Einführung in das Mathematikstudium und dessen Umfeld

LVA 405.000

C. Fuchs (gemeinsam mit A. Bathke, V. Bögelein, C. Buchta, A. Schröder)

Lehrveranstaltungsunterlagen **WS 2020/21**

Es werden folgende Themen besprochen: Kennenlernen der für das Studium relevanten Personen und Institutionen (z.B. Universität, ÖH), Kennenlernen des Curriculums, Tools zur Suche mathematischer Literatur, Einführung in mathematische Software, Vorstellung der verschiedenen Fachgebiete (Analysis, Diskrete Mathematik, Geometrie, Statistik/Stochastik, Technische Mathematik, Aktuarausbildung), Wiederholung von ausgewählten Teilen des Schulstoffes.

Inhaltsverzeichnis

Bei Fragen oder Bemerkungen (speziell Hinweise auf Fehler aller Art sind willkommen) schicken Sie ein Email an clemens.fuchs@sbg.ac.at. Dieses Dokument wurde unter Mithilfe von Melanie Löckinger (Studienassistentin am FB Mathematik im WS16/17) erstellt.

1 Einführung in die Lehrveranstaltung

1.1 Das 1. Semester

Es sind die folgenden Lehrveranstaltungen zu besuchen:

- STEOP: Einführung in das Mathematikstudium und dessen Umfeld (Bachelor), 2VU
- STEOP: Grundlagen der Mathematik, 3VU
- Diskrete Mathematik, 2VO+1UE
- STEOP: Analysis I, 5VO+2UE
- Einführung in die Programmierung, 3VO+2PS
- Freie Wahlfächer

Es sei bemerkt, dass die mit STEOP gekennzeichneten Lehrveranstaltungen absolviert werden müssen bevor eine endgültige Zulassung zum Studium erfolgt. Vor der Absolvierung dürfen nur Lehrveranstaltung im Umfang von 22 ECTS-Anrechnungspunkten absolviert werden; weitere Prüfungen können vor Beendigung der STEOP nicht abgelegt werden (eine Anmeldung über PLUSonline ist nicht möglich).

1.2 Kontakte

Informationen zum Studium findet an folgenden Stellen; es sind jeweils Ansprechpersonen inklusive der E-Mail-Adressen angegeben:

- Webseite des Fachbereichs Mathematik: www.uni-salzburg.at/mathematik
- **Studienberater:** Assoz.-Prof. Dr. Volker Ziegler, studienberater.math@sbg.ac.at
- **Sekretariat des Fachbereichs Mathematik:** Beatrice Haring, beatrice.haring@sbg.ac.at
- **ÖH-Vertretung Mathematik:** stv.mathe@oeh-salzburg.at
- **Mobilitätsbeauftragter:** Assoz.-Prof. Dr. Volker Ziegler, volker.ziegler@sbg.ac.at
- **Disability & Diversity:** DI Bettina Sereinig, bettina.sereinig@sbg.ac.at
- **Fachbereichsleiter:** Univ.-Prof. Dr. Andreas Schröder, andreas.schroeder@sbg.ac.at
- **Vorsitzender der Curricularkommission:** Univ.-Prof. Dr. Clemens Fuchs, clemens.fuchs@sbg.ac.at
- **Anrechnung von Prüfungen aus anderen Studien (§78 UG 2002):** Ao.Univ.-Prof. Dr. Wolfgang Schmid, wolfgang.schmid@sbg.ac.at

1.3 Berufsaussichten für Mathematiker/innen

Es gibt sehr gute Berufsaussichten. Denn:

- Kein Fortschritt ohne Mathematik
- Mathematiker sind gefragter denn je
- Mathematik als Schlüsselqualifikation
- Mathematiker bohren dicke Bretter
- Querdenken, Ideentransfer und Innovation
- Mathematische Modelle und Simulationen ersetzen Prototypen und Experimente
- Mathematikstudierende werden mehr
- Mathematiker müssen sich oft erst durchsetzen
- Die traditionellen Branchen und Berufe für Mathematiker...
- ...und die neuen Tätigkeitsbereiche
- Interdisziplinäres Denken und Arbeiten wird immer wichtiger

1.4 Vorlesungen, Übungen, Tutorien etc.

Die wichtigsten Lehrveranstaltungstypen sind die folgenden:

- **Vorlesung (VO)** gibt einen Überblick über ein Fach oder eines seiner Teilgebiete sowie dessen theoretische Ansätze und präsentiert unterschiedliche Lehrmeinungen und Methoden. Die Inhalte werden überwiegend im Vortragsstil vermittelt. Eine Vorlesung ist nicht prüfungsimmanent und hat keine Anwesenheitspflicht.
- **Vorlesung mit Übung (VU)** verbindet die theoretische Einführung in ein Teilgebiet mit der Vermittlung praktischer Fähigkeiten. Eine Vorlesung mit Übung ist nicht prüfungsimmanent und hat keine Anwesenheitspflicht.
- **Übung(UE)** dient dem Erwerb, der Erprobung und Perfektionierung von praktischen Fähigkeiten und Kenntnissen des Studienfaches oder eines seiner Teilbereiche. Eine Übung ist eine prüfungsimmanente Lehrveranstaltung mit Anwesenheitspflicht.
- **Übung mit Vorlesung (UV)** verbindet die theoretische Einführung in ein Teilgebiet mit der Vermittlung praktischer Fähigkeiten, wobei der Übungscharakter dominiert. Die Übung mit Vorlesung ist eine prüfungsimmanente Lehrveranstaltung mit Anwesenheitspflicht.
- **Seminar (SE)** ist eine wissenschaftlich weiterführende Lehrveranstaltung. Sie dient dem Erwerb von vertiefendem Fachwissen sowie der Diskussion und Reflexion wissenschaftlicher Themen anhand aktiver Mitarbeit seitens der Studierenden. Ein Seminar ist eine prüfungsimmanente Lehrveranstaltung mit Anwesenheitspflicht.

- **Proseminar**
- **Konversatorium**
- Tutorium

1.5 Leitfaden für Übungen und Proseminare

Übungen stellen einen wesentlichen Teil der Ausbildung im Mathematikstudium dar. Sie helfen nicht nur den Stoff der Vorlesungen besser zu verstehen, sondern sie erweitern auch das Wissen und sorgen für die notwendigen Rechenfertigkeiten. Zudem wir an vielen Stellen die Fähigkeit mathematische Schlüsse korrekt und nachvollziehbar anzugeben trainiert. Im folgenden sind einige Tipps zur erfolgreichen Teilnahme an Übungen zusammengestellt.

1.5.1 Herangehensweise zum Lösen von Übungsaufgaben

- Es wird von Ihnen das Lösen von Aufgaben erwartet, möglicherweise ohne vorher auch nur ein einziges ausgearbeitetes Beispiel gesehen zu haben.
- Rechtzeitig und nicht erst im letzten Moment mit dem Bearbeiten der Aufgaben beginnen.
- Legen Sie sich zuerst die dazugehörige Theorie zurecht. Die Aufgaben sind im Allgemeinen (und gerade am Studienanfang) insofern speziell, da sie in der Regel einen eng abgesteckten Theoriehintergrund haben, der zur Lösung der Aufgabe ausreicht.
- Klären Sie zuerst, was die in der Angabe vorkommenden Begriffe bedeuten (falls Sie die Definitionen nicht ohnehin parat haben). Was sind die Ergebnisse, die in der Vorlesung zu diesen Begriffen gemacht worden sind?
- Versuchen Sie die Aufgaben zuerst selbst zu lösen. Sind Sie dabei erfolgreich, so haben Sie den größten Nutzen!
- Falls Sie mit einer Aufgabe nicht weiterkommen, können Sie natürlich im Internet oder in der Bibliothek recherchieren.
- Bilden Sie mit Kolleg/inn/en Arbeitsgruppen, um gemeinsam über die Aufgaben (insbesondere auch die anspruchsvolleren) nachzudenken.

1.5.2 Vor der Übung

- Wie gut haben Sie die Beispiele vorbereitet?
- Sind Ihre Überlegungen klar strukturiert und logisch nachvollziehbar?
- Können Sie jeden einzelnen Rechenschritt begründen? (Sie können das Erklären von Rechenschritten zuvor mit Ihren Kolleg/inn/en üben.)

- Haben Sie Ihre Lösung mit jener von Kolleg/inn/en verglichen?
- Sind Ihre schriftlichen Unterlagen klar gegliedert und für Sie gut lesbar, wenn Sie dann an der Tafel stehen?

1.5.3 In der Übung

- Konzentrieren Sie sich auf die Bemerkungen des Übungsleiters/der Übungsleiterin. Er/sie weist auf wichtige Dinge und Fallstricke hin.
- Falls Sie etwas nicht verstanden haben oder es bei einer Aufgabe Verständnisschwierigkeiten gegeben hat, **nützen Sie die Übungsstunde um nachzufragen!**
- Beachte Sie, dass auch jene Aufgaben, die aus Zeit- oder anderen Gründen nicht in der Übungsstunde behandelt werden, prüfungsrelevant sind/sein können.

1.5.4 An der Tafel

- Haben Sie den Angabezettel (und allenfalls Ihre eigenen Unterlagen) dabei?
- Schreiben Sie leserlich?
- Ist Ihr Tafelbild übersichtlich?
- Halten Sie die aktuelle Tafel im Vordergrund?
- Sprechen Sie in angemessener Lautstärke, sodass Ihre Ausführungen für alle gut hörbar sind?
- Haben Sie die Nummer der Aufgabe und eine kurze Wiederholung der Angabe aufgeschrieben?
- Haben Sie die Angabe erklärt?
- Können Sie einen Überblick über Ihre Vorgangsweise bzw. Ihren Lösungsweg geben?
- Haben Sie etwaige Fallunterscheidungen klar formuliert und aufgeschrieben?
- Haben Sie jene Resultate der Vorlesung bereit, die Sie in Ihrer Rechnung/Ihrem Beweis verwenden?
- Kennen Sie die Definitionen jener mathematischen Objekte, die in der Aufgabe vorkommen (z.B.: wissen Sie, was die reellen Zahlen sind, falls diese in der Aufgabe eine wichtige Rolle spielen)?

1.5.5 Wie gehen Sie mit dem Erfolg oder Misserfolg beim Vorrechnen um?

- Haben Sie geklärt, ob Ihre Leistung als Erfolg oder als Misserfolg gewertet wird?
- Haben Sie Ihren Erfolg gefeiert?
- Haben Sie Ihren Misserfolg analysiert und verdaut? Sie sollten reflektieren: Was ist Ihre Motivation für dieses Studium? Warum tun Sie sich diese Arbeit an?

1.5.6 Prüfungsbedingungen

- Kennen Sie die genauen Prüfungsbedingungen?
- Wissen Sie bis wann und wo Sie Ihre Kreuze setzen sollen?
- Wird man zu den einzelnen Aufgaben aufgerufen oder kann man sich freiwillig melden?
- Darf man an der Tafel die eigenen Unterlagen verwenden?
- Wie viel Prozent der Aufgaben muss man angekreuzt haben?
- Gibt es einen (oder mehrere) Tests?
- Wie wird die Endnote aus der Leistung an der Tafel, der Note auf etwaige Tests usw. berechnet?
- Wie oft darf man fehlen? Welche Bedingungen gelten im Krankheitsfall?

2 Einführung in LaTeX

2.1 Microsoft Word vs. LaTeX

- Word folgt dem WYSIWYG = "what you see is what you get"-Prinzip. LaTeX hingegen ist nicht WYSIWYG! Man sieht nämlich die Formatierung beim Schreiben nicht.
- Word: Üblicherweise Buttons/Menüs zum Formatieren
  LaTeX: Kommandos.
- Code muss dann erst interpretiert werden (=compilieren), um das Layout zu sehen.
- Mit LaTeXerhält man ein professionelles Layout. Die Formatierung mathematischer Formeln ist sehr leicht und sieht schön aus (schon mal in Word probiert?!?).
- Das Programm ist kostenlos & open source.
- BibTeX u.a. Referenzierungen können leicht organisiert werden.
- **Vor allem: LaTeXist DER STANDARD in Mathematik für schriftliche Arbeiten.**

Fast alles kann auf die eigenen Bedürfnisse angepaßt werden. Am Anfang empfiehlt es sich, bei einer passenden Vorlage zu bleiben. Änderungen können z.B. mit den Befehlen newcommand, newenvironment im Frontmatter vorgenommen werden.

2.2 Literaturempfehlungen

Informationen und Manuals unterschiedlicher Länge finden Sie z.B. hier:
http://www-h.eng.cam.ac.uk/help/tpl/textprocessing/LaTeX_intro.html
Weitere Quelen sind Internet (Google, Wikipedia, etc.), eigentlich keine Literatur, aber sehr kompakt und fast vollständig: *http://en.wikibooks.org/wiki/LaTeX/Mathematics*, für Einsteiger: Kopka H. (2002). LaTeXBand 1: Einführung. Pearson Studium, München, wer es genauer wissen will: Grätzer, G. (1996). Math into LaTeX: an introduction to LaTeXand AMS-LaTeX. Birkhäuser, Boston, Mass. Sehr zu empfehlen ist eine Online-Recherche - für fast alle Fragen gibt es eine Antwort!

2.3 Get Started

In LaTeXwird eine Textdatei mit Endung .tex und mit Inhalt geschrieben:

- Buchstaben A,...,Z; a,...z; Ziffern 0,...,9 und mathematische Zeichen: + = | < >
- Satzzeichen: . : ; . ? ! ‘ ’ “ ( ) [ ] - / * @
- Sonderzeichen: # $ % & _ {} ∼ ˆ \
  Die Sonderzeichen haben alle eine Funktion (später mehr dazu; z.B. leitet % einen Kommentar ein); um die Sonderzeichen zu produzieren setzt man einen Backslash \ davor also z.B. \&

3 LaTeX-Befehle

Alle Befehle beginnen mit einem Backslash. Benötigt ein Befehl mehr Information, dann werden geschwungene Klammern verwendet. Sollen Optionen verwendet werden, dann kommen sie in eckige Klammern vor den geschwungenen Klammern.
Ein * nach dem Befehlsnamen unterdrückt die Nummerierungen.
Leerzeichen nach Befehlen ohne (leere geschwungene) Klammern werden ignoriert.
Geschwungene Klammern werden auch verwendet, um die Wirkung eines Befehls zu begrenzen.

Ein LaTeXDokument startet mit der Definition der Dokumentenklasse, der Text beginnt mit \begin{document} und endet mit \end{document}; dazwischen können noch weitere Frontmatters wie das Zuladen von Packeten geschaltet sein; also:

```
\documentclass[12pt,fleqn]{article}
\begin{document}
Hello World
\end{document}
```

3.1 Dokumentklassen, Optionen, Zusatzpakete

Die meistverwendeten Dokument-Klassen sind: article, report, book, letter, slides, proc, minimal und beamer.

- default Schriftgröße: 10pt; 11pt und 12pt können gewählt werden, größere Schriftgrößen müssen definiert werden
- weitere Optionen z.B. a4paper, letterpaper, fleqn, leqno, titlepage, notitlepage, onecolumn, twocolumn, twoside, oneside, etc.

Zusatzpakete werden mit dem Befehl \usepackage geladen. Beispiele für solche Packete sind:

- fontenc: spezifiert das Font-Encoding, das von LaTeX verwendet wird.
- inputenc: mit der Option utf8, damit Umlaute von deutschsprachigen Tastaturen richtig übernommen werden
- Babel mit der Option german lädt ein Packet zur Unterstützung der deutschen Sprache.
- graphicx

3.2 .tex-Dateien interpretieren

Die folgenden Befehle müssen in einem cmd-Fenster auf der Command-Line eingegeben werden:

1. latex helloworld.tex

2. evt. muss dies öfter gemacht werden wenn Referenzen Teil der Datei sind (Inhaltsverzeichnis, Literaturverzeichnis...)

3. Ansicht des dvi-files mit z.B. xdvi helloworld.dvi
   oder konvertiere dvi in ps Datei dvips -o helloworld.ps helloworld.dvi
   oder konvertiere ps in pdf Datei ps2pdf helloworld.ps
   Alternativen: pdflatex bzw. entsprechende Kommandos in der Entwicklungsumgebung

Es werden viele weitere Dateien beim compilieren erzeugt, z.B.: .dvi, .log, .toc, .lof, .lot, .aux, .idx, .ind.
Zudem haben noch Files mit der Endung .sty, .dtx, .ins, .cls, .fd eine spezielle Bedeutung.

3.3 Strukturierung

3.3.1 Kapitel und Unterkapitel

\section{Kapitel} \subsection{Unterkapitel}
\appendix gibt an, dass nun der Anhang beginnt, erzeugt aber keine Überschrift.
\tableofcontents erzeugt ein Inhaltsverzeichnis.

Es kann weiter unterteilt werden nach subsubsection, subsubsubsection etc. und mit \part, \chapter, \paragraph, \subparagraph, wobei nicht jedes Kommando in jeder Dokumentenklasse verfügbar ist.
Um Nummerierung zu unterdrücken fügt man ein * ein z.B. \section*{Kapitel}.

3.3.2 Umgebungen

Umgebungen werden mit \begin{Name} ... \end{Name} definiert.
Mögliche Umgebungen wären:

- quote - wörtliches Zitat
- verbatim - typographischer Text
- itemize - Aufzählung (Diese Liste hier ist z. Bsp. eine Aufzählung mit “itemize“)
- enumerate - Numerierung
- description - Aufzählung mit fett gedrucktem Begriff zu Beginn jedes Elements

LaTeX ist besonders gut geeignet um mathematische Texte zu verfassen. Diese mathematischen Umgebungen eignen sich besonders dafür:

- für Formeln: displaymath (ohne Numerierung) und equation (mit Numerierung)
- ist die Formelzeile zu lang, so verwendet man multiline oder split oder eqnarray

- man kann auch \[... \] statt \begin{displaymath} ... \end{displaymath} verwenden
- möchte man im Text eine Formel o.ä. angeben so macht man das mit \(... \) oder mit $ ... $
- oder auch mit \ensuremath
- proof für Beweise, inkl. end-of-proof Zeichen
- Theoreme, Sätze, Definitionen kann man selbst als Umgebung definieren und deren Numerierung anpassen
- \newtheorem{thmname}{angezText}
  definiert ein neues Theorem
- \newtheorem{thmname}{angezText}[section]
  Zähler startet bei jedem neuen Kapitel bei 1
- \newtheorem{thmname}{angezText}[nameZ] gibt dem Zähler einen Namen (nicht auf Kapitel bezogen)
- gemeinsame Numerierung: verweise auf Namen \newtheorem{thmname}[nameZ] {angezText}

3.4 Schrift

\textrm{römische Schrift}
\textsf{Schrift ohne Serifen}
\textsc{Kapitälchen Schrift}
\textit{*kursive Schrift*}
\footnotesize
\large
\LARGE
\Huge

\textbf{**fette Schrift**}
\textsl{*schräge Schrift*}
\texttt{`Schreibmaschinen-Schrift`}
\tiny \scriptsize
\small
\Large
\huge

Die Schriftgröße von \small etc. hängt aber von default Schriftgröße des Dokuments und der Kombination ab.

3.5 Tabulatur bzw. Tabellen

Die Umgebungen zur Erstellung von Tabellen wird mit tabbing oder tabular benannt. Der Text wird an Tabulatoren ausgerichtet.

Tabulatoren werden mit \= gesetzt und \¿ fügt den entsprechenden Leerraum ein (wie betätigen der Tab-Taste in Word)

Tabulatoren werden mit & definiert, müssen aber nicht gesetzt werden (Spaltenbreite wird von LaTeX angepasst)

Zeilen werden durch \\ oder durch \newline beendet (neue Zeile).

Der Befehl \newpage erzeugt eine neue Seite.

Möchte man die Tabelle visuell unterteilen so eignen sich horizontale Linien \hline oder vertikale Linien —.

3.6 Mathematische Kommandos

- tieferstellen mit _ und höherstellen mit ^
- Brüche mit / bzw. bei größeren Brüchen mit \frac{Zähler}{Nenner}
- oft genutzt außerdem
  - Summenzeichen $\sum$ \sum
  - Wurzel $\sqrt{x}$ \sqrt
  - Limes $\lim_{n\to\infty}$ \lim_{ n \rightarrow \infty}
  - Integral $\int_0^1$ \int_0^1
- array wird für Matrizen verwendet
- es gibt unterschiedliche Möglichkeiten, die Abstände innerhalb einer Formel selbst zu verändern
- mit \left ... \right können Klammern auf die Größe der sie umfassenden Ausdrücke eingestellt werden
- \arccos, \arcsin, \arctan, \arg, \sinh, \sec, \cos, \cosh, \cot, \coth, \, \sup, \sin, \csc, \deg, \det, \dim, \tan, \exp, \gcd, \hom, \inf, \tanh, \ker, \lg, \lim, \liminf, \min, \limsup, \ln, \log, \max, \Pr

Ausführliche Listen und Tabellen für mathematische Symbole findet man im Internet und in der Literatur.

3.7 Seitenformatierung

Der Grundbefehl ist von der Gestalt \setlength{Befehlsname}{Einheit} bzw. \addtolength{Befehlsname}{Einheit}. Es können dann folgende Befehle eingesetzt werden:

- Paragraphformatierung: \parindent, \parskip

- Seitenformatierung: \oddsidemargin, \evensidemargin, \hoffset, \voffset, \topmargin, \headheight, \headsep, \textheight, \textwidth, \marginparsep, \marginparwidth, \footskip

Verwendet werden gerne auch \indent und \noindent sowie \hspace bzw. *hspace und \vspace bzw. *vspace.

3.8 Bilder

Im Prinzip ähnelt die Funktionsweise für Bilder in LaTeX(figure) der Funktionsweise für Tabellen (table). LaTeX bestimmt für beide Komponenten den optimalen Platz.
Es gibt Optionen t, b, p, h und !: Mit diesen kann man Präferenzen für die Platzierung angeben (top, bottom, extra page, here, und ! verleiht dem Wunsch noch Nachdruck), also bei \begin{figure}[h!] sollte LaTeX das Bild genau hier platzieren.
Konvention ist, die Beschreibung/den Namen unter das Bild zu geben, aber über die Tabelle. Name und Beschreibung werden so angegeben: \caption{Text}

Möchte man Bilder einbinden, so muss das Paket graphicx (oder ein anderes Paket für Bilder) geladen werden mit \usepackage{graphicx}. Die möglichen Formate hängen vom Typesetting ab.

LaTeX dvi modus, dvips : eps

LaTeX dvi modus, dvipdfm(x) : pdf, png, jpeg, eps

pdfLaTeX pdf modus : pdf, png, jpeg, jbig2 (**empfohlen!**)

LuaTeX : kann außerdem jpeg 2000

Eventuell ist eine automatische Konvertierung durch inkludieren des epstopdf Pakets in der Präambel sinnvoll, dann werden eps Bilder automatisch in pdf Bilder konvertiert.

3.9 Referenzen

Damit sind Referenzen z.B. auf items einer Liste, auf Bilder oder ganze Kapitel gemeint. Diese werden erzeugt mit \label{name} wobei "Name" dann jener tag ist, den man später zum Referenzieren verwendet. Abgerufen wird mit \ref{name} bzw. \pageref{name}.
Wichtig ist, dass diese Referenzen in der entsprechenden Umgebung gesetzt werden (bei Bildern/Tabellen NACH caption).
Als Referenz gilt auch das Inhaltsverzeichnis, das (normalerweise zu Beginn) mit \tableofcontents erstellt wird. Analog gibt es \listoffigures, \listoftables.

3.10 Literaturlisten und deren Referenzierung

Hierfür gibt es zwei Möglichkeiten:

- semi-händisch

- BibTeX als separates Programm mit den entsprechenden .bib Dateien - Formatierung erfolgt automatisch

Referenziert werden die Einträge mit \cite{Referenz} und das Verzeichnis wird erzeugt mit \bibliography{NamebibDatei}, wobei auch mehrere Dateien angegeben werden können.

3.11 Übungsbeispiele

Zu veröffentlichende Arbeiten werden in der Mathematik meist mit der Documentclass "Article" oder "Amsart" geschrieben. Die Präambel eines Dokuments zu erstellen erfordert einiges an Zeit und Aufwand, bis alle benötigten Pakete von Ihnen erfasst wurden. Darum ist es von Vorteil, eine möglichst viel abdeckende Präambel immer wieder zu verwenden und gegebenfalls anzupassen.

Folgende Aufgaben sollen Ihnen den Umgang mit dem Programm näher bringen:

1. Dokument erstellen: Texen Sie eine kurze Präambel mit Documentclass und den Paketen amssymb,amsmath,german,amsfonts und mathrsfs. Beginnen Sie das Dokument und fügen Sie diesen Text ein: *Gestern war ein überaus schöner Tag.* Falls die Umlaute nicht (korrekt) angezeigt werden, laden Sie das Paket *inputenc* mit Option *utf8* und *fontenct* mit Option *T1* nach.

2. Gliederung: Gliedern Sie Ihr neu erstelltes Dokument in 1.Hobbys 2.Uni 3.Musik. Geben Sie die entsprechenden Unterkapitel an und erstellen Sie am Anfang des Dokuments ein automatisch generiertes Inhaltsverzeichnis. Listen Sie Ihre Hobbys mit dem Befehl \begin{itemize} in kursiver Schrift auf. Geben Sie drei Lieblingslieder an und nummerieren Sie diese.

3. Formeln: Texen Sie folgendes und unterdrücken Sie die Nummerierung:

$$\frac{1}{2}\cdot \iint\limits_{x^2+y^2\leq R^2} e^{-(x^2+y^2)}dxdy \quad = \frac{1}{2}\cdot \int\limits_0^{2\pi}\int\limits_0^{R} e^{-r^2(\cos^2\varphi+\sin^2\varphi)} r\ drd\varphi$$

$$\lim_{k\to 0}\frac{u(0,y+k)-u(0,y)}{k}+i\cdot\lim_{k\to 0}\frac{v(0,y+k)-v(0,y)}{k}=\frac{\partial u}{\partial y}+i\cdot\frac{\partial v}{\partial y}$$

4. Bilder: Fügen Sie unter 3. Musik ein 10 cm breites Bild Ihrer Lieblingsmusikgruppe ein, dieses sollte direkt unter der Liederliste erscheinen. Betiteln Sie das Bild mit "Beste Band". Geben Sie darunter einen kurzen Text über das neueste Album dieser Band. Fügen Sie am Ende des Dokuments noch ein Bildverzeichnis an.

5. Tabellen: Erstellen Sie eine Tabelle mit Titel, in der Sie Ihre aktuell besuchten Lehrveranstaltungen auflisten. Dabei sollte die 1. Spalte linksbündig und die vierte rechtsbündig sein. Alle Zeilen und Spalten sollten mit Linien voneinander getrennt sein.

Tabelle 1: Meine Lehrveranstaltungen

Titel	Leitung	ECTS-Punkte	Winter- oder Sommersemester
Analysis II	Blatt S.	7.5	Wintersemester

4 Ausblicke auf kommende Lehrveranstaltungen

In diesem Abschnitt werden exemplarische einige Gebiete des Mathematikstudiums aufgeführt. Genauere Informationen dazu, welche Lehrveranstaltungen wann im Studium vorgesehen sind findet man in der Broschüre "Studienführer für das Bachelorstudium Mathematik", welche in der LV ausgegeben wurde. Insbesondere sind darin Informationen zum modularen Aufbau des Studiums, zu Wahlmodulen und freien Wahlfächern zu finden. In zwei Anhängen werden Modulbeschreibungen von allen Modulen angegeben sowie Äquivalenzlisten, die insbesondere beim Übergang vom Curriculum 13W auf das neue Curriculum 16W hilfreich sein sollen.

4.1 Algebra

Die Algebra beschäftigt sich traditionell mit dem Gruppen, Ringen und Körper sowie mit deren Eigenschaften. Die Begriffe werden kurz erklärt:

Gruppen:
Sei G eine Menge und $+$ eine Operation auf G (d.h. eine Abbildung von G^2 nach G). Dann heißt $(G, +, 0)$ Gruppe, wenn folgende Gesetze gelten:

- **Assoziativität** $\forall a, b, c \in G : (a + b) + c = a + (b + c)$
- **Existenz eines neutralen Elements** $\exists e \in G : \forall a \in G : a + e = e + a = a$
  (Das neutrale Element wird üblicherweise mit 0 bezeichnet, wenn die Gruppenoperation $+$ ist; wird die Gruppenoperation mit $\cdot$ bezeichnet, so nennt man das neutrale Element 1.)
- **Existenz inverser Elemente** $\forall a \in G : \exists a^{-1} \in G : a + a^{-1} = a^{-1} + a = 0$

Gilt des weiteren, dass $\forall a, b, \in G : a + b = b + a$ (**Kommutativität**), so heißt $(G, +, 0)$ kommutative oder abelsche Gruppe.

Ringe:
Sei R eine Menge mit zwei Operationen $+$ und $\cdot$. $(R, +, \cdot)$ ist ein Ring, falls folgende Eigenschaften erfüllt sind:

- $(R, +, 0)$ ist eine **abelsche Gruppe**.
- **Assoziativität** $\forall a, b, c \in R : a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Distributivität** $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$ ebenso $(a + b) \cdot c = a \cdot c + b \cdot c$

Wenn zusätzlich gilt: $\forall a, b \in R : a \cdot b = b \cdot a$ so spricht man von einem **kommutativen** Ring. Ist des weiteren die Bedingung
$\exists n \in R : \forall a \in R : n \cdot a = a \cdot n = a$ erfüllt, so ist $(R, +, \cdot, 0, 1)$ ein kommutativer Ring mit **Einselement**. Üblicherweise wird n mit 1 bezeichnet.

Körper:
Ein kommutativer Ring mit Einselement K heißt Körper, falls K nullteilerfrei ist (=Integritätsbereich) und gilt: $\forall a \in K \backslash \{0\} : \exists a^{-1} \in K : a \cdot a^{-1} = 1$.

4.2 Differentialgleichungen

Eine Differentialgleichung ist eine Gleichung in der eine unbekannte Funktion und deren Ableitungen auftreten. Die Lösung einer Differentialgleichung ist eine Funktion, welche die Differentialgleichung erfüllt. Es gibt viele verschiedene spezielle Typen von Differentialgleichungen für die Lösungsverfahren bekannt sind (z.B. DGL mit getrennten Variablen, Bernoulli'sche DGL, Riccati'sche DGL, Clairaut'sche Differentialgleichung, lineare DGL mit konstanten Koeffizienten, etc.).

Differentialgleichungen mit getrennten, unabhängigen Variablen:

Wie kann folgende Diffenrentialgleichung gelöst werden?

$$y' = -\frac{x}{y}$$

Klar ist, dass gilt: $y \cdot y' = -x$ und $y' = \frac{dy}{dx}$
Durch weiteres Umformen

$$yy' = -x \Rightarrow y\,dy = -x\,dx \Rightarrow \int y\,dy = \int -x\,dx \Rightarrow \frac{y^2}{2} = -\frac{x^2}{2}c \Leftrightarrow y^2 + x^2 = 2c, \quad c \in R$$

erhält man eine Kreisgleichung, bzw. die Funktion in der exliziten Form: $y = \pm\sqrt{2c - x^2}$.

Exakte Differentialgleichungen und integrierender Faktor:

Folgende Differentialgleichung soll gelöst werden:

$$\tan y - 3x^2 + \frac{x}{\cos^2 y}y' = 0$$

Definiere $f_1 := \tan y - 3x^2$ und $f_2 := x/\cos^2 y$.

Lösungsansatz: Wir suchen eine Funktion $f(x, y)$ mit $f_x + f_y y' = 0$, wobei wir $f(x, y)$ Potential nennen. Das Integrabilitätskriterium für Exaktheit gibt eine Aussage über die Existenz einer solchen Funktion f: $(f_1)_y = 1/\cos^2 y = (f_2)_x$. Die Bestimmung der Stammfunktion erfolgt nun wie folgt: Zunächst integriert man f_1 nach x, wobei man y konstant

hält: $f_x = f_1 = \tan y - 3x^2 \Rightarrow f(x,y) = x\tan y - x^3 + C(y)$. Beachte, dass die Integrationskonstante eine Funktion von y ist, da y festgehalten wird. Durch Differenzieren von f nach x erhält man f_2. Somit ergibt sich $f_2 = \frac{x}{\cos^2 y} = f_x = \frac{x}{\cos^2 y} + C'(y) \Rightarrow C'(y) = 0 \Rightarrow C(y) = C = \text{konstant}$. Somit lautet die gesuchte Lösung $f(x,y) = x\tan y - x^3 + C$ und die gesuchte Lösung der Differentialgleichung ist gegeben durch $x\tan y - x^3 + C = 0$.

In vielen Fällen ist die Integrabilitätsbedingung $(f_1)_y = (f_2)_x$ nicht erfolgt, In diesem Fall kann oft mit einem Trick die DGL lösen, was wir im folgenden veranschaulichen.

Gelöst werden soll nun die folgende DGL:

$$y^2 - 3xy - 2x^2 + (xy - x^2)y' = 0$$

Wir definieren $f_1 := y^2 - 3xy - 2x^2$ und $f_2 := (xy - x^2)$.
Es folgt $(f_1)_y = 2y - 3x \neq y = (f_2)_x$. Multiplizieren wir aber die ganze Gleichung zunächst mit x, was die Lösung der ursprünglichen Gleichung nicht verändert, so ändert sich die Situation. Wir betrachten daher: $xy^2 - 3x^2y - 2x^3 + (x^2y - x^3)y' = 0$. Mit $f_1 = xy^2 - 3x^2y - 2x^3$, $f_2 = x^2y - x^3$ folgt $(f_1)_y = 2xy - 3x^2 = (f_2)_x$. Als Lösung findet man dann analog zu oben $f(x,y) = \frac{1}{2}x^2y^2 - x^3y - \frac{x^4}{2} - C = 0$ und somit $x^2y^2 - 2x^3y - x^4 = 2C$.

4.3 Numerik

In vielen wichtigen Fällen können Differentialgleichungen nicht gelöst werden. Sei $y' = f(x,y)$ gegeben und es sei bekannt, dass $y(x_0) = y_0$ ist. Da in jedem Punkt (x,y) die Steigung der Lösungskurve gegeben ist, kann zumindest näherungsweise eine Lösung bestimmt werden. Es ist also ein Richtungsfeld gegeben, für das jene Kurven $y = y(x)$ gesucht sind, deren Steigung in jedem Punkt vorgegeben ist.

Die Lösung kann dann z.B. mit dem Euler-Verfahren folgendermaßen näherungsweise berechnet werden: $x_n = x_0 + nh, y_n = y_{n-1} + hf(x_{n-1}, y_{n-1})$. Es handelt sich um ein Verfahren erster Ordnung, d.h. die Genauigkeit verhält sich nach $|y(x_n) - y_n| \leq \text{const} \cdot h$. Das Verfahren lässt sich auf folgende Weise verbessern: $x_n = x_0 + nh, y_n = y_{n-1} + h(f(x_n, y_n)$. Dazu muss nun in jedem Schritt die zweite Gleichung nach y_n aufgelöst werden, was z.B. mit dem Newton-Verfahren erfolgen kann. Man spricht vom impliziten Euler-Verfahren. Die Konvergenzordnung bleibt diesselbe, das Verfahren ist aber stabiler und daher auch für sogenannte steife DGL anwendbar.

Abgesehen vom numerischen Lösen von Differentialgleichungen beschäftigt sich die Numerik allgemeiner mit der Frage, wie die Mathematiktheorie sich verändert, wenn alle Berechnungen auf einem Computer durchgeführt werden. Da in einem Computer nicht alle Zahlen darstellbar sind, passiert in jedem Rechenschritt ein Fehler. Somit stehen Fragen wie Fehlerfortplanzung, Kondition, Stabilität und Konvergenz im Vordergrund.

4.4 Analysis

Einen wesentlichen Raum der Vorlesung in Analysis nimmt das Integrieren ein. Im Gegensatz zum Differenzieren gibt es beim Integrieren keinen allgemein anwendbaren Lösungsweg, allerdings kann mit einigen Methoden ein "kompliziertes" Integral ganz einfach gelöst werden. Außerdem werden noch weitere Integral-Arten eingeführt, wie zum Beispiel das Lebesgue-Integral.

Wir betrachten das folgende Beispiel: Die von zwei Variablen abhängige Funktion $e^{-(x^2+y^2)}$ soll über eine Kreisscheibe mit Radius R integriert werden (anschaulich wird die Fläche jenes zylindrischen Gebildes berechnet, die durch die x-y-Ebene und den Graphen der Funktion eingeschlossen wird). Wir setzen $x = r\cos(\varphi)$ und $y = r$
$sin(\varphi)$, $r \in \mathbb{R}$ und berechnen

$$\iint\limits_{x^2+y^2\leq R^2} e^{-(x^2+y^2)}dxdy = \int_0^{2\pi}\int_0^{R} e^{-r^2(\cos^2\varphi+\sin^2(\varphi))}r\ drd\varphi = \int_0^{2\pi}\int_0^{R} e^{-r^2\cdot 1}r\ drd\varphi$$
$$= 2\pi\cdot\int_0^{R} r\cdot e^{-r^2}dr;$$

dabei gilt $dxdy = rdrd\varphi$ aufgrund der Substitutionsregel für Mehrfachintegrale. Nun kann weiter $z = -r^2$ substituiert werden. Es folgt $z := r^2 \Leftrightarrow \frac{dz}{dr} = -2r \Leftrightarrow dr = -\frac{dz}{2r}$ und somit

$$2\pi\cdot\int_0^{R} r\cdot e^{-r^2}dr = -2\pi\cdot\int_0^{-R^2} e^z\cdot\frac{1}{2r}\cdot r\cdot dz = -\pi\cdot(e^z|_0^{-R^2}) = -\pi\cdot(e^{-R^2}-e^0) = -\pi\cdot e^{-R^2}+\pi$$

Für $R\to\infty$ gilt:

$$\iint\limits_{\mathbb{R}^2} e^{-(x^2+y^2)}dxdy = \pi$$

Daraus folgt

$$\iint\limits_{\mathbb{R}^2} e^{-(x^2+y^2)}dxdy = \int_\infty^{-\infty} e^{-y^2}\left(\int_\infty^{-\infty} e^{-x^2}dx\right)dy = \int_\infty^{-\infty} e^{-x^2}dx\cdot\int_\infty^{-\infty} e^{-y^2}dy = \left(\int_\infty^{-\infty} e^{-x^2}dx\right)^2$$

und somit $\int\limits_\infty^{-\infty} e^{-x^2}dx = \sqrt{\pi}$.

4.5 Funktionentheorie

Die Funktionentheorie befasst sich mit komplexwertigen Funktionen, deren Variablen ebenfalls komplex sind. Sie kann also als "Analysis in $\mathbb{C}$" interpretiert werden.

Wann sind komplexwertige Funktionen differenzierbar?

Sei U eine offene Teilmenge von $\mathbb{C}$, $z \in \mathbb{C}$ und $f : U \to \mathbb{C}, z \mapsto f(z)$ eine komplexwertige Funktion. Da $z \in \mathbb{C}$ gilt $z = x + iy,\ x, y \in R$. Daher können wir f folgendermaßen schreiben
$f(z) = f(x + iy) := u(x, y) + iv(x, y)$ mit $u, v : \mathbb{R}^2 \to \mathbb{R}$ und $x, y, \in R$

Zuerst bilden wir die Ableitungen entlang der reellen und der komplexen Achse:
$\mathrm{Re}(z) = x$:

$$\begin{aligned}\lim_{h\to 0} \frac{f(z+h) - f(z)}{h} &= \lim_{h\to 0} \frac{u(x+h, y) + iv(x+h, y) - (u(x, y) + iv(x, y))}{h} \\ &= \lim_{h\to 0} \frac{u(x+h, y) - u(x, y)}{h} + i \lim_{h\to 0} \frac{v(x+h, y) - v(x, y)}{h} = u_x + iv_x;\end{aligned}$$

$\mathrm{Im}(z) = y$:

$$\begin{aligned}\lim_{k\to 0} \frac{f(z+ik) - f(z)}{ik} &= \lim_{k\to 0} \frac{u(x, y+k) + iv(x, y+k) - (u(x, y) + iv(x, y))}{ik} \\ &= \lim_{k\to 0} \frac{u(x, y+k) - u(x, y)}{ik} + \lim_{k\to 0} \frac{v(x, y+k) - v(x, y)}{k} = \frac{1}{i} u_y + v_y \\ &= v_y - iu_y.\end{aligned}$$

Ein sinnvoller Ableitungsbegriff für komplexwertige Funktionen hat sicher zur Folge, dass die (Richtungs-)Ableitung in einem Punkt stets gleich ist; somit folgt durch Vergleich von Real- und Imaginärteil: $u_x = v_y$ und $u_y = -v_x$. Dieses Differentialgleichungssystem nennt man die Cauchy-Riemannschen Differentialgleichungen. Eine komplexe Funktion ist nun (komplex) differenzierbar, wenn die Cauchy-Riemannschen Differentialgleichungen gelten. Es gibt eine Reihe von äquivalenten Bedingungen, welche die Funktionentheorie zu einer der schönsten und faszinierensten Teilgebiete der Mathematik machen.

4.6 Übungsbeispiele

Lösen Sie folgende Differentialgleichungen in getrennten Variablen.

1. $y' = 2 \cdot \frac{y}{x}$
2. $y' = x \cdot \sqrt{y}$
3. $y' = 1 + x^2$
4. $y' = 1 + y^2$ unter der Bedingung, dass $y(0) = -1$
5. $y' = \frac{2x}{(x^2+1)} \cdot y^2$ (Substitutionsregel beim Integrieren!)

TIPP: Falls das Lösen von Differentialgleichungen neu für Sie sein sollte, wäre ein Blick auf Kapitel 4.2 Differentialgleichung sicherlich hilfreich. Die Variablen x und y müssen erst getrennt werden, damit anschließend ein zielführendes Integrieren gelingen kann.

5 Vorstellung der AG Diskrete Mathematik

5.1 Die AG Diskrete Mathematik

Worum geht es?

- Warum bietet Homebanking weitgehende Sicherheit?
- Warum vertragen DVD's Kratzer?
- Wie findet man effizient die Zerlegung großer Zahlen wie 1886052346252777 in Primzahlen?
- Wie tauschen Alice und Bob über eine unsichere Internet-Verbindung einen geheimen Schlüssel aus?
- Warum hat die Diophantische Gleichung $x^k + y^k = z^k$ für $k \geq 3$ keine nicht-trivialen Lösungen in natürlichen Zahlen x, y, z?

All diese Fragen werden mit Methoden der diskrete Mathematik beantwortet.

Die folgenden Lehrveranstaltungen werden von der AG Diskrete Mathematik betreut: Grundlagen der Mathematik, Diskrete Mathematik, Schulmathematik Grundlagen und Diskrete Mathematik, Zahlentheorie, Schulmathematik Zahlen und Zahlenbereiche, Lineare Algebra I, Lineare Algebra II und Geometrie, Algebra I, Algebra II, Höhere Algebra und Zahlentheorie. Zusätzliche werden Spezialvorlesungen und Seminare aus den Forschungsbereichen der AG als Wahlfächer angeboten, wie etwa "Mathematische Kryptografie", "Endliche Körper und Codierung", "Ergänzungen zur linearen Algebra", "Universelle Algebra", "Irrationalität und Transzendenz", "Elementare algebraische Geometrie" sowie "Elliptische Kurven". Wir betreuen Sie gerne beim Verfassen der Abschlussarbeit (Bachelor- und Masterarbeit) und können dafür interessante Themen anbieten.

Unsere Absolvent/inn/en arbeiten in den Bereichen Universität und FH, Datensicherheit (Banken, Internetprovider, Bundesheer), Lehrer/innen an der AHS, öffentliche Verwaltung, Energieversorger (z.B. Salzburg AG), Consulting (z.B. accenture).

5.2 Beispiel: Algebraische Codierungstheorie

Grundaufgabe: Information soll über einen fehlerbehafteten Kanal vom einem Sender zum Empfänger gesendet werden.

Bsp.: gesprochene Nachricht, Funk, Audiosysteme, Fernsehen, Computernetze, Satellitenkommunikation, Datenspeicherung, usw.

Ziel: man möchte erkennen können, ob (zufällige) Fehler aufgetreten sind und diese ggf. korrigieren. Achtung: Ensteht ein "sinnvoller" Fehler, kann die Codierungstheorie hier nicht eingreifen.

Bsp.: Apt natural. I have a gub. (von Woody Allen's Film "Take the money and run").

Um Fehler zu erkennen bzw. zu korrigieren, werden die folgenden beiden Prinzipien angewandt:

- Redundanz,
- Grammatik.

Diese Prinzipien sind uns von der natürlichen Sprache her wohlbekannt.

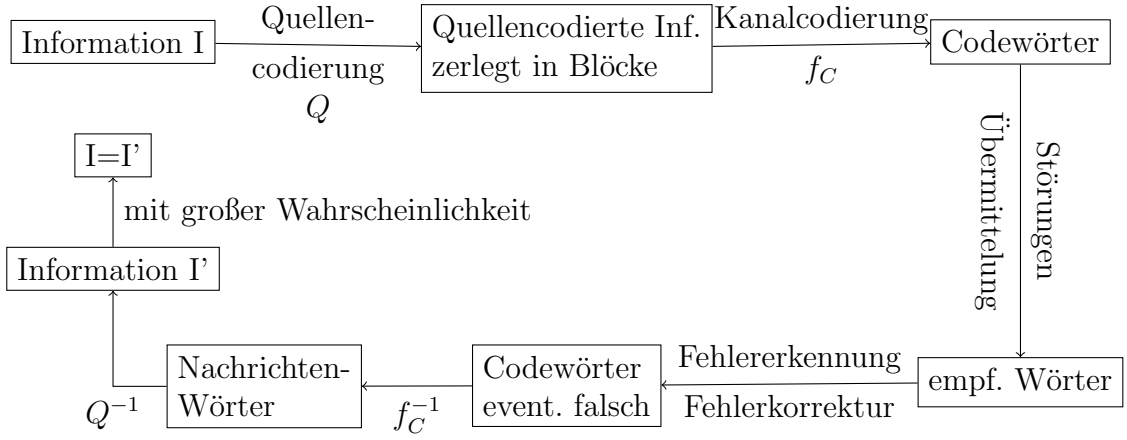

Abbildung 1: Codierungsschema

Durch die Quellencodierung wird die Information in eine Form gebracht, welche über den Kanal übertragen werden kann. Insbesondere soll sie:

- bewerkstelligen, dass alle gesandten Symbole mit ungefähr der gleichen Wahrscheinlichkeit auftreten,
- optimale Ausnützung der Übertragungskapazität des Kanals,
- event. Komprimieren der Information.

Bsp.: ASCII-Code; CD (Audiosignal wird 44.100 mal pro Sekunde abgetastet und der gefundene Wert in eines von $2^{16} = 65536$ Niveaus eingeordnet, Datenstrom aus Bytes "Alphabet" A mit 256 Buchstaben); Bildübertragung (sequentielle Anordnung der Bildpunkte, Farbe/Graustufe eines Bildpunkts = r-Tupel aus 0 und 1; Datenstrom aus Bits "Alphabet" $A = \{0, 1\}$, Datenstrom aus Buchstaben aus einem Alphabet A: stets Einteilung in Blöcke = "Wörter" zu k Buchstaben).

Im folgenden: eine Nachricht sei aus den *Symbolen* einer festen, endlichen Menge A aufgebaut (*Alphabet*); das Alphabet soll ein *Nullsymbol* besitzen, welches wir mit 0 bezeichnen; Elemente von A^n nennen wir *Wörter* der Länge n über dem Alphabet A.

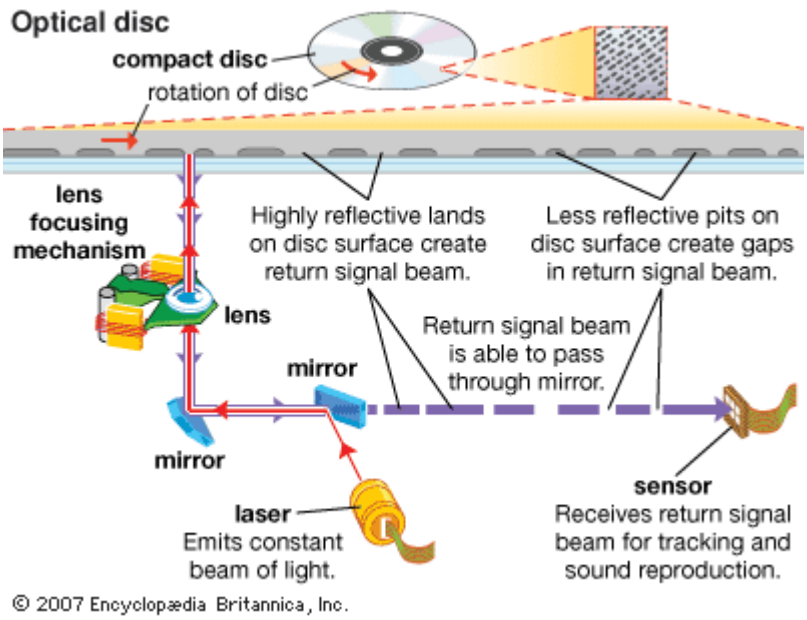

Abbildung 2: Funktionsweise einer CD

Um das Alphabet mit einer Grammatik auszustatten, verwenden wir einen endlichen Körper mit n Elementen. Es lässt sich zeigen, dass dann notwendigerweise $n = p^k$ mit $p \in \mathbb{P}, k \in \mathbb{N}$ ist. Der einfachste Fall, den wir im folgenden in den Beispielen stets verwenden werden, ist $n = 2$. Somit ist $A = \mathbb{F}_2 = \{0, 1\}$ und

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

5.2.1 Kanalcodierung

Bei der Kanalcodierung werden Nachrichtenwörtern der Länge k genau $n-k$ Kontrollsymbole hinzugefügt; dies ergibt ein *Codewort* der Länge n. Hinzufügen der Kontrollsymbole i.a. hinten; man spricht von einem *systematischen Code*. Dies vereinfacht die Umkehrung der Kanalcodierung.

Sei N die Menge aller Nachrichtenwörter über A. Die *Codierungsvorschrift* (oder *Encoder*) ist eine injektive Abbildung $f_C : N \subseteq A^k \longrightarrow A^n$. Es sei $f_C(N) = C, f_C$ eine bijektive Abbildung von $N \longrightarrow C$. Die Menge C aller Codewörter wird *Blockcode* genannt.

Bsp.:

1. Paritycheck-Code: $A = \{0, 1\}, N = A^k$ und

$$f_C(a_1, \ldots, a_k) = \left(a_1, \ldots, a_k, \left(\sum_{i=1}^{n} a_i\right) \mod 2\right).$$

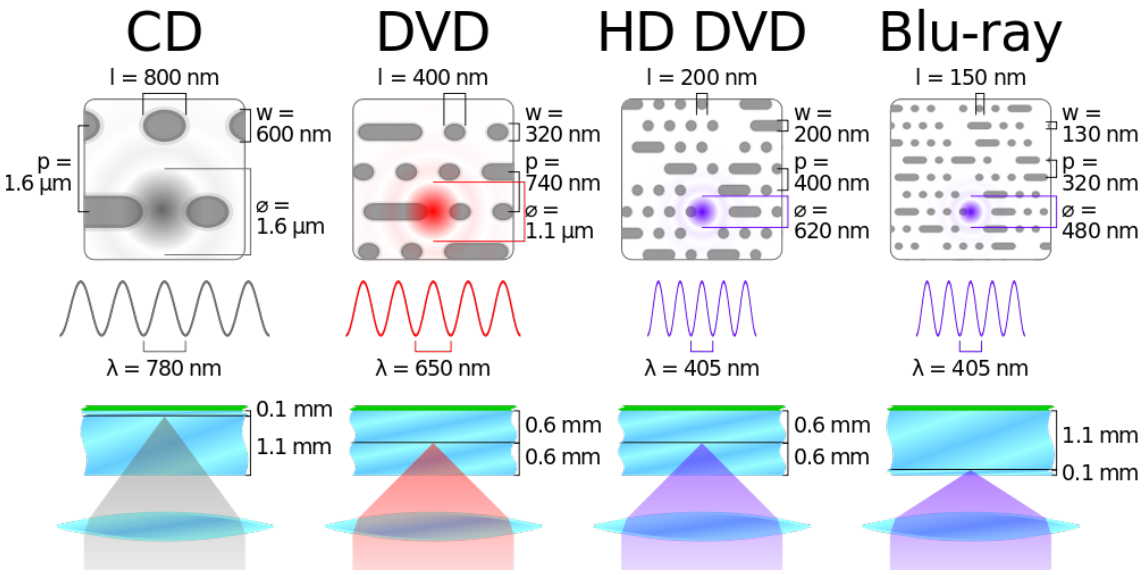

Abbildung 3: Vergleich zwischen CD, DVD, HD-DVD und Blue-ray

2. r-fach Wiederholungscode: A beliebig, $N = A^k$ und

$$f_C(a_1, \ldots, a_k) = (a_1, \ldots, a_k, \ldots, a_1, \ldots, a_k)$$

(r-fach wiederholt).

Forderungen an Kanalcodierung:

- Wahrscheinlichkeit einer falschen Korrektur möglichst gering
- schnelle Algorithmen für Codierung und Decodierung
- möglichst wenig Kontrollsymbole (Widerspruch zum ersten Punkt - eine gute Fehlererkennung geht Hand in Hand mit der Ineffizienz des Codes)

5.2.2 Decodierung

Dazu wird der Hamming-Abstand von zwei n-Tupel $a = (a_1, \ldots, a_n)$ und $b = (b_1, \ldots, b_n)$ wie folgt definiert: $d(a, b) =$ Anzahl der $i \in \{1, \ldots, n\}$ mit $a_i \neq b_i$.

Bsp.: $d((1, 1, 0, 1), (0, 1, 1, 1)) = 2$.

Prinzip der Decodierung: Wir nehmen das zum empfangenen (eventuell fehlerbehafteten) Wort nächstliegende Codewort (aus dem dann das Nachrichtenwort ablesbar ist).

Es gilt: Ein Code kann genau dann jede Kombination von t oder weniger Fehlern entdecken bzw. korrigieren, wenn der Hamming-Abstand zwischen zwei beliebigen Codewörtern mindestens $t + 1$ bzw. $2t + 1$ ist. Sei d der minimale Abstand zwischen zwei verschiedenen

Codewörtern (man spricht vom Minimalabstand des Codes), so gilt: Der Code kann t Fehler entdecken, falls $t+1 \leq d$ und t Fehler korrigieren, falls $2t+1 \leq d$.

Bsp.: Der Paritycheck-Code erkannt 1 Fehler, falls höchsten 1 Fehler auftritt. Der r-fach Wiederholungscode erkennt bis zu $r-1$ Fehler und kann bis zu $[\frac{r-1}{2}]$ Fehler korrigieren.

5.2.3 Effiziente Codierung und Decodierung mittels Polynomcodes

Wir verwenden die folgende Identifikation: $w = (w_0, \ldots, w_{m-1}) \leftrightarrow p_w(x) = w_0 + w_1 x + \cdots + w_{m-1}x^{m-1}$.
Gegeben sei nun ein Polynom $g(x)$ vom Grad $n-k$ mit Koeffizienten in A.
Es sei $R_{g(x)}(p(x))$ der Rest bei Division von $p(x)$ durch $g(x)$.
Dann ist $f_C : A^k \to A^{n-k}$ gegeben durch: $f_C(a_0, \ldots, a_{k-1}) = (c_0, c_1, \ldots, c_{n-k-1}, a_0, a_1, \ldots, a_{k-1})$ wobei $c_0 + c_1 x + \cdots + c_{n-k-1}x^{n-k-1} + a_0 x^{n-k} + a_1 x^{n-k+1} + \cdots + a_{k-1}x^{n-1} = p_a(x)x^{n-k} - R_{g(x)}(p_a(x)x^{n-k})$ ist.

Bsp.: $(7,4)$-Code über $\mathbb{F}_2$ mit $g(x) = 1 + x + x^3$. Wir können zeigen, dass $f_C(a) = 1 + x + x^4 + x^6 = (1,1,0,0,1,0,1)$:
Betrachte $a = (0,1,0,1)$. Wir ordnen a ein Element p_a zu: $p_a(x) = 0 + 1 \cdot x + 0 \cdot x^2 + 1 \cdot x^3$.
Die Codierungs-Vorschrift lautet:

$$p_a(x) \cdot x^{n-k} = p_a(x) \cdot x^3 = x^6 + x^4$$

Weiters muss eine Division mit Rest von $p_a(x) \cdot x^{n-k}$ mit $g(x)$ durchgeführt werden:

$$\begin{aligned} &(x^6 + x^4) : (x^3 + x + 1) = x^3 + 1 \\ +&\underline{(x^6 + x^4 + x^3)} \\ &\qquad x^3 \\ &\qquad \underline{x^3 + x + 1} \\ &\qquad\quad x + 1 \to \mathit{Rest} \end{aligned}$$

$x+1$ ist Rest, da $\deg(x^3+1) < \deg(x+1) \Rightarrow$ Codewort ist $p_a(x) \cdot x^3 + R_{g(x)}(p_a(x) \cdot x^3) = x^6 + x^4 + x + 1 \mapsto (1,1,0,0,1,0,1)$.

Bsp.:

a) Codierung mittels $(7,1)$-Wiederholungscode über $\mathbb{F}_2$:

Nachrichtenwörter	Codewörter
0	0000000
1	1111111

$C = \{(0,0,0,0,0,0,0), (1,1,1,1,1,1,1)\} \Rightarrow d = 7$. $2t+1 \leq 7 \Rightarrow$ Code korrigiert bis zu 3 Fehler.

b) Sequentielle Anordnung der "Pixel": Farbe 1 = $(0,0)$, Farbe 2 = $(0,1)$, Farbe 3 = $(1,0)$, Farbe 4 = $(1,1)$. Farbinhalt zweier aufeinanderfolgenden Pixels = ein Wort; somit $k = 4$. Codierung mittels $(7,4)$-Polynomcode über $\mathbb{F}_2$ mit $g(x) = 1 + x + x^3$.

Nachrichtenwörter	Codewörter
0000	0000000
0001	1010001
0010	1110010
0011	0100011
0100	0110100
0101	1100101
0110	1000110
0111	0010111
1000	1101000
1001	0111001
1010	0011010
1011	1001011
1100	1011100
1101	0001101
1110	0101110
1111	1111111

Empirisch: $d = 3$. Durch theoretische Überlegung: $a, b \in C \Rightarrow a - b \in C$ (f_C ist linear, C ist ein Untervektorraum von A^k). Damit $d(a,b) = \#$ Einsen in $a - b =: c \in C \Rightarrow d =$ minimale # von Einsen in einem $c \in C, c \neq 0$; somit $d = 3$. Darüberhinaus $2t + 1 \leq 3 \Rightarrow$ Code korrigiert 1 Fehler.

Bsp.: Bei einer Compact Disc wird $A = \mathbb{F}_{256} = \mathbb{F}_{2^8}$ gewählt. Zudem werden zwei verkürzten RS-Codes (Reed-Solomon Codes) verwendet. Es handelt sich um Polynomcodes, welche optimal sind, d.h. es gilt $d = n - k + 1$ (es gilt stets $\leq$). Die Schritte zur Codierung sind:

- Musik wird 44100 mal pro Sekunde (ticks) abgetastet und 2 (Stereo) binäre Werte der Länge 16 zugeordnet $\rightsquigarrow$ 4 Byte codiert als $m_{4t}m_{4t+1}m_{4t+2}m_{4t+3} \in \mathbb{F}_{2^8}^4$. CD-Player verarbeitet $44100 \cdot 32 = 1411200$ Audio-Bits pro Sekunde.
- 6 ticks bilden eine Nachricht $M_t = m_{24t} \ldots m_{24t+23} \in \mathbb{F}_{256}^{24}$. Codierung mit verkürztem $(28,24)$-RS-Code C_1 über $\mathbb{F}_{256}$. $d = n - k + 1 = 5 \Rightarrow$ Code korrigiert 2 Byte-Fehler $\Rightarrow$ Code korrigiert alle "Fehlerbündel" bis zu 9 Bits.
- Interleaving zum Aufteilen großer Fehlerbündel; dazu werden 28 Wörter á 28 Bytes zu 28 neuen Wörtern á 28 Bytes zusammengefaßt.
- Anwendung eines $(32,28)$-verkürzten RS-Codes C_2 auf den neu organisierten Datenstrom $\rightarrow$ weiteres Byte für Kontrollzwecke und Display

- EFM (eight to fourteen) Modulation: durch Table-Lookup wird jedem Element in $\mathbb{F}_{256}$ eine andere Darstellung zugeordnet und jeweils 3 weiter Puffer-Bits hinzugefügt, sodass: zwischen mindestens zwei 1en mindestens 2 und höchstens 10 0en (physikalische Limitierung des Lasers). Insgesamte Länge der binären Nachricht: $33 \cdot 17 = 561$.
- 27 weitere Bits für Synchronisationszwecke; aus ursprünglich $24 \cdot 8 = 196$ (= 6 ticks) sind auf CD 588 Bits geworden. Verarbeitete Bits pro Sekunde: 4321800. CD mit 75 Minuten Spielzeit speichert: 20 Milliarden Bits.
- Weitere Tricks: Bits auf ungeraden und geraden Positionen werden vermischt; Bits zwischen linker und rechter Tonspur werden gemischt (ermöglicht Korrektur durch Interpolation); etc.

Zum Abspielen einer CD wird wie folgt vorgegangen: Demodulation, Datenpuffer, Decodierung mittels C_2, Umkehrung des Interleavings, Decodierung mittels C_1, Interpolation, Umwandlung der digitalen Information in Audiosignale.

5.3 Ausflug in die Welt der endlichen Körper

Sei $\mathbb{F}$ ein endlich Körper; es folgt, dass $n = |\mathbb{F}| = p^k, p \in \mathbb{P}, k \in \mathbb{N}$. Es gilt:

$n = 2$: $\mathbb{F}_2 = \{0, 1\}$ mit

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$n = 3$: $\mathbb{F}_3 = \{0, 1, 2\}$ mit

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$n = 5$: $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ mit $a+b :=$ (berechne $a+b$ in $\mathbb{Z}$ und dann den Rest bei Division durch 5), $a \cdot b :=$ (berechne ab in $\mathbb{Z}$ und dann den Rest bei Division durch 5).

$n = p \in \mathbb{P}$: Analog wie für $n = 2, 3, 5$; $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$, $+, \cdot$ als Rest bei Division durch p nach der Addition/Multplikation in $\mathbb{Z}$.

Für n zusammengesetzt funktioniert diese Methode nicht, da mit $n = ab$ in $\mathbb{Z}_n$ gilt $ab = 0$ mit $a, b \neq 0$, was in einem Körper nicht richtig sein kann.

$n = 4 = 2^2$: Betrachte auf $\mathbb{F}_2[x]$ die Äquivalenzrelation $f \sim g :\Leftrightarrow x^2 + x + 1 | (f - g)$. Definiere $\mathbb{F}_4 := \mathbb{F}_2[x]/\sim$. Die Operationen werden wie folgt eingeführt: $[f] + [g] :=$ [berechne $f + g$ in $\mathbb{F}_2[x]$ und dann den Rest bei Division durch $x^2 + x + 1$], $[f][g] :=$ [berechne fg in

$\mathbb{F}_2[x]$ und dann den Rest bei Division durch $x^2 + x + 1$].

Analog kann bei $n = p^k$ vorgegangen werden, indem anstatt $\mathbb{F}_2[x]$ der Polynomring $\mathbb{F}_p[x]$ und anstatt x^2+x+1 ein irreduzibles (d.h. das Polynom kann nicht in das Produkt zweier Polynome von kleinerem Grad zerlegt werden) Polynom in $\mathbb{F}_p[x]$ vom Grad k betrachtet wird.

5.4 Übungsbeispiele

1. Sei $A = \{0, 1\}, c_1 = 01010, c_2 = 01101, c_3 = 11101$. Berechne die Hamming-Distanzen zwischen diesen Elementen.

2. Sei $A = \{0, 1, 2, 3, 4\}, c_1 = 1234, c_2 = 1423, c_3 = 3214$. Berechne die Hamming-Distanzen zwischen diesen Elementen.

3. Zeige, dass für die Hamming-Distanz stets $d(u, v) \geq 0, d(u, v) = d(v, u)$ und $d(u, v) = 0 \Leftrightarrow u = v$ gilt.

4. Berechne die Minimaldistanz für die Codes $C_1 = \{00000, 0011111, 11111\}$ und $C_2 = \{000000, 000111, 111222\}$.

5. Dividiere das Polynom $x^3 + 2x^2 + 3x + 1 \in \mathbb{Q}[x]$ mit Rest durch das Polynom $x^2 - x - 1$.

6. Dividiere das Polynom $x^3 + x + 1 \in \mathbb{Z}[x]$ mit Rest durch das Polynom $x^2 + 1$. Führe anschließend die selbe Rechnung durch, wobei nun die Polynome aber als Elemente von $\mathbb{F}_2[x]$ gedeutet werden.

7. Konstruiere einen Code, der einen Fehler korrigiert, zur Übermittlung der Nachrichtenwörter $001, 011, 100, 101$.

8. Wieviele binäre $(n, 1)$-Codes mit Minimaldistanz $n \geq 2$ gibt es?

9. Zeige, dass der 4-fach Wiederholungscode ein Polynomcode ist; wie lautet das zugehörige Polynom $g(x)$?

10. Codiere die Wörter 110 und 010 mit dem Code aus dem letzten Beispiel.

11. Ist der Code aus dem letzten Beispiel perfekt?

12. Für den $(9, 4)$-Polynomcode über $\mathbb{F}_2$ mit dem Polynom $g(x) = 1 + x + x^2 + x^4 + x^5$ überprüfe man, ob die folgenden Wörter fehlerhaft sind: 100110010, 100100101, 00011 1110, 100001110, 111101100.

6 Suche mathematischer Literatur

Für die Suche mathematischer Literatur ist das World Wide Web bestens geeignet. Doch nicht alle Angebote sind auch seriös oder für wissenschaftliche Arbeiten geeignet. Darum finden Sie in folgendem Kapitel eine Auflistung brauchbarer Websites und Links, die Ihnen die Literatursuche vereinfachen sollen.

6.1 UBSearch

Ein besonders nützliches Tool zur Literatursuche ist die universitätseigene Suchmaschine der Bibliothek. Sie ermöglicht den Zugang zu allen Medien der Universität Salzburg. Man findet den Link auf der Homepage *www.uni-salzburg.at* → Bibliothek → UBSearch oder unter *ubsearch.sbg.ac.at*.
In der Option *Hilfe* kann nachgelesen werden, wie genau die eigene Suche optimiert werden kann um nur gewünschte Suchergebnisse zu erhalten.
Über UBSearch kann man des Weiteren nicht nur auf die physisch vorhandene Literatur der Universität zugreifen, sondern auch auf zusätzliche Ressourcen (wie andere elektronische Datenbanken), sowie online verfügbare Volltexte und Literaturquellen. Online Versionen sind allerdings nur im internen Uni-Netzwerk abrufbar.

6.2 Fachbibliothek NAWI

Mathematische Literatur/Fachjournale sind sowohl im Handapparat der Lehrbücher als auch bei den Zeitschriften in der 1. Etage der Bibliothek zu finden. Die restliche gebundene Literatur befindet sich in der 2. Etage der Bibliothek.

6.3 MSC2010

Die MSC2010-Database (MSC=Mathematics Subject Classification) ist eine weltweit verwendete Datenbank der American Mathematical Society mit dem Ziel, Forschungsgebiete möglichst übersichtlich zu klassifizieren. Die Unterteilung nach dem Stand 2010 kann unter *http://www.ams.org/msc/msc2010.html* nachgesehen werden. Diese Klassifikation ist international in Verwendung.

6.4 Foren - Austausch mit KollegInnen

Foren eigenen sich gut um aktuelle Probleme in der eigenen Forschung zu recherchieren und mit erfahrenen KollegInnen zu diskutieren. Man kann äußerst viel dabei lernen und findet manchmal in solchen Foren die zündende Idee:
http://math.stackexchange.com/
http://mathoverflow.net/ (für professionellere MathematikerInnen)

ACHTUNG: Foren sind nicht geprüft und können daher falsche oder fehlerhafte Informationen enthalten! Die oben angeführten Seiten haben aber eine hohe Glaubwürdigkeit und unterliegen eine internen Qualitätskontrolle durch die ForumsteilnehmerInnen.

6.5 Forschungsartikel finden

Auf *https://arxiv.org/archive/math* können aktuellen mathematischen Veröffentlichungen ("Paper") gefunden werden - neues Wissen völlig kostenlos.

Wenn ein interessantes Paper gefunden wurde, kann noch auf *http://www.ams.org/mathscinet/* eine Zusammenfassung der Publikation gelesen werden ("mathematical reviews"). Allerdings ist der freie Zugriff auf diese Datenbank nur vom Uni-Netzwerk aus möglich. Ebenso dafür geeignet ist:
https://zbmath.org/

6.6 Stammbaum der MathematikerInnnen

Das Mathematics Genealogy Project hat zum Ziel, alle MathematikerInnen weltweit in einer Art Stammbaum zu registrieren, der jeweils die/den BetreuerIn angibt. So kann verfolgt werden, wer bei wem dissertierte. *https://genealogy.math.ndsu.nodak.edu/index.php*

6.7 OEIS

Die Online-Enzyklopädie der Zahlenfolgen ist eine Datenbank gefüllt mit Folgen ganzer Zahlen. Es kann nach einem Begriff wie "prime numbers" gesucht werden, aber auch eine bestimmte Abfolge an Zahlen eingegeben werden, z. Bsp.: 1,4,9,16 - das Ergebnis sind mögliche passende Folgen.

§L. Literatur

1. L. Alcock, How to Study for a Mathematics Degree, Oxford University Press, 2013, ISBN978-0-19-966132-9
2. Studien- und Berufsplaner Mathematik, Springer Spektrum, 2015, ISBN978-3-658-04128-1
3. Studienführer für das Bachelorstudium Mathematik ab dem Wintersemester 2016/17, FB Mathematik, Universität Salzburg, 2016