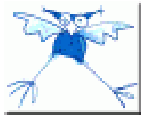
Algorithms for Internet-Applications

Jürgen Branke

Wintersemester 2007/2008

Institut für Angewandte Informatik
und Formale Beschreibungsverfahren
Universität Karlsruhe (TH)

http://www.aifb.uni-karlsruhe.de/Lehre/Winter2007-08/AIA/



Universitärer Lehrverbund Informatik

Lecturer: PD. Dr. Jürgen Branke
Kollegiengebäude am Ehrenhof
Room 223
Office hours: Wednesday 11:00 - 12:00
e-mail: branke@aifb.uni-karlsruhe.de

This course will be presented as

- live lectures
- lecture is recorded : slides, annotations, sound using Camtasia
- recorded lectures available as avi-documents (streaming and avi, via the web pages of the course and at DIVA)
- can be viewed with **any media player** (freely available for various operating systems)
- best viewed with the **Camtasia player** (link on web page)

All relevant information on this course available on the web page
http://www.aifb.uni-karlsruhe.de/Lehre/Winter2007-08/AIA/

Online-VV https://lsf.zvw.uni-karlsruhe.de/

„Virtual University“

- **Course has been part of the “Universitärer Lehrverbund Informatik” (bmbf-project, 2001-2003),**
  - Local students at Karlsruhe
  - Distant students / learners from other universities (e.g. at Hannover, Freiburg, Mannheim)
  - Distant students follow recorded lectures, get on-line tutoring

- **Current situation**:
  - Course is offered simultaneously to students at University of Hannover
  - Course is offered within “EUCORvirtuale” to all students of the EUCOR universities
- All students from other universities who want to take this course for credit, should send a message to my assistant
  Andreas Kamper <aka@aifb.uni-karlsruhe.de>

Time and location of this course:

Scheduled Times: Tuesday 9:45 – 11:15

Location: Multimedia Lecture Hall
(Faculty of Informatics, building 50.34, room -102)

Tutorials

- Assistant: Dipl.-Inform. Andreas Kamper
  Room 225, Kollegiengebäude am Ehrenhof
  Office hour: as arranged
  Email: aka@aifb.uni-karlsruhe.de

- Unfortunately: no tutors
- Instead: One large tutorial every other week
  Friday, 11:30 - 13:00, Room -102, Building 50.34
- First tutorial: 9.11.2007

Concept and Bonus

- Goals:
  - Examples for typical problems
  - Exercise how to approach typical problems
  - Possibility to ask questions
  - Incentive for students to learn during the semester
  - Early feedback for students
- Concept:
  - Forum
  - 6 assignments (exercises in tutorials + home assignments)
  - Assignments will be discussed in the tutorials, there you will get the solutions.
  - For learning control: at the end of each tutorial (except first one): 10 minute quiz
    - Bring your student ID
  - 1 programming assignment, its correct handling will count as one of the two needed well-done tasks of the bonus-examination
  - Bonus if you solve 3 out of (5 quizes + programming assigment)
- **Bonus amounts to 3 extra points for a passed exam (i.e. an improvement of your mark by 0.3)**
- **Students out of Karlsruhe get the possibility to make a Bonus exam in January.**

Algorithms for Internet-Applications

- 4,5 / 5 ECTS credits / (2+1) SWS ("Semesterwochenstunden")

at Karlsruhe, this course is offered for students of

- **Business Engineering (Wirtschaftsingenieurwesen), Economics Engineering (Technische VWL)**
  - core course (“Kernvorlesung”)
  - may be combined with any other course in Applied Informatics (offered by Institute AIFB)
  - within and informatics module in the new master program
  - within an informatics module in the new bachelor program
- **Information Engineering and Management (Informationswirtschaft)**
  - one of the courses in elective area 5 : "network information services"
  - exam in "informatics electives" may be split into different exams for individual courses
  - within an informatics module in year 3 of the new bachelor program
  - within an informatics module in the new master program
- and for some other programmes (Business Math, Techno Math, ...)

at Hannover or at an EUCOR university :
you have to check with your local programme of study

What type of exam?

- written exam on Tuesday or Wednesday of the first week after the end of term (Feb 19 or 20, 2008)
- **written exam questions will be in English but you may answer in German.**

Why do we present English courses?

- Internationalisation
- Improving English language skills
- preparation for
  - foreign studies
  - job life
  - “the global marketplace”
- attract foreign students

English courses are offered in (almost) all subjects of this faculty.

Motivation

The internet has changed our lives...

... the way we communicate

- Email
- Instant messaging
- Voice over IP
- Video conferencing
- Computer Supported Cooperative Work (CSCW)

-> the distance between communication partners is no longer determined by their spatial distance but by communication bandwidth and latency

... the way we search for information

- Search engines (Google, Yahoo, ASK, ...)
- Wikipedia
- Newsgroups/Forum
- Job markets
- Electronic journals
- ...

... the way we shop

- Amazon
- iTunes
- ebay
- mobile.de, autoscout24.de
- Electronic banking
- Hotels
- Flights
- Personalized products (Dell, Shirts, Nike, ...)

... the way we compute

- Grid computing
- Seti@home

... the way we teach

- Recorded lectures
- Podcasts
- Teleseminars
- Forum
- Learning management systems
- combination of curricula contents
  - from different real universities,
  - from different authors

Do we still need regular lectures?

Motivation

The internet has changed our lives...

... and algorithms make the difference!

This course is about some advanced algorithms for internet applications.

Contents

What do **you** expect?

What would **you** like to learn?

... the way we communicate

- Email
- Instant messaging
- Voice over IP
- Video conferencing
- Computer Supported Cooperative Work (CSCW)

-> the distance between communication partners is no longer determined by their spatial distance but by communication bandwidth and latency

How can we ensure a reliable communication?

How can we avoid undesired messages?

What can we do about undesired communication of criminals?

How do we make sure the person we communicate with is the person we think it is?

How do we make sure that the message has not been modified?

How can we make sure no one else can read the messages we send?

How can we transfer and store large amounts of data?

... the way we search for information

- Search engines (Google, Yahoo, ASK, ...)
- Wikipedia
- Newsgroups/Forum
- Job markets
- Electronic journals
- ...

How can we efficiently search huge databases?

How can we identify relevant information?

How can we ensure the quality of information?

What is the price for information?

How do we protect intellectual property?

What are the consequences of the Internet for politics ?

... the way we shop

- Amazon
- iTunes
- ebay
- mobile.de, autoscout24.de
- Electronic banking
- Hotels
- Flights
- Personalized products (Dell, Shirts, Nike, ...)

How can we pay electronically?

How can we remain anonymous?

How do we find the products we want?

... the way we compute

- Grid computing
- Seti@home

How is computing power distributed?

How do we protect against faulty data?

How do we ensure interoperability of different platforms?

How can we protect ourselves (data, computer) from access through others?

Overview: *Algorithms for Internet Applications*

2 Internet History and Technology

- history
- technology
  - TCP / IP, routing
  - IPv6
- (ATM)

3 Searching for Information

- textual search (pattern matching)
- information and document retrieval
- full text search
- index construction
- search engine technology

overview: *(cont.)*

4 Cryptographic Algorithms

- steganography/watermark
- symmetric methods (DES, IDEA, AES..)
- asymmetric methods
- RSA, Diffie-Hellmann
- digital signatures
- authentication
- protocol for secure communication

5 Electronic Payment Systems

- requirements
- SSL/TLS
- SET
- CyberCash
- DigiCash (ecash)
- smartcards

Overview (cont.)

6 Firewalls

7 Data Compression

- Huffman
- Lempel/Ziff
- ZIP
- fractals
- iterated function systems
- MP3
- JPEG

further interesting topics:

- **digital libraries**
  - electronic publishing
  - electronic documents
  - information services
  - retrieval
- **web computing**
  - hypercomputing
  - metacomputing
  - grid computing
  - “algorithm-servers”
- **spam protection**
  - spam filters
  - authentication
  - spam barriers
- **electronic commerce**
  - EDI/EDIFACT
  - business-to-consumer applications
  - business-to-business applications

(rather to be found in Angewandte Informatik II)

References:

Multitude of information in the Internet, e.g:

- web catalogs like yahoo (www.yahoo.com)
- RFC's (http://www.cis.ohio-state.edu/hypertext/information/rfc.html)•
- WWW- Consortium (http://www.w3.org/) •
- Internet history (http://www.isoc.org/internet-history/) •
- specific links on web pages of this course
- ...

Journal articles:

- Communications of the acm (lots of survey articles and special topics,...)
- IEEE Computer
- IEEE Internet Computing
- …

References *(cont.)*

Books:

- Tanenbaum: Computer Networks, 4th edition, Prentice-Hall 2003
- Frakes, Baeza-Yates: Information Retrieval: Data Structures and Algorithms. Prentice Hall 1992
- Baeza-Yates, Ribeiro-Neto: Modern Information Retrieval. Addison-Wesley, 1999
- Stallings: Network and Internetwork Security.3rd edition, Prentice Hall
- Stallings: Cryptography and Network Security. Prentice Hall, 2002
- Garfinkel, Spafford: Web Security & Commerce, O'Reilly&Ass., 1997
- Wobst: Abenteuer Kryptologie : Methoden, Risiken und Nutzen der Datenverschlüsselung, 3rd edition. Addison-Wesley, 2001.
- Schneier: Applied Cryptography, John Wiley, 1996
- Furche, Wrightson: Computer money : Zahlungssysteme im Internet [Übers.: Monika Hartmann]. - 1. Aufl. - Heidelberg : dpunkt, Verl. für Digitale Technologie, 1997.
- Lynch, Lundquist: digital money, The New Era of Internet Commerce. Wiley 1996
- …