cm]{image}
  ```

lengths, pagebreaks, indents etc.

- when using the same LaTeX source for e.g. PDF output of A4 as well as A5, better don't include images like this:

  ```
  \includegraphics[width=7cm]{image}
  ```

  Use relative lengths:

  ```
  \includegraphics[.5\textwidth]{image}
  ```

lengths, pagebreaks, indents etc.

- try to avoid manual pagebreaks

lengths, pagebreaks, indents etc.

- try to avoid manual pagebreaks
  - they are often used to manually prevent “Hurenkinder und Schusterjungen” (widows and orphans); better use `\widowpenalty` and `\clubpenalty`

lengths, pagebreaks, indents etc.

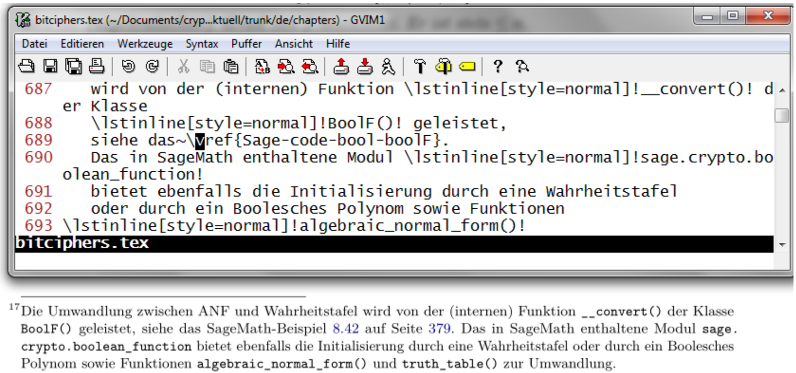
- try to avoid manual pagebreaks
  - they are often used to manually prevent “Hurenkinder und Schusterjungen” (widows and orphans); better use `\widowpenalty` and `\clubpenalty`
  - manual pagebreaks are often used to get floating objects (like pictures) to not float

lengths, pagebreaks, indents etc.

- try to avoid manual pagebreaks
  - they are often used to manually prevent “Hurenkinder und Schusterjungen” (widows and orphans); better use `\widowpenalty` and `\clubpenalty`
  - manual pagebreaks are often used to get floating objects (like pictures) to not float
  - use option `H` from package `float` if you really want to place a float here

lengths, pagebreaks, indents etc.

- try to avoid manual pagebreaks
  - they are often used to manually prevent "Hurenkinder und Schusterjungen" (widows and orphans); better use `\widowpenalty` and `\clubpenalty`
  - manual pagebreaks are often used to get floating objects (like pictures) to not float
  - use option `H` from package `float` if you really want to place a float here
  - use `cleverref` and/or `varioref`



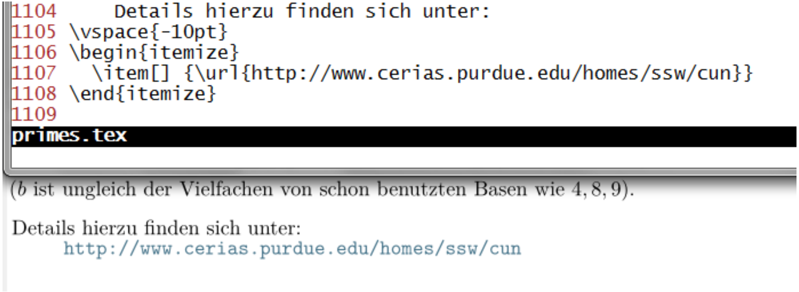
bitciphers.tex (~/Documents/cryp...ktuell/trunk/de/chapters) - GVIM1
Datei
Editieren
Werkzeuge
Syntax
Puffer
Ansicht
Hilfe
bitciphers.tex

```
    wird von der (internen) Funktion \lstinline[style=normal]!__convert()! der Klasse
    \lstinline[style=normal]!BoolF()! geleistet,
    siehe das~\vref{Sage-code-bool-boolF}.
    Das in SageMath enthaltene Modul \lstinline[style=normal]!sage.crypto.boolean_function!
    bietet ebenfalls die Initialisierung durch eine Wahrheitstafel
    oder durch ein Boolesches Polynom sowie Funktionen
\lstinline[style=normal]!algebraic_normal_form()!
```

[17] Die Umwandlung zwischen ANF und Wahrheitstafel wird von der (internen) Funktion `__convert()` der Klasse `BoolF()` geleistet, siehe das SageMath-Beispiel 8.42 auf Seite 379. Das in SageMath enthaltene Modul `sage.crypto.boolean_function` bietet ebenfalls die Initialisierung durch eine Wahrheitstafel oder durch ein Boolesches Polynom sowie Funktionen `algebraic_normal_form()` und `truth_table()` zur Umwandlung.

lengths, pagebreaks, indents etc.

- don't adjust vertical spacing manually:



```
    Details hierzu finden sich unter:
\vspace{-10pt}
\begin{itemize}
  \item[] {\url{http://www.cerias.purdue.edu/homes/ssw/cun}}
\end{itemize}

```

primes.tex

(b ist ungleich der Vielfachen von schon benutzten Basen wie $4, 8, 9$).

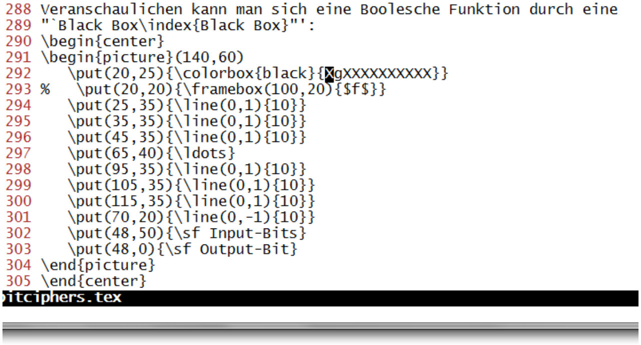
Details hierzu finden sich unter:
    http://www.cerias.purdue.edu/homes/ssw/cun

lengths, pagebreaks, indents etc.

- don’t define the width of a box to be equal to the width of a word in the actual fontsize ;-)

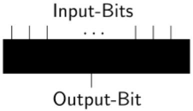
lengths, pagebreaks, indents etc.

- don't define the width of a box to be equal to the width of a word in the actual fontsize ;-)
  before:



```
Veranschaulichen kann man sich eine Boolesche Funktion durch eine
"`Black Box\index{Black Box}"':
\begin{center}
\begin{picture}(140,60)
   \put(20,25){\colorbox{black}{XgXXXXXXXXXX}}
%   \put(20,20){\framebox(100,20){$f$}}
   \put(25,35){\line(0,1){10}}
   \put(35,35){\line(0,1){10}}
   \put(45,35){\line(0,1){10}}
   \put(65,40){\ldots}
   \put(95,35){\line(0,1){10}}
   \put(105,35){\line(0,1){10}}
   \put(115,35){\line(0,1){10}}
   \put(70,20){\line(0,-1){10}}
   \put(48,50){\sf Input-Bits}
   \put(48,0){\sf Output-Bit}
\end{picture}
\end{center}
```

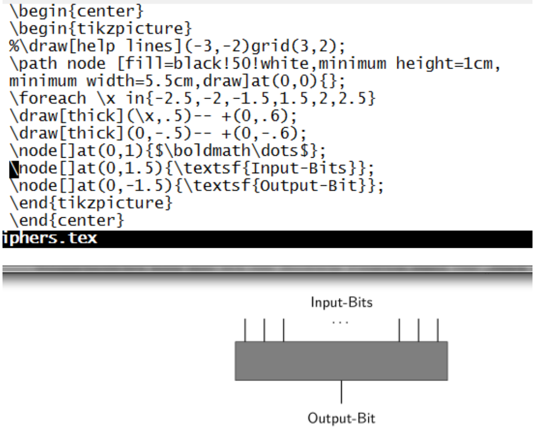
itciphers.tex



lengths, pagebreaks, indents etc.

- don't define the width of a box to be equal to the width of a word in the actual fontsize ;-)

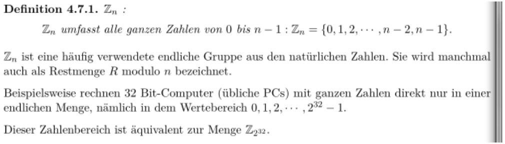
  now:



```
\begin{center}
\begin{tikzpicture}
%\draw[help lines](-3,-2)grid(3,2);
\path node [fill=black!50!white,minimum height=1cm,
minimum width=5.5cm,draw]at(0,0){};
\foreach \x in{-2.5,-2,-1.5,1.5,2,2.5}
\draw[thick](\x,.5)-- +(0,.6);
\draw[thick](0,-.5)-- +(0,-.6);
\node[]at(0,1){$\boldmath\dots$};
\node[]at(0,1.5){\textsf{Input-Bits}};
\node[]at(0,-1.5){\textsf{Output-Bit}};
\end{tikzpicture}
\end{center}
```

lengths, pagebreaks, indents etc.

- don’t use indentation when there’s a lot of math:



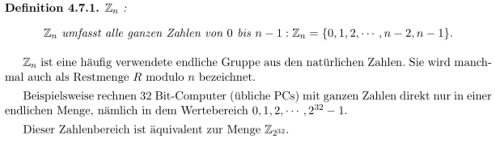
Definition 4.7.1. $\mathbb{Z}_n$ *:*

$\mathbb{Z}_n$ umfasst alle ganzen Zahlen von 0 *bis* $n-1:\mathbb{Z}_n=\{0,1,2,\cdots,n-2,n-1\}$.

$\mathbb{Z}_n$ ist eine häufig verwendete endliche Gruppe aus den natürlichen Zahlen. Sie wird manchmal auch als Restmenge R modulo n bezeichnet.

Beispielsweise rechnen 32 Bit-Computer (übliche PCs) mit ganzen Zahlen direkt nur in einer endlichen Menge, nämlich in dem Wertebereich $0,1,2,\cdots,2^{32}-1$.

Dieser Zahlenbereich ist äquivalent zur Menge $\mathbb{Z}_{2^{32}}$.



Definition 4.7.1. $\mathbb{Z}_n$ *:*

$\mathbb{Z}_n$ umfasst alle ganzen Zahlen von 0 *bis* $n-1:\mathbb{Z}_n=\{0,1,2,\cdots,n-2,n-1\}$.

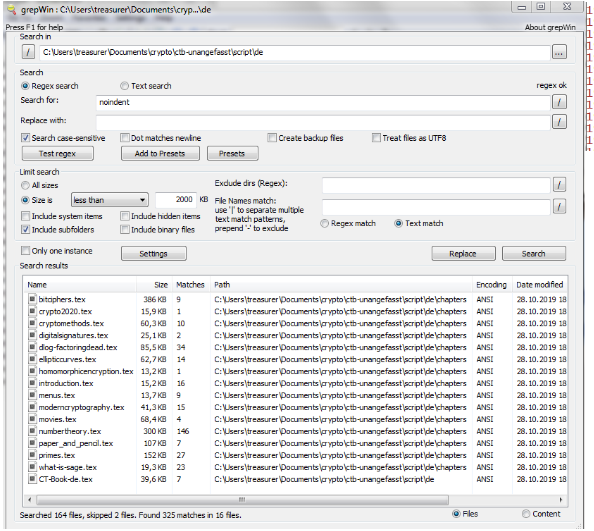
$\mathbb{Z}_n$ ist eine häufig verwendete endliche Gruppe aus den natürlichen Zahlen. Sie wird manchmal auch als Restmenge R modulo n bezeichnet.

Beispielsweise rechnen 32 Bit-Computer (übliche PCs) mit ganzen Zahlen direkt nur in einer endlichen Menge, nämlich in dem Wertebereich $0,1,2,\cdots,2^{32}-1$.

Dieser Zahlenbereich ist äquivalent zur Menge $\mathbb{Z}_{2^{32}}$.

lengths, pagebreaks, indents etc.

- dont' use `\noindent` a hundred times:



grepWin : C:\Users\treasurer\Documents\cryp...\de

Press F1 for help — About grepWin

Search in: C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de

Search: ● Regex search ○ Text search — regex ok

Search for: noindent

Replace with:

☑ Search case-sensitive ☐ Dot matches newline ☐ Create backup files ☐ Treat files as UTF8

Limit search: ○ All sizes ● Size is less than 2000 KB

☐ Include system items ☐ Include hidden items

☑ Include subfolders ☐ Include binary files

Exclude dirs (Regex):

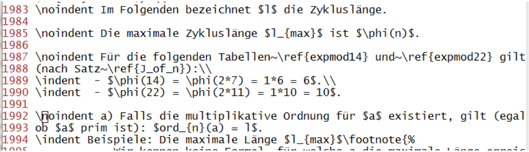
File Names match: use '|' to separate multiple text match patterns, prepend '-' to exclude — ○ Regex match ● Text match

☐ Only one instance

Search results

Name	Size	Matches	Path	Encoding	Date modified
bitciphers.tex	386 KB	9	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
crypto2020.tex	15,9 KB	1	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
cryptomethods.tex	60,3 KB	10	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
digitalsignatures.tex	25,1 KB	2	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
dlog-factoringdead.tex	85,5 KB	34	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
ellipticcurves.tex	62,7 KB	14	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
homomorphicencryption.tex	13,2 KB	1	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
introduction.tex	15,2 KB	16	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
menus.tex	13,7 KB	9	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
moderncryptography.tex	41,3 KB	15	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
movies.tex	68,4 KB	4	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
numbertheory.tex	300 KB	146	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
paper_and_pencil.tex	107 KB	7	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
primes.tex	152 KB	27	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
what-is-sage.tex	19,3 KB	23	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de\chapters	ANSI	28.10.2019 18
CT-Book-de.tex	39,6 KB	7	C:\Users\treasurer\Documents\crypto\ctb-unangefasst\script\de	ANSI	28.10.2019 18

Searched 164 files, skipped 2 files. Found 325 matches in 16 files. ● Files ○ Content



```
\noindent Im Folgenden bezeichnet $l$ die Zykluslänge.

\noindent Die maximale Zykluslänge $l_{max}$ ist $\phi(n)$.

\noindent Für die folgenden Tabellen~\ref{expmod14} und~\ref{expmod22} gilt
(nach Satz~\ref{J_of_n}):\\
\indent  - $\phi(14) = \phi(2*7) = 1*6 = 6$.\\
\indent  - $\phi(22) = \phi(2*11) = 1*10 = 10$.

\noindent a) Falls die multiplikative Ordnung für $a$ existiert, gilt (egal
ob $a$ prim ist): $ord_{n}(a) = l$.
\indent Beispiele: Die maximale Länge $l_{max}$\footnote{%
            Wir kennen keine Formel, für welche a die maximale Länge erreic
```

lengths, pagebreaks, indents etc.

- for setting the indent globally to zero we could have used `\setlength{\parindent}{0cm}` in the preamle

lengths, pagebreaks, indents etc.

- for setting the indent globally to zero we could have used `\setlength{\parindent}{0cm}` in the preamle
- without paragraph indentation one usually wants to have a vertical space between paragraphs: `\vskip3em plus 1em minus 1em` tells TEX to “choose” an inter paragraph spacing from 2 to 4 times the width of the letter m in the actual font size, defaulting to `3em` (concept of “glue”);

lengths, pagebreaks, indents etc.

- for setting the indent globally to zero we could have used `\setlength{\parindent}{0cm}` in the preamle
- without paragraph indentation one usually wants to have a vertical space between paragraphs: `\vskip3em plus 1em minus 1em` tells TEX to “choose” an inter paragraph spacing from 2 to 4 times the width of the letter m in the actual font size, defaulting to `3em` (concept of “glue”);
- but using `\vskip3em` in the preamble can have side effects, e.g. in our case it affected also the table of contents in an unwanted way; though using the package `parskip` would have been a solution, I decided to switch to KOMA-Script (named after Markus Kohm)

switching to KOMA

- How I got involved . . .
- tasks
- Inventory taking (May 2018)
- Arara
- transision from `bibtex` zu `biblatex`
- transition from pdflatex to lualatex
- lengths, pagebreaks, indents etc.
- switching to KOMA
- (some of the) introduced packages
- misc
- to-do-list

switching to KOMA

- in KOMA-Script you define parskip and parindent as an option to the documentclass:

  ```
  \documentclass[parskip=half-,...]{scrbook}
  ```

switching to KOMA

- in KOMA-Script you define `parskip` and `parindent` as an option to the documentclass:
  `\documentclass[parskip=half-,...]{scrbook}`
- use KOMA-Script e. g. for letters, large documents, advanced layouting needs;

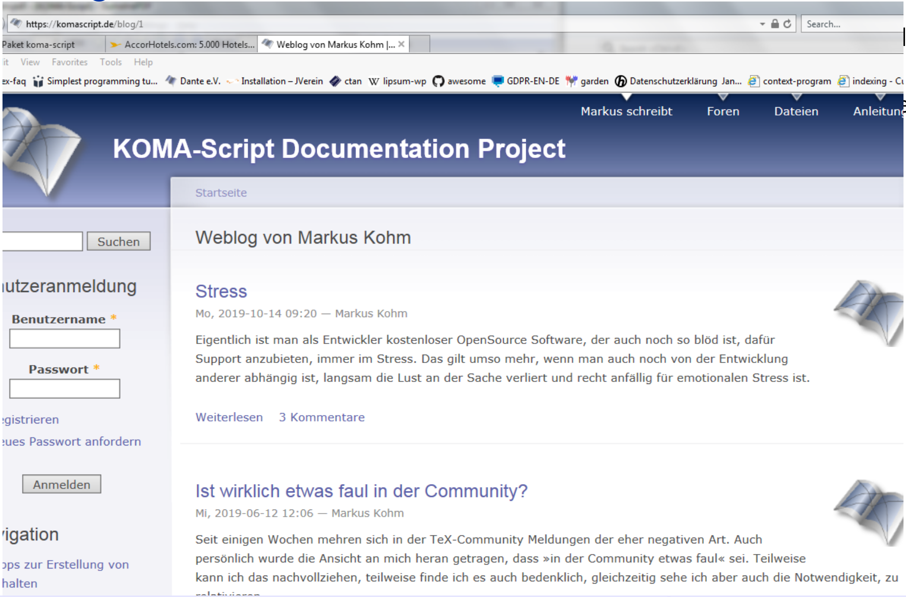
switching to KOMA

- in KOMA-Script you define `parskip` and `parindent` as an option to the documentclass:
  `\documentclass[parskip=half-,...]{scrbook}`
- use KOMA-Script e. g. for letters, large documents, advanced layouting needs;
- Markus Kohm has the website https://komascript.de/blog/1 (in german)

switching to KOMA

locumentclass:

eds;



KOMA-Script Documentation Project

utzeranmeldung

Benutzername *

Passwort *

egistrieren

eues Passwort anfordern

igation

ps zur Erstellung von

halten

Weblog von Markus Kohm

Stress

Mo, 2019-10-14 09:20 — Markus Kohm

Eigentlich ist man als Entwickler kostenloser OpenSource Software, der auch noch so blöd ist, dafür Support anzubieten, immer im Stress. Das gilt umso mehr, wenn man auch noch von der Entwicklung anderer abhängig ist, langsam die Lust an der Sache verliert und recht anfällig für emotionalen Stress ist.

Weiterlesen 3 Kommentare

Ist wirklich etwas faul in der Community?

Mi, 2019-06-12 12:06 — Markus Kohm

Seit einigen Wochen mehren sich in der TeX-Community Meldungen der eher negativen Art. Auch persönlich wurde die Ansicht an mich heran getragen, dass »in der Community etwas faul« sei. Teilweise kann ich das nachvollziehen, teilweise finde ich es auch bedenklich, gleichzeitig sehe ich aber auch die Notwendigkeit, zu relativieren

switching to KOMA

- in KOMA-Script you define `parskip` and `parindent` as an option to the documentclass:

  `\documentclass[parskip=half-,...]{scrbook}`
- use KOMA-Script e. g. for letters, large documents, advanced layouting needs;
- Markus Kohm has the website `https://komascript.de/blog/1` (in german)
- side effect: LaTeX used with `\documentclass{scrbook}` throws an error whereas with `\documentclass{book}` it doesn't: deprecated commands like `\bf` are not allowed (`\sc`, `\sf`, `\tt`, `\it`)

switching to KOMA

- in KOMA-Script you define `parskip` and `parindent` as an option to the documentclass: `\documentclass[parskip=half-,...]{scrbook}`
- use KOMA-Script e. g. for letters, large documents, advanced layouting needs;
- Markus Kohm has the website `https://komascript.de/blog/1` (in german)
- side effect: LaTeX used with `\documentclass{scrbook}` throws an error whereas with `\documentclass{book}` it doesn't: deprecated commands like `\bf` are not allowed (`\sc`, `\sf`, `\tt`, `\it`)
- read *l2tabu – Obsolete packages and commands*, see `https://ctan.org/pkg/l2tabu?lang=en`

switching to KOMA

- in KOMA-Script you define `parskip` and `parindent` as an option to the documentclass:
  `\documentclass[parskip=half-,...]{scrbook}`
- use KOMA-Script e. g. for letters, large documents, advanced layouting needs;
- Markus Kohm has the website `https://komascript.de/blog/1` (in german)
- side effect: LaTeX used with `\documentclass{scrbook}` throws an error whereas with `\documentclass{book}` it doesn't: deprecated commands like `\bf` are not allowed (`\sc`, `\sf`, `\tt`, `\it`)
- read *l2tabu – Obsolete packages and commands*, see `https://ctan.org/pkg/l2tabu?lang=en`
- use `\enquote{...}` from package `csquotes` instead of `\glqq` or `"‘` from package `ngerman`

(some of the) introduced packages

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

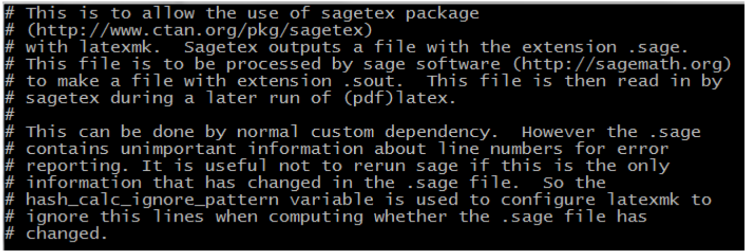
(some of the) introduced packages

misc

to-do-list

(some of the) introduced packages

- `enumitem`: easier changes of itemize item spacing
- `listings`: source code printer for LaTeX, highly customisable
- (not yet) `sagetex`:



```
# This is to allow the use of sagetex package
# (http://www.ctan.org/pkg/sagetex)
# with latexmk.  Sagetex outputs a file with the extension .sage.
# This file is to be processed by sage software (http://sagemath.org)
# to make a file with extension .sout.  This file is then read in by
# sagetex during a later run of (pdf)latex.
#
# This can be done by normal custom dependency.  However the .sage
# contains unimportant information about line numbers for error
# reporting. It is useful not to rerun sage if this is the only
# information that has changed in the .sage file.  So the
# hash_calc_ignore_pattern variable is used to configure latexmk to
# ignore this lines when computing whether the .sage file has
# changed.
```

- `siunitx`: units and numbers, e. g. 10000000 vs. 100 000 000
- `cleverref`: The cleveref package enhances LaTeX's cross-referencing features, allowing the format of cross-references to be determined automatically according to the "type" of cross-reference (equation, section, etc.) and the context in which the cross-reference is used. (description taken from the package doc)

misc

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

misc

- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  ```
  \newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}
  ```

misc

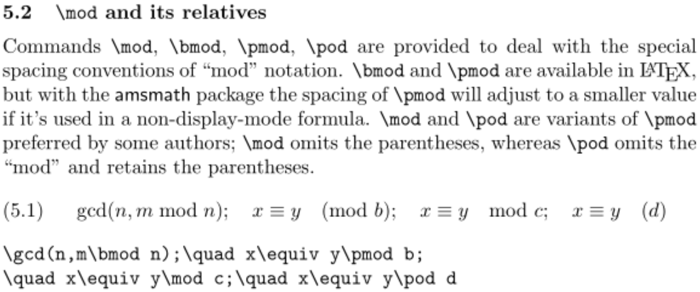
- newcommand: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  `\newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}`
- take your time and read the documentation of amsmath before producing larger amounts of math . . .

misc

- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:

  ```
  \newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}
  ```

- take your time and read the documentation of `amsmath` before producing larger amounts of math . . .



5.2 \mod and its relatives

Commands \mod, \bmod, \pmod, \pod are provided to deal with the special spacing conventions of "mod" notation. \bmod and \pmod are available in LaTeX, but with the amsmath package the spacing of \pmod will adjust to a smaller value if it's used in a non-display-mode formula. \mod and \pod are variants of \pmod preferred by some authors; \mod omits the parentheses, whereas \pod omits the "mod" and retains the parentheses.

$$\gcd(n,m\bmod n);\quad x\equiv y\pmod b;\quad x\equiv y\mod c;\quad x\equiv y\pod d \tag{5.1}$$

```
\gcd(n,m\bmod n);\quad x\equiv y\pmod b;
\quad x\equiv y\mod c;\quad x\equiv y\pod d
```

misc

- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  ```
  \newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}
  ```
- take your time and read the documentation of `amsmath` before producing larger amounts of math . . .

  . . . or even buy a book:

  https://www.dante.de/dante-e-v/literatur/mathematiksatz/

misc

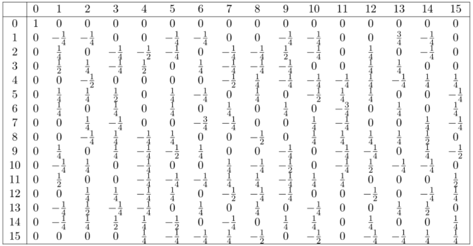
- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  `\newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}`
- take your time and read the documentation of `amsmath` before producing larger amounts of math . . .
- urlbreaks: package `xurl`

misc

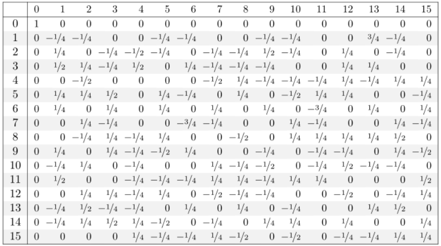
- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  `\newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}`
- take your time and read the documentation of `amsmath` before producing larger amounts of math ...
- urlbreaks: package `xurl`
- linkcolor: just not blue and underlined ;-) change it e. g. like this:
  `\hypersetup{colorlinks=true,urlcolor=blue!50!black,linkcolor=brown}`

misc

- `newcommand`: over 200 occurrences, many not even used once; some authors like to reinvent the wheel:
  `\newcommand{\mmod}{\hspace{1mm}{\rm mod}\hspace{1mm}}`
- take your time and read the documentation of `amsmath` before producing larger amounts of math …
- urlbreaks: package `xurl`
- linkcolor: just not blue and underlined ;-) change it e. g. like this:
  `\hypersetup{colorlinks=true,urlcolor=blue!50!black,linkcolor=brown}`
- tables old vs. new



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{3}{4}$	$-\frac{1}{4}$	0
2	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{2}$	$-\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0
3	0	$\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0	0
4	0	0	$-\frac{1}{2}$	0	0	0	0	$-\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
5	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$
6	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{3}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$
7	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{3}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$
8	0	0	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
9	0	$\frac{1}{4}$	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	$\frac{1}{4}$	0	0	$-\frac{1}{4}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	$-\frac{1}{2}$
10	0	$-\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0
11	0	$\frac{1}{2}$	0	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	0	$\frac{1}{2}$
12	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	0	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$\frac{1}{4}$
13	0	$-\frac{1}{4}$	$\frac{1}{2}$	$-\frac{1}{4}$	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{2}$	0
14	0	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$
15	0	0	0	0	$\frac{1}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	$-\frac{1}{2}$	0	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	−1/4	−1/4	0	0	−1/4	−1/4	0	0	−1/4	−1/4	0	0	3/4	−1/4	0
2	0	1/4	0	−1/4	−1/2	−1/4	0	−1/4	−1/4	1/2	−1/4	0	1/4	0	−1/4	0
3	0	1/2	1/4	−1/4	1/2	0	1/4	−1/4	−1/4	−1/4	0	0	1/4	1/4	0	0
4	0	0	−1/2	0	0	0	0	−1/2	1/4	−1/4	−1/4	−1/4	1/4	−1/4	1/4	1/4
5	0	1/4	1/4	1/2	0	1/4	−1/4	0	1/4	0	−1/2	1/4	1/4	0	0	−1/4
6	0	1/4	0	1/4	0	1/4	0	1/4	0	1/4	0	−3/4	0	1/4	0	1/4
7	0	0	1/4	−1/4	0	0	−3/4	−1/4	0	0	1/4	−1/4	0	0	1/4	−1/4
8	0	0	−1/4	1/4	−1/4	1/4	0	0	−1/2	0	1/4	1/4	1/4	1/4	1/2	0
9	0	1/4	0	1/4	−1/4	−1/2	1/4	0	0	−1/4	0	−1/4	−1/4	0	1/4	−1/2
10	0	−1/4	1/4	0	−1/4	0	0	1/4	−1/4	−1/2	0	−1/4	1/2	−1/4	−1/4	0
11	0	1/2	0	0	−1/4	−1/4	−1/4	1/4	1/4	−1/4	1/4	1/4	0	0	0	1/2
12	0	0	1/4	1/4	−1/4	1/4	0	−1/2	−1/4	−1/4	0	0	−1/2	0	−1/4	1/4
13	0	−1/4	1/2	−1/4	−1/4	0	1/4	0	1/4	0	−1/4	0	0	1/4	1/2	0
14	0	−1/4	1/4	1/2	1/4	−1/2	0	−1/4	0	1/4	1/4	0	1/4	0	0	1/4
15	0	0	0	0	1/4	−1/4	−1/4	1/4	−1/2	0	−1/2	0	−1/4	−1/4	1/4	1/4

to-do-list

How I got involved . . .

tasks

Inventory taking (May 2018)

Arara

transision from `bibtex` zu `biblatex`

transition from pdflatex to lualatex

lengths, pagebreaks, indents etc.

switching to KOMA

(some of the) introduced packages

misc

to-do-list

to-do-list

- english
- sage
- pictures
- integrate lattices
- font
- layout
- tagged PDF, accessibility