Ad-hoc Networking – Models and Methods

Holger Hermanns Sven Johr

Universität des Saarlandes

May 4, 2004

Part I

A brief introduction to probability theory

Characteristics

- Quantitative description of trials with random outcome.
- Arbitrary number of trials under the same conditions.
- Events related to outcomes.
- Different events occur with different frequentness.

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Fundamental Terms

- Sample space.
  - Collection of elementary events.
  - Notation: Ω.
- Set of events.
  - Collection of sets of elementary events.
  - Notation: $E \subseteq 2^{\Omega}$.
- Probability function.
  - Mapping from E to $[0, 1]$.
  - Notation: $\Pr : 2^{\Omega} \longrightarrow [0, 1]$.

Probability Function

- $0 \leq \Pr[e] \leq 1, e \in E$.
- $\Pr[\Omega] = 1$.
- $e_1, e_2, \ldots$ events with $e_i \cap e_j = \emptyset$ for all i, j:

$$\Pr\left[\bigcup_i e_i\right] = \sum_i \Pr[e_i] \ .$$

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Probability Space

- $(\Omega, E, \Pr)$.
- Sample space Ω.
- Set of events E. σ-algebra E on Ω.
  - $\emptyset \in E$.
  - $A \in E \Rightarrow A^C \in E$.
  - $A_1, A_2, \dots \in E \Rightarrow \bigcup_i A_i \in E$.
- Probability function $\Pr$ on E.

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Example

Rolling a fair die.

- $\Omega = \{1, 2, 3, 4, 5, 6\}$.
- $E = 2^{\Omega}$.
- $\Pr[\{e\}] = \frac{1}{6}$, $e \in \Omega$.
- Probability of rolling an even number $\Pr[\{2, 4, 6\}] = \frac{1}{2}$.
- e_0: rolling an even number, e_1: rolling at least 3.
  - $\Pr[e_0 \cup e_1] = \Pr[e_0] + \Pr[e_1] - \Pr[e_0 \cap e_1] = \frac{1}{2} + \frac{2}{3} - \frac{1}{3} = \frac{5}{6}$.

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Conditional Probability

- Probability of e_1 given that e_0 holds.
- Notation: $\Pr[e_1 | e_0] = \frac{\Pr[e_1 \cap e_0]}{\Pr[e_0]}$.
- Elementary events of e_0 induces a sample space.
- Probability of event $e_1 \cap e_0$ given the induced sample space.
- Often used to calculate probabilities. [Law of total probability, Bayes' Rule.]

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Example

Probability that a student at the University of Saarbrücken studies computer science.

- e_0: human being is a student at the University of Saarbrücken.
- e_1: human being studies computer science.

OR

- e_0: student is a student at the University of Saarbrücken.
- e_1: student studies computer science.

Stochastic Independence

- Occurence of e_0 no impact on e_1.
- $\Pr[e_1|e_0] = \Pr[e_1] = \frac{\Pr[e_1 \cap e_0]}{\Pr[e_0]}$.
- e_0 and e_1 stochastically independent iff

$$\Pr[e_0 \cap e_1] = \Pr[e_0] \cdot \Pr[e_1] \ .$$

- $e_0, e_1, \ldots e_n$ stochastically independent iff

$$\Pr[e_0 \cap e_1 \cap \cdots \cap e_n] = \Pr[e_0] \cdot \Pr[e_1] \cdot \cdots \cdot \Pr[e_n] \ .$$

- *Mutual exclusive* events **not** stochastically independent.

Example

Pairwise independent but not independent.
Tossing two fair coins in a row.

- e_0: first coin head, $\Pr[e_0] = \frac{1}{2}$.
- e_1: second coin tail, $\Pr[e_1] = \frac{1}{2}$.
- e_2: both coins show same result, $\Pr[e_2] = \frac{1}{2}$.
- Pairwise independent.

$$\begin{aligned} \Pr[e_0 \cap e_1] &= \tfrac{1}{4} = \Pr[e_0] \cdot \Pr[e_1] \ , \\ \Pr[e_0 \cap e_2] &= \tfrac{1}{4} = \Pr[e_0] \cdot \Pr[e_2] \ , \\ \Pr[e_1 \cap e_2] &= \tfrac{1}{4} = \Pr[e_1] \cdot \Pr[e_2] \ . \end{aligned}$$

- Not independent.

$$\Pr[e_0 \cap e_1 \cap e_2] = 0 \neq \Pr[e_0] \cdot \Pr[e_1] \cdot \Pr[e_2] = \frac{1}{8} \ .$$

Motivation and Definition

- Sample space without numbers.
- Interessting outcome function on events.
- $X : \Omega \to \mathbb{R}$.
- Example: toin cossing.
  $\Pr[head] = p$, X number of tosses until head:
  $\Pr[X = n] = (1 - p)^{n-1} \cdot p$.

Discrete Random Variables

- Mapping to $\mathbb{N}$.
- Probability distribution function, cumulative density function: $\Pr[X \leq n] = F_X(n)$.
- Probability density function, probability mass function: $\Pr[X = n] = f_X(n)$.
- $F_X(n) = \sum_{i=0}^{n} f_X(i)$.
- $\sum_i f_X(i) = 1$.

Continuous Random Variables

- Mapping to $\mathbb{R}$.
- Probability of particular x is 0.
- Probability distribution function, cumulative density function: $F_X(x) = \Pr[X \leq x]$.
- If probability density function exists $f_X(x) = \frac{dF_X(x)}{dx}$.
- $F_X(x) = \int_{-\infty}^{x} f_x(u)du$.
- $\int_{-\infty}^{\infty} f_x(u)du = 1$.

Examples

Discrete random variables.

- Number of failures of a computer system per minute.
- Sum of outcomes of (two) dices.
- ...

Continuous random variables.

- Duration until two mobile devices get connected.
- Exact position of mobile devices.
- ...

Moments

- First moment called mean or expected value: μ, $E[X]$.

$$E[N] = \sum_{i=0}^{\infty} i \cdot f_N(i), E[X] = \int_{-\infty}^{\infty} x \cdot f_X(x)dx \ .$$

  - Rolling a die. $E[N] = 3.5$.
- kth moment, $(k = 1, 2, \dots)$:

$$E[N^k] = \sum_{i=0}^{\infty} i^k \cdot f_N(i), E[X^k] = \int_{-\infty}^{\infty} x^k \cdot f_X(x)dx \ .$$

Central Moments

- Second central moment called variance: σ_X^2, $\mathrm{var}[X]$.

$$E[(X - E[X])^2] \ .$$

  - Rolling a die. $\mathrm{var}[N] = 2,9167$.
- kth central moment, $(k = 1, 2, \dots)$:

$$E[(X - E[X])^k] \ .$$

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Multiple Random Variables

- Joint probability distribution function:
  $F_{X_1,X_2,\dots,X_n}(x_1, x_2, \dots, x_n) =$
  $\Pr[X_1 \leq x_1, X_2 \leq x_2, \dots, X_n \leq x_n]$.
- Joint probability density function:
  $f_{X_1,X_2,\dots,X_n}(x_1, x_2, \dots, x_n) =$
  $\Pr[X_1 = x_1, X_2 = x_2, \dots, X_n = x_n]$.
- Relation
  - $F_{X_1,X_2,\dots,X_n}(x_1, x_2, \dots, x_n) =$
    $\sum_{i_1 \leq x_1} \sum_{i_2 \leq x_2} \cdots \sum_{i_n \leq x_n} f_{X_1,X_2,\dots,X_n}(i_1, i_2, \dots, i_n)$.
  - $F_{X_1,X_2,\dots,X_n}(x_1, x_2, \dots, x_n) =$
    $\int_{-\infty}^{x_1} \int_{-\infty}^{x_2} \dots \int_{-\infty}^{x_n} f_{X_1,X_2,\dots,X_n}(i_1, i_2, \dots, i_n) di_1 di_2 \dots di_n$.

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Multiple Random Variables Cont'd

- Conditional probability density function:
  $f_{X_1|X_0}(x_1|x_0) = \frac{f_{X_1,X_0}(x_1,x_0)}{f_{X_0}(x_0)}$.
- Independence: $f_{X_1,X_0}(x_1, x_0) = f_{X_1}(x_1) \cdot f_{X_0}(x_0)$.
  - With marginal probability density

$$f_{X_0}(x_0) = \sum_{i=0}^{\infty} f_{X_1,X_0}(i, x_0) \ ,$$

$$f_{X_0}(x_0) = \int_{-\infty}^{\infty} f_{X_1,X_0}(i, x_0) di \ .$$

- Both apply to cumulative density function.

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Probability spaces and measures Conditional probabilities and Stochastic Independence Random Variables Distributions Problems

Convolution

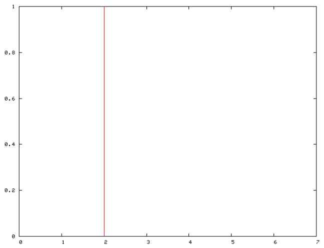
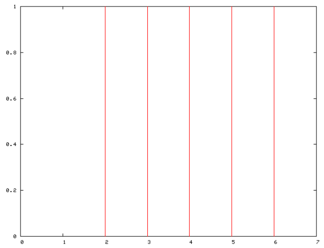
- Sum of two independent random variables determined by convolution.
- Probability density function:
  $f_{X_0+X_1}(z) = \sum_{u=0}^{\infty} f_{X_0}(u) \cdot f_{X_1}(z - u)$,
  $f_{X_0+X_1}(z) = \int_{-\infty}^{\infty} f_{X_0}(u) \cdot f_{X_1}(z - u) du$.
- Probability distribution function:
  $F_{X_0+X_1}(z) = \sum_{u=0}^{\infty} f_{X_0}(u) \cdot F_{X_1}(z - u)$,
  $F_{X_0+X_1}(z) = \int_{-\infty}^{\infty} f_{X_0}(u) \cdot F_{X_1}(z - u) du$.

Holger Hermanns, Sven Johr:
Ad-hoc Networking – Models and Methods

Finite Support

Degenerate distribution.

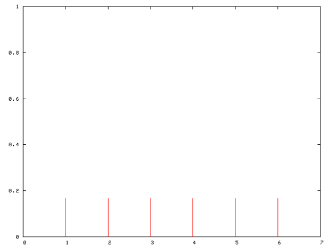
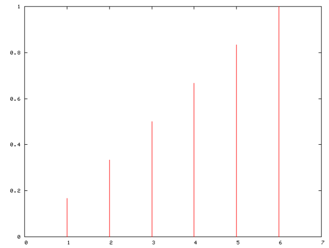
- X takes value x_0.
- $f_X(x) = 1$ iff $x = x_0$.

Finite Support Cont'd

Uniform distribution.

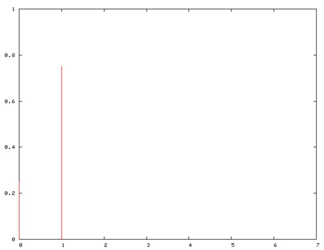
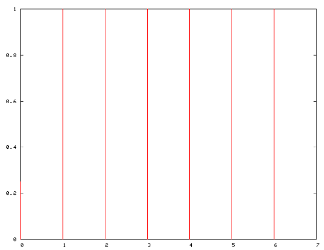
- Elements of finite set $S = \{x_1, x_2, \ldots, x_n\}$ are equally likely.
- $f_X(x_i) = \frac{1}{n}$.

Finite Support Cont'd

Bernoulli distribution.

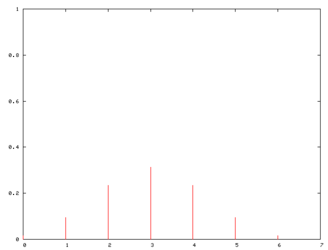
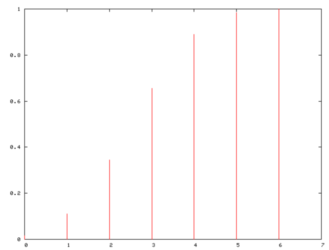
- Value 1 probability p, value 0 probability $1 - p$.
- $f_X(x) = \begin{cases} p & \text{if } x = 1, \\ 1 - p & \text{if } x = 0. \end{cases}$

Finite Support Cont'd

Binomial distribution.

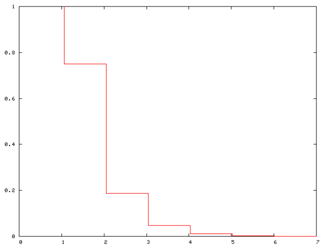
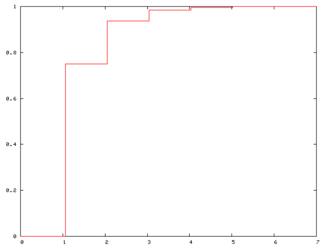
- Number of successes in n independent Bernoulli experiments.
- $f_X(k) = \binom{n}{k} p^k (1-p)^{n-k}$, $k = 0, 1, \ldots, n$.

Infinte Support

Geometric distribution.

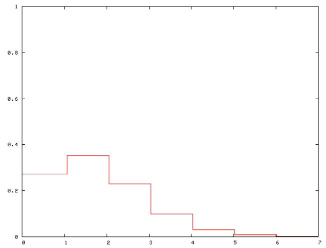
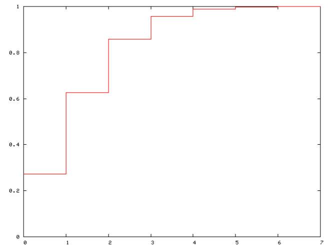
- Number of Bernoulli trials until one success.
- $f_X(n) = (1-p)^{n-1}p, n = 1, 2, \dots$.

Infinte Support Cont'd

Poisson distribution.

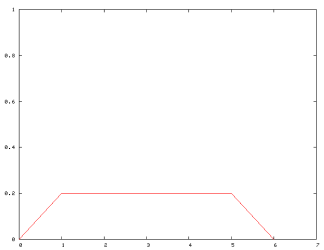
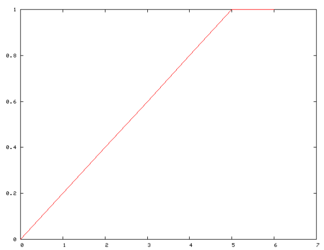
- Number of events occuring during time t.
- $f_X(k) = e^{-\lambda}\frac{\lambda^k}{k!}$.

(Semi) Finite Interval

Uniform distribution.

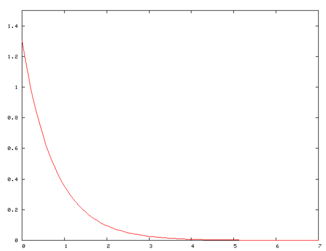
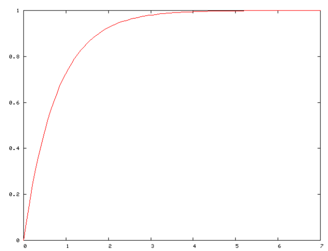
- $f_X(x) = \begin{cases} \frac{1}{b-a} & \text{for } a \leq x \leq b, \\ 0 & \text{otherwise.} \end{cases}$
- $F_X(x) = \begin{cases} 0 & \text{for } x < a, \\ \frac{x-a}{b-a} & \text{for } a \leq x < b, \\ 1 & \text{for } x \geq b. \end{cases}$

(Semi) Finite Interval Cont'd

Exponential distribution.

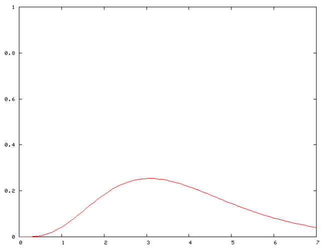
- Time between two consecutive events.
- $f_X(x) = \lambda e^{-\lambda x}$.
- $F_X(x) = 1 - e^{-\lambda x}$.

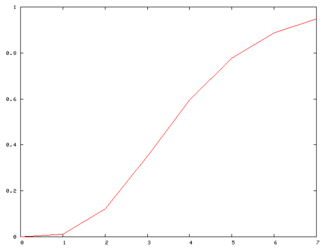



(Semi) Finite Interval Cont'd

Erlang-n distribution.

- Sum of n exponential distributions (independent, identical).
- $f_X(x) = \frac{\lambda(\lambda x)^{n-1} e^{-\lambda x}}{(n-1)!}$ for $x > 0$.
- $F_X(x) = 1 - e^{-\lambda x} \sum_{i=0}^{n-1} \frac{(\lambda x)^i}{i!}$ for $x > 0$.





(Semi) Finite Interval Cont'd

Hypoexponential distribution.

- Generalization of Erlang.
- Exponential variables with different parameters.

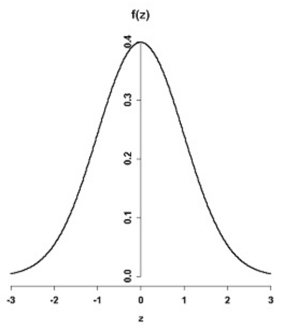
Hyperexponential distribution.

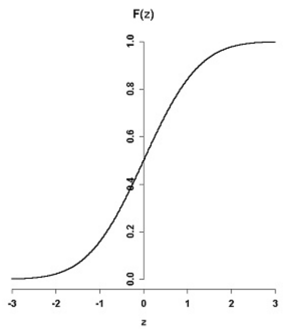
- Choice between two (or more) exponentially distributed variables.

Complete Reals

Normal distribution.

- $f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/2\sigma^2}$.
- Transformation to standard normal.





Insecure Connections

Suppose two mobile devices try to connected at a time.

- 2% of all connections are on average *insecure*.
- During a detection phase
  - with 94% probability an insecure connection is detected as insecure,
  - with 97% probability a secure connection is detected to be secure.
- Suppose a connection is detected to be insecure. What is the probability that this connection is indeed insecure?

Hint: Use Bayes' Rule: $\Pr[A_i|B] = \frac{\Pr[B|A_i]\Pr[A_i]}{\sum_j \Pr[B|A_j]\Pr[A_j]}$

σ-Algebra

- X is the set of natural numbers $\mathbb{N}$.
- $\mathcal{A}$ is a set of subsets of X containing set A iff
  - either A is finite,
  - or A^C is finite.
- Prove or disprove that $\mathcal{A}$ is a σ-algebra.