Proseminar Bakkelaureat TM 501.549 (2PS)

(Datensicherheit und Versicherungsmathematik)
Ch. Aistleitner, W. Müller

Themenliste

Wahrscheinlichkeitstheorie:

1. Erzeugung nicht gleichverteilter Zufallszahlen (Methoden zur Erzeugung von Zufallszahlen aus bekannten Verteilungen wie Exponentialverteilung, Cauchyverteilung, Normalverteilung und Poissonverteilung)
   Krengel S. 459–462.

2. "Coupon Collectors Problem" (Problem der vollständigen Sticker-Alben): Wie viele Päckchen mit Bildern von Fußballern muß man kaufen um das Album zur Fuballweltmeisterschaft 2006 vollständig zu füllen? Wie beschleunigen Tauschstrategien den Vorgang?
   K. Hayes, A. Hannigan , Stirzaker.

3. Das Langzeitverhalten von Markovketten mit endlichem Zustandsraum (Wie verteilen sich die Versicherungsnehmer im Bonus-Malus System der KfZ-Haftpflichtversicherung auf die Prämienstufen?)
   Krengel S. 204–206, Hesse S. 338–345.

4. Parrandos Paradoxon (Es gibt zwei für den Spieler ungünstige Spiele, die zu einem langfristig günstigen Spiel kombiniert werden können.)
   Hesse S. 347–349.

Literatur zur Wahrscheinlichkeitstheorie:
Ch. Hesse, *Angewandte Wahrscheinlichkeitstheorie*, Vieweg 2003, K. Hayes, A. Hanning, *Trading coupons: completing the World Cup football sticker album*, Significance, September 2006, vol 3, issue 3, p. 142-144, U. Krengel, *Einführung in die Wahrscheinlichkeitstheorie und Statistik*, 7. Auflage, Vieweg 2003. D. Stirzaker, *Elementary Probability Theory*, Cambridge Univ. Press, 2003.

Datensicherheit:

5. Klassische Verschlüsselungsverfahren:
   Cäsar-Substitution, Substitutionskryptosysteme im allgemeinen, Vignére-System, Hill-System, lineare Blockchiffren mit Kryptoanalyse

6. DES, AES:
   Unterschied zwischen DES und AES, Funktionsweise von AES insbesondere Schlüsselexpansion, Vorrunde, Verschlüsselungsrunde, Schlußrunde

7. Public-Key-Kryptograpie:
   Unterschied zu symmetrischen Verschlüsselungsverfahren, Einwegfunktionen, Diffie-Hellman-Schlüsseltauschverfahren, Massey-Omura-Kryptosystem

8. RSA-Verfahren I:
   Mathematische Grundlagen und Korrektheit des RSA-Verfahrens, schnelle Ver- und Entschlüsselung, Zusammenhang zwischen RSA-Sicherheit und dem Faktorisierungsproblem

9. RSA-Verfahren II:
   Praktische Wahl der Parameter beim RSA-Verfahren: Länge des Schlüssels, Wahl des Exponenten, etc., Attacken auf das RSA-Verfahren: Low-Exponent-Attacke, Common-Modulus-Attacke, Angriff durch Iteration

10. El-Gamal-Verfahren:
    Verschlüsselungsvorschrift und Korrektur des Verfahrens über Restklassenringen modulo einer Primzahl, Verallgemeinerungen, Ausblick auf El-Gamal über elliptischen Kurven (Vorteile?)

11. Authentikation und digitale Signatur:
    Nachrichtenauthentikation durch Cipher-Block-Chaining-Modus und DSA-Verfahren, Benutzerauthentikation durch elektronische Unterschrift, Passwortmechanismus mittels Einwegfunktion, Challenge-and-Response-Methode

12. Zero-Knowledge Proofs:
    Begriffsbildung, quadratische Kongruenzen, Protokoll und Korrektheit des Fiat-Shamir Schemas

13. Deterministische Primzahltests:
    Probedivision, Primitivwurzeln und Pratt-Zertifikat, Agrawal-Kayal-Saxena-Test

14. Probabilistische Primzahltests:
    Fermat-Test, Pseudoprimzahlen und Carmichael-Zahlen, Miller-Rabin-Test

15. Faktorisierungsmethoden:
    Probedivision, Pollard'sche $(p-1)$-Methode, Fermat-Faktorisierung

Literatur zur Datensicherheit:
A. Konheim: *Cryptography. A Primer*, A. Menezes et al.: *Handbook of Applied Cryptography*, R. Mollin: *An Introduction to Cryptography*, N. Koblitz: *A course in number theory and cryptography*, N. Koblitz: *Algebraic aspects of cryptography*, J. Buchmann: *Einführung in die Kryptographie*

Codierungstheorie:

16. Grundlagen der Codierungstheorie:
    Blockcodes, Gewicht und Hamming-Distanz, Prinzip des Decodierens, Paritycheck-Code und Wiederholungscode

17. Linearcodes:
    Minimaldistanz und Gewicht bei Linearcodes, Anführer und Fehlerkorrekturs-schema, Generator- und Kontrollmatrix, Syndrom und Fehlerkorrektur

Literatur zur Codierungstheorie:
D. Hoffmann et al.: *Coding Theory. The Essentials*, S. Ling und C. Xing: *Coding Theory. A first course*, C. Fuchs: *Algebraisch geometrische Codes*, O. Pretzel: *Error-Correcting Codes and Finite Fields*

Theoretische Informatik:

18. NP-vollständige Probleme:
    Begriffsbildung, Methode zur Überprüfung auf NP-Vollständigkeit, ausgewählte bekannte NP-Probleme: z.B. SAT, Rucksackproblem, Travelling-Salesman,...

19. Sortieralgorithmen:
    Einfache Sortierverfahren, Quicksort und mathematische Analyse, weitere Sortierverfahren (z.B. Bubblesort, m-Wege-Mischen)

20. Rekursive Funktionen:
    Primitiv-rekursive Funktionen und Programme mit Schleifen, rekursive Funktionen und rekursive Programme, Ackermann- und Goodstean-Funktion

Literatur zur Theoretischen Informatik:
U. Manber: *Introduction to Algorithms. A creative approach*, T. Cormen et al.: *Introduction to Algorithms*, N. Koblitz: *Algebraic aspects of Cryptography*, L. Blum et al.: *Complexity and real Computation*, J. van Leeuwen: *Algorithms and complexity*, M. Davis: *Computability and Unsolvability*, D. Cohen: *Computability and Logic*

Versicherungsmathematik:

21. Lebensdauer eines x-jährigen:
    Sterbe- Überlebenswahrscheinlichkeiten (ganz- bzw. unterjährig), Sterblichkeitsintensität, klassische analytische Verteilungen, Schätzung von Sterbenswahrscheinlichkeiten

22. Kapitalversicherungen:
    Einfache Versicherungsformen, aufgeschobene Versicherung, Auszahlung unmittelbar nach Ableben

23. Kommutationszahlen und Äquivalenzprinzip:
    Definitionen und Bildungsgrundlagen, Äquivalenzprinzip am Beispiel von Erlebens- bzw. Todesfallversicherungen, Nettojahresprämien

24. Deckungskapital:
    Prospektive und retrospektive Methode, rekursive Darstellung, Überlebensrisiko, unterjähriges Deckungskapital

25. Gesamtschaden eines Portfeuilles:
    Individuelles- und kollektives Risikomodell, Rückversicherung (Exzedenten, Stop-Loss), Normalverteilungs- und Poissonapproximation

26. Versicherung auf mehrere Leben:
    Versicherungsarten, elementare Beispiele für zwei Personen (Erlebensfallversicherung, Verbindungsrenten, Todesfallversicherungen), Zustand verbundener Leben, Gompertz'sches Sterbegesetz, allgemeiner symetrische Zustand

27. Pensions- und Hinterbliebenenversicherung:
    Rechnungsgrößen, Ausscheideordnungen, Anwartschaft, entsprechende Renten

28. Krankenversicherungsmathematik:
    Kopfschaden (normierter Kopfschaden, Profil), Prämien nach Art der Lebensversicherung, Altersrückstellung (Zuführung)

29. Klassische Risikomodelle:
    Individuelles- bzw. kollektives Risikomodell, freie Reserve, Cramér-Lundberg Modell, Sparre-Andersen Modell, Schadenshöhenverteilung

30. Solvency I&II:
    Mindestkapitalanforderungen, Risikomanagement, Berichterstattungspflicht

Literatur zur Versicherungsmathematik:
N. Bowers: *Actuarial Mathematics*, H.U. Gerber: *Lebensversicherungsmathematik*, F. Isenbart und H. Münzer: *Lebensversicherungsmathematik für Praxis und Studium*, W. Saxer: *Versicherungsmathematik I,II*

Finanzmathematik:

31. Zinssätze:
    Verschiedene Zinssätze (Schatzzinsen, LIBOR, Nullkupon Zinsen), Anleihen bzw. Bonds (Null Kupon Bond, Kupon Bond), Forward Zinsen, Forward Rate Agreement

32. Einfache Derivate:
    Arbitrage, Forward, Future, long Position, short Position, Optionen (Call, Put Option), Europäische-, Amerikanische Optionen

33. Exotische Optionen:
    Asiatische Optionen, Barriere Optionen, Lookback Optionen, Shout Optionen, Exchange Optionen

34. Binomiale Optionspreis Modelle:
    1-Stufen Binomial Modell, Risiko-Neutrale Bewertung, 2-Stufen Binomial Modell, Anwendung (Amerikanische Option)

35. Zinsderivate:
    Zins-Futures, Swaps, Swaptions, Caps

36. Hedging (Hedgen mit Futures):
    Grundidee, short Hedge, long Hedge, Basis Risiko, optimal Hedge Ratio, Probleme (Rolling the Hegde Forward)

37. Finanzkrise:
    Große Verluste, Absicherung des Risikos, interne Kontrollen

Literatur zur Finanzmathematik:
J. Hull: *Options Futures and other derivatives*, P. Zhang: *Exotic Options*, I. Nelken: *The Handbook of Exotic Options*, N. Bingham und R Kiesel: *Risk-Neutral Valuation*