Vorlesungsverzeichnis

M.Sc. Computer Science for Digital Media

SoSe 2023

Stand 20.04.2023

M.Sc. Computer Science for Digital Media

Faculty Welcome for Master's Students Computer Science for Digital Media
Monday, 3rd April 2023, 11.00 a.m., Schwanseestraße 143, room 2.16

Project fair
Monday, 3rd April 2023, 5 p.m., Steubenstraße 6, Audimax

Modeling

301016 Complex dynamics

B. Rüffer Veranst. SWS: 4
Vorlesung
Di, wöch., 07:30 - 10:45, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be able to analyse mathematical models that describe dynamic behaviour, as they occur in engineering (e.g. mechanical coupling of building structures), in biology and in physics, but also in multi-agent systems in computer science, or as opinion dynamics in psychology. Based on examples from different disciplines, students learn to build simplified models that allow to answer questions on their long-term behaviour. Students will be able to apply methods of feedback design that help shape the dynamics of a given system, along with the relevant stability concepts. As several topics lend themselves for computer simulation, students of this course will develop a proficiency to both implement and analyse mathematical models using computational tools and software.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B.Sc., knowledge in Matlab or Python

Leistungsnachweis

1 written exam

"Complex dynamics"

120 min (100%) / **SuSe** + WiSe

301017 Mathematics for data science

B. Rüffer, M. Schönlein Veranst. SWS: 4
Vorlesung
Mi, Einzel, 13:30 - 16:45, Coudraystraße 13 B - Hörsaal 3, 05.04.2023 - 05.04.2023
Mo, wöch., 09:15 - 12:30, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 written exam

”Complex dynamics”

120 min (100%) / **SuSe** + WiSe

417130003 Discrete Optimization

A. Jakoby Veranst. SWS: 4

Vorlesung

Do, wöch., 15:15 - 16:45, Schwanseestraße 143 - Seminarraum 2.16, Lecture , ab 13.04.2023
Do, wöch., 17:00 - 18:30, Schwanseestraße 143 - Seminarraum 2.16, lab class, ab 13.04.2023

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkommentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination (individual apppointments via Moodle)

Distributed and Secure Systems

419140050 Introduction to Modern Cryptography

S. Lucks, N. Lang, J. Leuther Veranst. SWS: 3

Vorlesung

Fr, wöch., 09:15 - 10:45, Schwanseestraße 143 - Seminarraum 2.16, 1st lecture: April 14th, 2023 start lab classes: April 21st, 2023, ab 14.04.2023
Mo, wöch., 13:30 - 15:00, Schwanseestraße 143 - Seminarraum 2.16, Lecture, ab 17.04.2023

Beschreibung

Früher galt die Kryptographie als Werkzeug für Militärs, Geheimdienste und Diplomaten. Aus dieser Zeit stammt auch noch die berühmte Enigma-Chiffriermaschine.

Heute entwickelt sich die Kryptographie buchstäblich zu einer Schlüsseltechnologie für sichere Kommunikation und Mediennutzung. Von der Öffentlichkeit kaum bemerkt hat die Kryptographie schon längst Einzug gehalten in alltäglich genutzte Geräte wie Geldautomaten und Mobiltelefone.

Der Entwurf kryptographischer Komponenten ist schwierig, und in der Praxis trifft man oft auf erhebliche Entwurfsfehler. (Dies kommentiert der IT-Sicherheitsexperte Bruce Schneier mit drastischen Worten: "Milliarden von Dollar werden für Computersicherheit ausgegeben, und das Meiste davon wird für unsichere Produkte verschwendet.")

Nicht nur der Entwurf kryptographischer Komponenten ist schwierig, auch der Einsatz von "an sich guten" Komponenten für sichere IT-systeme ist fehlerträchtig und erfordert ein genaues Verständnis der jeweiligen Bedingungen, unter denen eine kryptographische Komponente als "sicher" gelten kann.

Die Vorlesung gibt einen Einblick in Denkweise und Methodik der Mediensicherheit und der modernen Kryptographie und die Anwendung der Kryptographie, um Sicherheitsprobleme zu lösen.

engl. Beschreibung/ Kurzkommentar

Bemerkung

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Für Studierende, die in ihrem früheren Bachelor-Studium keine Einführung in die Kryptographie besucht haben, ist die Veranstaltung ihrerseits Zulassungsvoraussetzung für fortgeschrittene Kryptographie-Vorlesungen.

Voraussetzungen

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Leistungsnachweis

M.Sc.: Mündliche Prüfung
Beleg als Voraussetzung zur Klausurzulassung

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther Veranst. SWS: 4

Vorlesung

Mi, wöch., 11:00 - 12:30, Marienstraße 13 C - Hörsaal D, Lecture, ab 12.04.2023
Fr, wöch., 11:00 - 12:30, Schwanseestraße 143 - Seminarraum 3.09, Lab class, ab 14.04.2023

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/ TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzen Hashfunktionenwie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Strukture von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichen Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidate drehen. Basieren auf den Erkenntnissen und Kandidate des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einfürung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

mündliche Prüfung

Intelligent Information Systems

420160000 Introduction to Natural Language Processing

B. Stein, M. Wolska, N. Kolyada, N. Mirzakhmedova, M. Wiegmann Veranst. SWS: 4

Vorlesung

Mo, wöch., 15:15 - 16:45, Schwanseestraße 143 - Seminarraum 2.16, Lab class, ab 24.04.2023
Do, wöch., 15:15 - 16:45, Lecture

Beschreibung

This course gives an overview of basic techniques of working with language data. We will introduce basic linguistic notions, issues involved in building and working with language corpora, current standard techniques for preparing text for analysis, and methods of computational processing of a subset of language phenomena. By the end of the course students will

(1) have an understanding of key word-level, syntactic, semantic, and discourse phenomena,

(2) be aware of issues involved in building text corpora,

(3) be familiar with typical language processing tasks addressed in the NLP community and methods of addressing them, and

(4) will be able to perform tasks that are part of a standard NLP pipeline.

Leistungsnachweis

Klausur

4336010 Image Analysis and Object Recognition

V. Rodehorst, C. Benz Veranst. SWS: 3

Vorlesung

Di, wöch., 15:15 - 16:45, Coudraystraße 9 A - Hörsaal 6, Lecture, ab 04.04.2023
Do, wöch., 11:00 - 12:30, Coudraystraße 9 A - Hörsaal 6, Lab class, ab 13.04.2023

Beschreibung

Bildanalyse und Objekterkennung

Die Vorlesung gibt eine Einführung in die Grundlagen der Mustererkennung und Bildanalyse. Behandelt werden unter anderem die Bildverbesserung, lokale und morphologische Operatoren, Kantenerkennung, Bilddarstellung im Frequenzraum, Fourier-Transformation, Hough-Transformation, Segmentierung, Skelettierung, Objektklassifizierung und maschinelles Lernen zur visuellen Objekterkennung.

engl. Beschreibung/ Kurzkommentar

Image analysis and object recognition

The lecture gives an introduction to the basic concepts of pattern recognition and image analysis. It covers topics as image enhancement, local and morphological operators, edge detection, image representation in frequency domain, Fourier transform, Hough transform, segmentation, thinning, object categorization and machine learning for visual object recognition.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungen und Klausur (sowie des Final Projects für das Erreichen der 6 ECTS)

Graphical and Interactive Systems

4556227 Usability Engineering & Testing

J. Ehlers Veranst. SWS: 4
Vorlesung
Di, wöch., 13:30 - 15:00, Marienstraße 13 C - Hörsaal B, Lecture
Do, wöch., 17:00 - 18:30, Lab class online

engl. Beschreibung/ Kurzkommentar

Usability indicates the ”absence of frustration”. But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesising. We will also discuss procedures for quantitative data analysis and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

Leistungsnachweis

Empirical exercises (tutorial) and written exam

Electives

4336010 Image Analysis and Object Recognition

V. Rodehorst, C. Benz Veranst. SWS: 3
Vorlesung
Di, wöch., 15:15 - 16:45, Coudraystraße 9 A - Hörsaal 6, Lecture, ab 04.04.2023
Do, wöch., 11:00 - 12:30, Coudraystraße 9 A - Hörsaal 6, Lab class, ab 13.04.2023

Beschreibung

Bildanalyse und Objekterkennung

Die Vorlesung gibt eine Einführung in die Grundlagen der Mustererkennung und Bildanalyse. Behandelt werden unter anderem die Bildverbesserung, lokale und morphologische Operatoren, Kantenerkennung, Bilddarstellung im Frequenzraum, Fourier-Transformation, Hough-Transformation, Segmentierung, Skelettierung, Objektklassifizierung und maschinelles Lernen zur visuellen Objekterkennung.

engl. Beschreibung/ Kurzkommentar

Image analysis and object recognition

The lecture gives an introduction to the basic concepts of pattern recognition and image analysis. It covers topics as image enhancement, local and morphological operators, edge detection, image representation in frequency domain, Fourier transform, Hough transform, segmentation, thinning, object categorization and machine learning for visual object recognition.

Leistungsnachweis

Erfolgreiche Bearbeitung der Übungen und Klausur (sowie des Final Projects für das Erreichen der 6 ECTS)

420160004 Image Analysis and Object Recognition – Final Project

V. Rodehorst, C. Benz Veranst. SWS: 1
Independent Study

Beschreibung

Im Abschlussprojekt der Vorlesung „Image Analysis and Object Recognition" sollen die Kenntnisse der Vorlesung an einer größeren praktischen Aufgabe vertieft werden.

Voraussetzungen

Erfolgreiche Teilnahme an der Vorlesung „Image Analysis and Object Recognition"

Leistungsnachweis

Dokumentation, Abschlusspräsentation

4555262 Visualisierung

B. Fröhlich, D. Kiesel, G. Rendle, P. Riehmann Veranst. SWS: 3
Vorlesung
Do, wöch., 13:30 - 15:00, Lecture / Lab class , ab 13.04.2023
Do, wöch., 13:30 - 15:00, Schwanseestraße 143 - Seminarraum 2.16, 1st Lecture: in person, ab 13.04.2023
Mo, wöch., 17:00 - 18:30, Schwanseestraße 143 - Lintpool 2.17, Lab class, ab 17.04.2023
Di, wöch., 09:15 - 10:45, Schwanseestraße 143 - Lintpool 2.17, Lab class, ab 18.04.2023

Beschreibung

Im ersten Teil der Veranstaltung werden die wichtigsten Verfahren und Techniken aus dem Bereich der Informationsvisualisierung für folgende Datentypen vorgestellt: multi-dimensionale und hierarchische Daten, Graphen, Zeitreihen und mengenbasierte Daten. Der zweite Teil beschäftigt sich mit verschiedenen Ansätzen und Algorithmen zur Visualisierung volumetrischer und vektorieller Simulations- und Messdaten. Die Veranstaltung wird englischsprachig angeboten.

In den Übungen werden eine Auswahl der in den Vorlesungen vorgestellten Visualisierungsansätze umgesetzt, getestet und evaluiert. Ein separates Abschlussprojekt wird angeboten und mit zusätzlich 1,5 ETCS angerechnet.

Bemerkung

Bitte beachten:
um die vollen 6 ECTS zu erhalten, muss auch Abschlussprojekt bestanden werden: "Visualization – Final Project"

Voraussetzungen

Programmierkenntnisse sowie gute Kenntnisse von Algorithmen und Datenstrukturen sind erforderlich, z.B. nachgewiesen durch den erfolgreichen Abschluss der entsprechenden Lehrveranstaltungen des Bachelor-Studiengangs Medieninformatik.

In den Laborveranstaltungen werden JavaScript- und grundlegende GLSL-Programmierung eingesetzt. Grundkenntnisse der Computergrafik sind hilfreich, z.B. erworben durch die Vorlesung Computergrafik im Bachelor-Studiengang Medieninformatik.

Leistungsnachweis

Vorlesungsbegleitende Übungen, mündliche oder schriftliche Prüfung.

Ein abschließendes Projekt wird separat bewertet und erhält zusätzliche 1.5 ECTS.

420160006 Visualization - Final Project

B. Fröhlich, N.N., J. Reibert, G. Rendle Veranst. SWS: 1
Independent Study

Beschreibung

Im Abschlussprojekt der Vorlesung „Visualisierung" sollen die Teilnehmer die erlangten theoretischen und praktischen Fertigkeiten auf den Entwurf, die Implementierung und die Präsentation eines eigenständigen kleinen Forschungsprojektes anwenden. Dazu soll ein Problem ausgewählt, eine Lösung entwickelt, eine effiziente Implementierung realisiert und die Ergebnisse abschließend in einem Vortrag präsentiert werden.

Dies ist eine wertvolle Gelegenheit, an einem selbst gewählten Thema im Bereich der Visualisierung zu arbeiten.

Voraussetzungen

Erfolgreiche Teilnahme an der Vorlesung „Visualization"

Leistungsnachweis

Dokumentation, Abschlusspräsentation

301016 Complex dynamics

B. Rüffer Veranst. SWS: 4
Vorlesung
Di, wöch., 07:30 - 10:45, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be able to analyse mathematical models that describe dynamic behaviour, as they occur in engineering (e.g. mechanical coupling of building structures), in biology and in physics, but also in multi-agent systems in computer science, or as opinion dynamics in psychology. Based on examples from different disciplines, students learn to build simplified models that allow to answer questions on their long-term behaviour. Students will be able to apply methods of feedback design that help shape the dynamics of a given system, along with the relevant stability concepts. As several topics lend themselves for computer simulation, students of this course will develop a proficiency to both implement and analyse mathematical models using computational tools and software.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B.Sc., knowledge in Matlab or Python

Leistungsnachweis

1 written exam

”Complex dynamics”

120 min (100%) / **SuSe** + WiSe

301017 Mathematics for data science

B. Rüffer, M. Schönlein Veranst. SWS: 4

Vorlesung

Mi, Einzel, 13:30 - 16:45, Coudraystraße 13 B - Hörsaal 3, 05.04.2023 - 05.04.2023
Mo, wöch., 09:15 - 12:30, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 written exam

”Complex dynamics”

120 min (100%) / **SuSe** + WiSe

417130003 Discrete Optimization

A. Jakoby Veranst. SWS: 4

Vorlesung

Do, wöch., 15:15 - 16:45, Schwanseestraße 143 - Seminarraum 2.16, Lecture , ab 13.04.2023
Do, wöch., 17:00 - 18:30, Schwanseestraße 143 - Seminarraum 2.16, lab class, ab 13.04.2023

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkommentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination (individual apppointments via Moodle)

419140050 Introduction to Modern Cryptography

S. Lucks, N. Lang, J. Leuther Veranst. SWS: 3

Vorlesung

Fr, wöch., 09:15 - 10:45, Schwanseestraße 143 - Seminarraum 2.16, 1st lecture: April 14th, 2023 start lab classes: April 21st, 2023, ab 14.04.2023
Mo, wöch., 13:30 - 15:00, Schwanseestraße 143 - Seminarraum 2.16, Lecture, ab 17.04.2023

Beschreibung

Früher galt die Kryptographie als Werkzeug für Militärs, Geheimdienste und Diplomaten. Aus dieser Zeit stammt auch noch die berühmte Enigma-Chiffriermaschine.

Heute entwickelt sich die Kryptographie buchstäblich zu einer Schlüsseltechnologie für sichere Kommunikation und Mediennutzung. Von der Öffentlichkeit kaum bemerkt hat die Kryptographie schon längst Einzug gehalten in alltäglich genutzte Geräte wie Geldautomaten und Mobiltelefone.

Der Entwurf kryptographischer Komponenten ist schwierig, und in der Praxis trifft man oft auf erhebliche Entwurfsfehler. (Dies kommentiert der IT-Sicherheitsexperte Bruce Schneier mit drastischen Worten: "Milliarden von Dollar werden für

Computersicherheit ausgegeben, und das Meiste davon wird für unsichere Produkte verschwendet.")

Nicht nur der Entwurf kryptographischer Komponenten ist schwierig, auch der Einsatz von "an sich guten" Komponenten für sichere IT-systeme ist fehlerträchtig und erfordert ein genaues Verständnis der jeweiligen Bedingungen, unter denen eine kryptographische Komponente als "sicher" gelten kann.

Die Vorlesung gibt einen Einblick in Denkweise und Methodik der Mediensicherheit und der modernen Kryptographie und die Anwendung der Kryptographie, um Sicherheitsprobleme zu lösen.

engl. Beschreibung/ Kurzkommentar

Bemerkung

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Für Studierende, die in ihrem früheren Bachelor-Studium keine Einführung in die Kryptographie besucht haben, ist die Veranstaltung ihrerseits Zulassungsvoraussetzung für fortgeschrittene Kryptographie-Vorlesungen.

Voraussetzungen

Die Studierenden dürfen bisher keine Einführung in Kryptographie besucht haben. Zum Nachweis sind bei der Anmeldung zur Prüfung die "Transcript of Records" aus früheren Studien vorzulegen.

Leistungsnachweis

M.Sc.: Mündliche Prüfung
Beleg als Voraussetzung zur Klausurzulassung

420160000 Introduction to Natural Language Processing

B. Stein, M. Wolska, N. Kolyada, N. Mirzakhmedova, M. Wiegmann Veranst. SWS: 4

Vorlesung

Mo, wöch., 15:15 - 16:45, Schwanseestraße 143 - Seminarraum 2.16, Lab class, ab 24.04.2023
Do, wöch., 15:15 - 16:45, Lecture

Beschreibung

This course gives an overview of basic techniques of working with language data. We will introduce basic linguistic notions, issues involved in building and working with language corpora, current standard techniques for preparing text for analysis, and methods of computational processing of a subset of language phenomena. By the end of the course students will

(1) have an understanding of key word-level, syntactic, semantic, and discourse phenomena,

(2) be aware of issues involved in building text corpora,

(3) be familiar with typical language processing tasks addressed in the NLP community and methods of addressing them, and

(4) will be able to perform tasks that are part of a standard NLP pipeline.

Leistungsnachweis

Klausur

422150031 Generative Software Engineering

J. Ringert Veranst. SWS: 4
Vorlesung
Mi, wöch., 09:15 - 10:45, Marienstraße 13 C - Hörsaal A, Lecture
Fr, wöch., 13:30 - 15:00, Coudraystraße 9 A - Hörsaal 6, Lab class

Beschreibung

We introduce main approaches and techniques to generative software development.

- Model Driven Engineering
- Software Modeling languages for structure and behavior
  - Class Diagrams, Object Diagrams, OCL
  - Sequence Diagrams and State Machines
- Software model consistency and semantics
- Code Generation from class diagrams
- Code generation from State Machines
- Reactive Synthesis from temporal specifications
- Software Product Lines
- Domain Specific Languages
- Model Transformations

After completion students will be able to

- Contrast different modelling languages and chose based on purpose
- Analyze model consistency
- Evaluate and apply code generators
- integrate generated code in software projects
- create and analyze temporal specifications
- synthesize software from temporal specifications
- understand domain specific languages and model transformations

Bemerkung

Lecturer: Prof. Ringert

423150020 Advanced Topics in Software Engineering

J. Ringert
Seminar
Fr, wöch., 15:15 - 16:45, Coudraystraße 13 B - Hörsaal 3

423150021 Deep Learning for Computer Vision

V. Rodehorst, J. Eick, D. Tschirschwitz Veranst. SWS: 4
Integrierte Vorlesung
Di, wöch., 09:15 - 10:45, ab 04.04.2023
Fr, wöch., 11:00 - 12:30, ab 14.04.2023

Beschreibung

In diesem Kurs für Fortgeschrittene werden die Prinzipien, Techniken und Anwendungen des tiefgehenden Lernens in Computer Vision behandelt. Die Teilnehmer lernen, wie man neuronale Netze für die Bildklassifizierung, Objekterkennung, semantische Segmentierung und andere Computer-Vision-Aufgaben entwickelt, trainiert und validiert. Es werden auch Techniken zur Verbesserung der Leistung von Deep-Learning-Modellen und Veranschaulichungen behandelt, um Anhaltspunkte für die weitere Modellentwicklung zu erhalten. Am Ende des Kurses werden die Studierenden in der Lage sein, Deep-Learning-Techniken anzuwenden, um reale Probleme in verschiedenen Bereichen zu lösen.

Bemerkung

Bitte melden Sie sich bis zum 11.04.2023 mit Ihrer Univeritäts-E-Mail über die Moodle-Plattform (https://moodle.uni-weimar.de/course/view.php?id=43615) an und füllen Sie den bereitgestellten Fragebogen aus. Bei Überschreitung der Teilnehmerzahl wird die Teilnahme an der Lehrveranstaltung "Introduction to Machine Learning and Data Mining" als Auswahlkriterium herangezogen.

Voraussetzungen

Bachelor: Software Engineering II (B.Sc.), Analysis (B.Sc.) and Linear Algebra (B.sc.) oder gleichwertig.

Master: Object Oriented Modeling and Programming (M.Sc.) and Software Engineering (M.Sc.) oder gleichwertig.

Leistungsnachweis

Erfolgreiche Teilnahme an den Laborübungen und dem Projekt mit abschließender Klausur.

Gewichtung: 50% Projekt und 50% Klausur

423150022 Firewalling und Netzwerktrennung

A. Jakoby Veranst. SWS: 2
Seminar
Di, wöch., 17:00 - 18:30, Lab, R. 2.38, S143

Beschreibung

Im Seminar Firewalling und Netzwerktrennung werden die unterschiedlichen Linux Hilfsmittel zum Aufbau einer Firewall vorgestellt und umgesetzt. Neben dem klassischen Firewalling sollen auch weitere Konzepte der Netzwerktrennung, wie z.B. die Datendiode diskutiert werden.

Bei der Vergabe der beschränkten Seminarstellen werden Studierende des Masterstudienganges CS4DM und des Bachelorstudienganges Informatik mit Schwerpunkt Data Science and Security bevorzugt. Die Anmeldung erfolgt über Email an Andreas Jakoby.

423150023 Procedural Character Animation

F. Andreussi, C. Wüthrich Veranst. SWS: 3
Seminar
Mi, Einzel, 13:30 - 15:00, Coudraystraße 13 B - Seminarraum 210, 26.04.2023 - 26.04.2023

Beschreibung

Organic and believable Character Animation is increasingly important not only for Game Development but also for AR/VR applications and movie production (think about special effects, animating fantastical creatures and generating large scenes with thousands of characters, which would hardly be feasible using only real actors); however, animating by hand or using motion capture for every possible movement could be an extremely long, demanding and expensive task hence the development of techniques that use Machine Learning to generate Character Animations is more relevant than ever before.

During this seminar, we will explore together the evolution of the field during the last 10 years understanding various possible approaches to the problem (from the more data-intensive to the more training-based), then the participants will select a specific paper to focus on, understand in detail and present to the class and, after the presentations, there will be a time for discussing what has been learned and for comparing findings and opinions both on the theory and ideas behind the publications and on the implementation details, which will be part of the practical part at the end of the course and, hopefully, will lead to a Research Project in the following semesters.

Outline of the seminar (which could be modified):

* Introduction and Overview of the topics as frontal lectures (2-3 weekly meetings):

    * What is Procedural Animation?

    * Overview of the field and its common challenges/approaches/techniques

    * Overview of some fundamental papers + interesting talks from conferences where important techniques (like Motion Matching) were presented by their creator

* Individual paper study and presentation preparation (2-3 weeks – no meetings)

* Student presentations of selected papers (1-2 weekly meetings)

* Discussion/Round-table with students about papers, for questions and exchange of ideas (1-2 weekly meetings)

* Implementation tools (Unity/Unreal + Tensorflow/PyTorch, and alternatives)

* Eventual Final Project: Tutorial-like ML Implementation with chosen tools

Bemerkung

the final course dates/times will be discussed at the first meeting

Voraussetzungen

basic knowledge in ML and Computer graphics

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther Veranst. SWS: 4

Vorlesung

Mi, wöch., 11:00 - 12:30, Marienstraße 13 C - Hörsaal D, Lecture, ab 12.04.2023
Fr, wöch., 11:00 - 12:30, Schwanseestraße 143 - Seminarraum 3.09, Lab class, ab 14.04.2023

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/ TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzen Hashfunktionenwie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Strukture von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichen Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidate drehen. Basieren auf den Erkenntnissen und Kandidate des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einfürung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

mündliche Prüfung

4526501 Academic English Part One

G. Atkinson Veranst. SWS: 2

Kurs

Mi, wöch., 15:30 - 16:45, Consultations, R.218, S143 (indiv.appointments), ab 26.04.2023
Mi, wöch., 17:00 - 18:30, Schwanseestraße 143 - Seminarraum 3.09, Academic English Part I+II (alternating), ab 26.04.2023

Beschreibung

This is the first part of a two-part course which aims to improve your ability to express yourself clearly in written English and to develop a suitably coherent academic writing style. Part One concentrates mainly on structure in writing academic articles, essays and reports. We begin by examining the structure of individual paragraphs and move on to extended texts of various types (e.g. process essays, cause/effect, comparison/contrast, etc.). Particular attention is paid to connectives, i.e. transitional phrases and constructions which help you link ideas and paragraphs in a logical, systematic way.

Bemerkung

You are advised to take Part One first, although it is possible to take both parts in reverse order or concurrently (i.e. in the same semester). You may only do the latter on the authority of the course leader (Atkinson).

Voraussetzungen

Registration (compulsory)

All students must register. First time particpants are required to present a B2 English Level certificate along with their email registration. All students, **including those who have already taken Academic English Part Two and those who need to repeat Academic English Part One,** must register by contacting Howard Atkinson at: howard.atkinson@uni-weimar.de**.**

You will be informed by email when registration opens and when the deadline is. Please do not attempt to register until you have received this Email. Registration Emails should be given the subject heading: AE I Registration.

Leistungsnachweis

continuous assessment

4526502 Academic English Part Two

G. Atkinson Veranst. SWS: 2

Kurs

Mi, wöch., 15:30 - 16:45, Consultations, R.2.18, S143 (indiv.appointments), ab 26.04.2023
Mi, wöch., 17:00 - 18:30, Schwanseestraße 143 - Seminarraum 3.09, Academic English Part I+II alternating, ab 26.04.2023

Beschreibung

Part Two of the Academic English course concentrates on improving and refining aspects of academic writing style. It includes sections on clause and sentence structure, punctuation rules and how to incorporate quotations, statistics and footnotes into academic texts.

Bemerkung

You are advised to take Part One first, although it is possible to take both parts in reverse order or concurrently (i.e. in the same semester). You may only do the latter on the authority of the course leader (Atkinson).

Voraussetzungen

Registration (compulsory)

All students must register. First time particpants are required to present a B2 English Level certificate along with their email registration. All students, **including those who have already taken Academic English Part One and those who need to repeat Academic English Part Two,** must register by contacting Howard Atkinson at: howard.atkinson@uni-weimar.de**.**

You will be informed by email when registration opens and when the deadline is. Please do not attempt to register until you have received this Email. Registration Emails should be given the subject heading: AE II Registration.

Leistungsnachweis

continuous assessment

4556227 Usability Engineering & Testing

J. Ehlers Veranst. SWS: 4

Vorlesung

Di, wöch., 13:30 - 15:00, Marienstraße 13 C - Hörsaal B, Lecture
Do, wöch., 17:00 - 18:30, Lab class online

engl. Beschreibung/ Kurzkommentar

Usability indicates the ”absence of frustration”. But what makes a product or a service really usable? The course will introduce to the basic concepts, theories and methods of usability engineering and testing. We will discuss quality attributes that constitute good usability and will identify design flaws and product defects. Special emphasis will be put on quantitative measures to determine the ease-of-use of a system in various stages of development. Students will learn how to set up and run an empirical user study, including (but not limited to) test setting (field vs. lab), random sampling, designing and hypothesising. We will also discuss procedures for quantitative data analysis

and adequate forms of documentation. To deepen the knowledge, the lecture is accompanied by practical training courses that link theoretical findings to systems and applications in the field of human-computer interaction.

Leistungsnachweis

Empirical exercises (tutorial) and written exam

Research Seminar: Affective Computing (Part 2)

J. Ehlers Veranst. SWS: 3
Seminar
Fr, wöch., 15:15 - 16:45, Marienstraße 13 C - Hörsaal C

Beschreibung

Physiological computing (and its sub-discipline Affective Computing) applies data from the body's periphery (brain waves, skin conductance changes, pupil dynamics, heart rate variability etc.) to generate user-state representations and enable computer systems to dynamically adapt to changes in cognitive and/or affective processing. However, research usually focuses on controlled environments and certified measuring devices. The two-part research seminar aims to explore techniques to apply physiological/affective computing in daily scenarios via adapted instruments and to compare the results to findings from experimental lab studies. Students are asked to form small working groups and tackle (self-chosen) research questions by collecting and analysing physiological data from different experimental settings.

Part 2 aims to carry out data collection in noisy environments and on basis of customized instruments (e.g. smart phones, web cams).

Please note: Taking part does NOT require the attendance of the previous course (Part 1, WiSe 22/23).

Bemerkung

Please note: Taking part does NOT require the attendance of the previous course (Part 1, WiSe 22/23).

Leistungsnachweis

Empirical report

Project

423110005 Bauhaus Gamesfabrik II

C. Wüthrich, W. Kissel, G. Pandolfo Veranst. SWS: 10
Projekt
Mi, wöch., 13:30 - 15:30, Raum 205, Marienstr. 7b, ab 12.04.2023

Beschreibung

"Bauhaus Gamesfabrik" ist ein interdisziplinäres Projekt zwischen Studierende der Fakultät K&G und der Fakultät Medien, dass sich in diesem Jahr mit der praktischen Entwicklung von Computerspielen (auch analogen Spielformaten) befasst.

Bemerkung

Ort und Zeit werden zur Projektbörse bekanntgegeben.

Voraussetzungen

Studierende der Medieninformatik sollten Programmierkenntnisse mitbringen.Studierende der Medienwissenschaft ein grundlegendes Interesse für Storytelling / Game Design

Leistungsnachweis

Abschlusspräsentation, fertiges Spiel.

423110006 Content Warning Detection

B. Stein, M. Wolska, M. Wiegmann Veranst. SWS: 10
Projekt

Beschreibung

Content warnings are often assigned to online content to give vulnerable groups an opportunity to avoid potentially discomforting or distressing content. However, most online content requires the creator to add warning labels, which is often not done. We have previously created a large datasets (300k+) fanfiction stories with warning labels. In this project, we want to develop (one or more) machine learning models that add content warnings automatically. Depending on our success, we might submit the best model to a scientific competition on this dataset.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Abschlusspräsentation und Ausarbeitung

423110007 Fifty shades of ChatGPT

B. Stein, M. Gohsen, K. Heinrich, J. Bevendorff Veranst. SWS: 10
Projekt

Beschreibung

Large language models such as ChatGPT or GPT-3 represent a significant advance in the field of artificial intelligence. These models are trained on massive amounts of text data, which enables them to understand and generate human-like text. This project aims to investigate large language models for their capabilities to solve the following problems: (1) generating conversational responses and matching the generated information with knowledge from a knowledge base, and (2) generating coherent and engaging stories. A common requirement for these tasks is a low-latency infrastructure for our own language model, which we will try to develop in this project.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Abschlusspräsentation und Ausarbeitung

423110009 Homo Economicus Meets the Metaverse

B. Fröhlich, E. Schott, S. Mühlhaus, T. Zöppig Veranst. SWS: 10
Projekt

Beschreibung

Given current developments in virtual reality technologies and the metaverse, it is time to examine how we make decisions in social virtual environments. Behavioral economics studies the human decision-making process by conducting various experiments based on game theory and comparing the results to the best economic solutions. We know from real-world studies that psychology, culture, emotions, and cognition generally influence our decisions and keep us from acting like homo economicus, a hypothetical human being who makes optimal decisions in accordance with their rational self-interest.

In this project we will study the influence of the virtual environment and the appearance and expressiveness of avatars on decision making in social virtual reality. This behavioral economics study will be prepared, performed and analyzed in collaboration with Prof. Jürgen Rösch, Professor of Digital Economics, and a group of media management master's students.

Bemerkung

time and place: t.b.a.

Voraussetzungen

Solid software programming / scripting experience (e.g. C#, C++, Python). Experience in Unity strongly recommended.

423110010 Kryptographie im Kopf -- Single-Page Crypto Challenge

S. Lucks, J. Leuther, N. Lang Veranst. SWS: 10
Projekt

Beschreibung

Does a cryptosystem need to be complex in order to be secure? No! We want to create a simple state-of-the-art cryptosystem whose source code can fit easily onto one single page in print, or even on two slides for a presentation -- without refering to a crypto library.

Simplicity does not mean that the computations will be trivial or that users have to make compromises about the security. Simplicity means that independent implementations ``from memory'' will be compatible with each other: when a ``sender'' encrypts a message M under a key K and a ``receiver'' decrypts the ciphertext under the same key K, then the receiver will get M again, even when both sender and receiver are using their own implementation of the scheme they both memoized.

Bemerkung

time and place to be announced at the project fair.

room:S143 Medsec/Webis-Lab

Leistungsnachweis

Abschlusspräsentation, Abschlussbericht

423110011 LinuxDome 2.0 / Imaging Pipelines

F. Andreussi, G. Pandolfo, C. Wüthrich Veranst. SWS: 10
Projekt

Beschreibung

In this project, we will work on two distinct tasks: on one side, the physical assembly of

a new FullDome at S134, including a 3D soundsystem and multiple projectors

running on a F.O.S.S. platform. On the other side, we will need to specify and

build a Vulkan based System allowing to pipeline output from

video processing software into the input of a different video processing hardware,

in a similar way that Syphon and Spout do it in the Mac and Windows environments.

Bemerkung

time and place to be announced at the project fair.

423110012 Mining Arguments from Podcasts

B. Stein, N. Mirzakhmedova, M. Wiegmann, J. Kiesel Veranst. SWS: 10
Projekt

Beschreibung

Computational argumentation tries to present a user with pro and/or contra arguments on a controversial topic. These arguments are usually mined (extracted) from long and well-structured debates from websites like debate.org. However, the debates on these websites often cover few and outdated topics. An alternative source for a broad variety of up-to-date topics are transcribed podcasts. This project will leverage cutting-edge argument mining technologies and apply them to podcast data, providing insights into the nature of arguments in this context and how they differ from traditional debates.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Abschlusspräsentation und Ausarbeitung

423110013 Projekt MLOM II: Machine learning models on Arduino (Part II)

J. Ringert, B. Burse Veranst. SWS: 10
Projekt

Beschreibung

As part of the Software Engineering for Trusted Autonomous Systems we will develop a platform for an autonomous vehicle based on the Robot Operation System (ROS).

Bemerkung

Time and place will be announced at the project fair.

423110014 Projekt SETAV III-Software Engineering for Trusted Autonomous Systems (PartIII)

J. Ringert, .. Soaibuzzaman Veranst. SWS: 10
Projekt

Beschreibung

As part of the Software Engineering for Trusted Autonomous Systems we will develop a platform for an autonomous vehicle based on the Robot Operation System (ROS).

Bemerkung

Time and place will be announced at the project fair.

423110015 Quantum Crypto Rescue

S. Lucks, J. Leuther, N. Lang Veranst. SWS: 10
Projekt

Beschreibung

The future advent of quantum computers leads to a new analysis of current cryptographic schemes toward their post-quantum security. This does not only include asymmetric crypto schemes but also symmetric ones.
The goal of this project is to discuss and elaborate strategies of salvaging currently used schemes such that we will still be able to use them securely despite having quantum computers.

Bemerkung

time and place to be announced at the project fair.

Room: S143 Medsec/Webis-Lab

Voraussetzungen

At least one lecture passed in Cryptography (e.g. Introduction to Modern Cryptography) and one in the field of theoretical computer science

Leistungsnachweis

Abschlusspräsentation, Abschlussbericht

423110017 Teaching VR in VR

B. Fröhlich, A. Lammert, E. Schott, T. Zöppig Veranst. SWS: 10
Projekt

Beschreibung

Since the pandemic, distance learning, teaching and training services have thrived. Last semester, we took our first steps towards exploring techniques for immersive teaching and learning of virtual reality concepts in virtual reality. Our vrEDUsys Unity teaching framework supports live teaching in VR as well as recording and playback of lectures in VR. Compared to regular teaching methods, this gives students first-hand exposure to virtual reality concepts. As a result, students have a greater awareness of usability issues and possible usage scenarios of virtual reality technology and 3D interaction concepts.

In this project, we aim to explore and develop further tools to support students and teachers in learning and teaching in virtual reality. Our research will start with reviewing and designing different concepts for virtual classrooms to address the following questions: What is the best way to combine knowledge transfer and hands-on experience in an interactive virtual environment? To what extent can gamification be used to foster a deeper understanding of different virtual reality techniques and concepts?

During the project you will be encouraged to design, develop and prototype your own concepts. The results of this project can be incorporated into the next iteration of our vrEDUsys Unity teaching framework and may be experienced by many future students.

Bemerkung

time and place: t.b.a.

Voraussetzungen

Solid software programming / scripting experience (e.g. C#, C++, Python). Experience in Unity strongly recommended.

Hot Topics in Computer Vision: Cloudy with a chance of scene understanding

V. Rodehorst, C. Benz, P. Debus, J. Eick
Projekt

Beschreibung

Die Teilnehmer werden an ein aktuelles forschungs- oder industrierelevantes Thema herangeführt. Es ist nicht beabsichtigt einen festgelegten Bereich in voller Breite zu explorieren. Stattdessen werden die Teilnehmer mit der vollen Komplexität eines begrenzten Themas konfrontiert und die Eigeninitiative gefördert. Es ermöglicht einen Einblick in die Forschungs- und Entwicklungsprojekte des Fachgebiets.

Bemerkung

Ort und Zeit werden zur Projektbörse bekanntgegeben.

Voraussetzungen

Gute Programmierkenntnisse (z.B. C/C++, MATLAB, OpenCL/CUDA)

Leistungsnachweis

Aktive Mitarbeit, Einführungsvortrag, Abschlusspräsentation, Dokumentation

Multimodal Sequence Representations for Feed Data

B. Stein, T. Gollub, J. Kiesel Veranst. SWS: 10
Projekt

Beschreibung

Social media has become a significant part of our every day life, and continues to change the way we interact with each other on a global scale. In this project, we work on the development of computational tools and methods for the analysis of social media at large scale. A core task will be the development of a neural representation for social media feeds (i.e., sequences of posts that may be commented and liked) using pre-trained multimodal neural networks from Hugging Face (https://huggingface.co/). The envisioned representation is supposed to capture the topical preferences of a feed, including topic-specific stances. Along the work on representations, we will work on an analysis toolbox facilitating among others the clustering of feeds into user groups, the classification of feeds, e.g. with respect to specific stances, and even the generation of feed-related posts.

Bemerkung

Time and place will be announced at the project fair.

Leistungsnachweis

Abschlusspräsentation und Ausarbeitung

Our Digital Limbs: Exploring Full-Body Movements for Stress Measurement

J. Ehlers Veranst. SWS: 10
Projekt

Beschreibung

In the first third of the project, participants will work themselves into the Rokoko Studio Pro Software and provide a brief documentation for future generations of users. Afterwards they are asked to design and carry out an empirical study on the possibilities of determining levels of stress through various movements or body postures. Findings need to be statistically tested and documented in a lab report.

Bemerkung

time and place will be announced at the project fair.

Voraussetzungen

We assume you are interested to explore a software that enables to track body movements and to conduct an empirical study on the relationship between motions and stress experience.

Leistungsnachweis

Project members need to get familiar with the Rokoko Studio Pro Software and provide a brief documentation for future users. Also, they will implement an empirical study with regards to stress-related body movements or postures. The latter findings need to be statistically tested and documented in a lab report.

Rearranging Pixels X

C. Wüthrich, F. Andreussi Veranst. SWS: 10
Projekt

Beschreibung

Since the introduction of digital cameras, computer raster monitors and printing devices, the world of pixels has been ordered on a square based raster, limiting optimal signal sampling to two main directions, and creating collateral problems where the grid density causes undersampling of the light signal. This project will tackle the problem,

exploring new and unconventional ways of sampling light signals. The focus will be set on the development of new robust methods and on their evaluation, and compare traditional square sampling to the new methods. The conception and development of new devices will be a major focus of the project.

Bemerkung

Time and place will be announced at the project fair.

Specialization

301016 Complex dynamics

B. Rüffer Veranst. SWS: 4
Vorlesung
Di, wöch., 07:30 - 10:45, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be able to analyse mathematical models that describe dynamic behaviour, as they occur in engineering (e.g. mechanical coupling of building structures), in biology and in physics, but also in multi-agent systems in computer science, or as opinion dynamics in psychology. Based on examples from different disciplines, students learn to build simplified models that allow to answer questions on their long-term behaviour. Students will be able to apply methods of feedback design that help shape the dynamics of a given system, along with the relevant stability concepts. As several topics lend themselves for computer simulation, students of this course will develop a proficiency to both implement and analyse mathematical models using computational tools and software.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B.Sc., knowledge in Matlab or Python

Leistungsnachweis

1 written exam

”Complex dynamics”

120 min (100%) / **SuSe** + WiSe

301017 Mathematics for data science

B. Rüffer, M. Schönlein Veranst. SWS: 4
Vorlesung
Mi, Einzel, 13:30 - 16:45, Coudraystraße 13 B - Hörsaal 3, 05.04.2023 - 05.04.2023
Mo, wöch., 09:15 - 12:30, Coudraystraße 13 A - Hörsaal 2

Beschreibung

After the course the students will be familiar with the fundamental concepts of data science. The participants can analyse given data sets with respect to dimensionality reduction and clustering. They also know the basic structure of neural networks and support vector machines to solve classification tasks. The participants know relevant methods from linear algebra and optimization and can apply these techniques. This embraces the design of appropriate algorithms and the implementation of different numerical methods to solve the corresponding problems.

Bemerkung

Examples of complex dynamics. Models for dynamical systems in continuous and discrete time. Computer simulation. Control and Feedback. Stability, stabilization, and Lyapunov functions. Coupled systems: Disturbance or Cooperation? Networks of systems. Consensus. Synchronization.

The topics will be presented in a lecture, deepened by exercises. Some of the exercise include computer programming and simulation.

Voraussetzungen

B. Sc.; Analysis and Linear Algebra at Bachelor level, knowledge of Matlab or Python

Leistungsnachweis

1 written exam

”Complex dynamics”

120 min (100%) / **SuSe** + WiSe

417130003 Discrete Optimization

A. Jakoby Veranst. SWS: 4

Vorlesung

Do, wöch., 15:15 - 16:45, Schwanseestraße 143 - Seminarraum 2.16, Lecture , ab 13.04.2023
Do, wöch., 17:00 - 18:30, Schwanseestraße 143 - Seminarraum 2.16, lab class, ab 13.04.2023

Beschreibung

Diskrete Optimierung

Die diskrete / kombinatorische Optimierung ist ein Gebiet an der Schnittstelle von Mathematik und Informatik. Anwendungen für derartige Optimierungsprobleme sind in den vielfältigsten Bereichen zu finden.

Betrachtet werden sowohl diskrete Optimierungsprobleme, die effizient lösbar sind (kürzeste Wege, Flußprobleme), als auch NP-schwierige Probleme. Für letztere werden sowohl exakte Verfahren (Greedy-Algorithmen über Matroiden, Branch-and-Bound-Verfahren), als auch Heuristiken und Metaheuristiken zur näherungsweisen Lösung behandelt.

engl. Beschreibung/ Kurzkommentar

Discrete Optimization

Discrete / combinatorial optimization is an area at the borderline of mathematics and computer science. Applications for such optimization problems can be found in the most varied areas.

Consideration is given to discrete optimization problems, which are efficiently solvable (e.g. shortest paths, flow problems), as well as NP-hard problems. For the latter, both exact methods (greedy algorithms on matroids, branch-and-bound methods), as well as heuristics and metaheuristics, are introduced.

Voraussetzungen

Bsc in a relevant study field

Leistungsnachweis

oral examination (individual apppointments via Moodle)

4345550 Cryptographic Hash Functions

S. Lucks, N. Lang, J. Leuther Veranst. SWS: 4

Vorlesung

Mi, wöch., 11:00 - 12:30, Marienstraße 13 C - Hörsaal D, Lecture, ab 12.04.2023
Fr, wöch., 11:00 - 12:30, Schwanseestraße 143 - Seminarraum 3.09, Lab class, ab 14.04.2023

Beschreibung

Kryptographische Hashfunktionen sind unübliche kryptographische Algorithmen, da sie, im Gegensatz zu Blockchiffren und MACs ohne geheimen Schlüssel auskommen. Dennoch, sie gehören zu den Arbeitstieren in vielen Algorithmen und werden in so gut wie allen kryptographischen Protokollen verwendet (z. B.: SSH, SSL/ TLS, RSA-OAEP). Seit dem Jahre 2000, haben Kryptographen kritischen Sicherheitslücken in alltäglich genutzen Hashfunktionenwie MD5 oder SHA-1 gefunden. Nur die SHA-2-Familie scheint gegen solche Angriffe resistent zu sein. Jedoch, da die Strukture von SHA-2 der von SHA-1 sehr ähnelt, hat das NIST einen Wettbewerb ausgerufen, um einen neuen Hashfunktionen-Standard (SHA-3) zu finden. Zwei der eingereichen Kandidaten für den Wettbewerb stammen vom Lehrstuhl für Mediensicherheit der Bauhaus-Universität Weimar, wobei einer (Skein) es sogar ins Finale geschafft hat. Im ersten Teil wird es um die Einführung und praktische Nutzung kryptographischer Hashfunktionen gehen. Der zweite Teil beschäftigt sich mit generischen Angriffen und deren Einfluss in der Praxis. Der dritte Teil wird sich um die SHA-3-Kandidate drehen. Basieren auf den Erkenntnissen und Kandidate des Password-Hashing-Wettbewerbs (PHC), wird es einen möglichen vierten Teil der Vorlesung geben, der sich mit Password-Hashing und den darunterliegenden Problemstellungen, sowie mit den Kandidaten des Wettbewerbs beschäftigt.

Voraussetzungen

Zulassungsvoraussetzung: Eine vorausgegangene Einfürung in die Kryptographie, z.B. "Kryptographie und Mediensicherheit", "Modern Cryptography", oder ein entsprechender Kurs einer anderen Hochschule. Studierende, die die Einführung an einer anderen Hochschule besucht haben, müssen diese Voraussetzung bei der Anmeldung zur Prüfung anhand ihres "Transcript of Records" nachweisen.)

Leistungsnachweis

mündliche Prüfung