# Security models

## Lecture Notes 1

Date: 24.09.2009

### Contents

1. **Introduction**  
   - 1.1 Motivation ........................................ 2  
   - 1.2 Traditionnal security properties .......................... 2  
   - 1.3 Mechanisms for Authentication .............................. 3  
   - 1.4 Example ............................................ 3  
     - 1.4.1 Banking ........................................ 3  
     - 1.4.2 E-voting ........................................ 3  

2. **Probability theory: Basic definitions**  
   - 2.1 Probability distribution .................................. 4  
     - 2.1.1 Probability distribution properties ................. 4  
     - 2.1.2 DeMorgan’s law ................................... 5  
     - 2.1.3 Distributive law .................................. 5  
   - 2.2 Conditionnal distribution ................................ 6  
   - 2.3 Bayes’s theorem ...................................... 6  
   - 2.4 Random variables ...................................... 8  
     - 2.4.1 Independent random variables ........................ 8  
   - 2.5 Expectation .......................................... 9  
   - 2.6 Variance ........................................... 11  
   - 2.7 Theorems ........................................... 12  
     - 2.7.1 Markov’s inequality .................................. 12  
     - 2.7.2 Chebyshev’s inequality .............................. 13  
     - 2.7.3 Chernoff bound ................................... 14  

3. **Birthday Paradox**  
4. **Negligible fonction**  
5. **Noticeable function**
1 Introduction

1.1 Motivation

We need security in various field

- **Secure communication** via the Internet, telephone, email, fax.
  **Objectives** confidentiality and integrity of transmitted information.

- **Internet banking**
  **Objectives** confidentiality of transactions and account information, prevention of false transactions, impossibility of repudiating (denying) a transaction by a user . . .

- **E-voting systems**
  **Objectives** System availability during the vote, vote’s integrity, voting information privacy, only registered voters can vote and only once.

- **Digital payment systems** . . .

1.2 Traditionnal security properties

Common security properties are

- **Confidentiality or Secrecy** No improper disclosure of information

- **Authentication** To be sure to talk with the right person. Disclosure of information

- **Integrity** No improper modification of information

- **Availability** No improper impairment of functionality/services, access to important information should be available at any time.

Further security properties may be

- **Non-repudiation or accountability** is where one can establish responsibility for actions

- **Fairness** is the fact there is no advantage to play one role in a protocol comparing with the other ones

- **Privacy**
  - Anonymity: secrecy of principal identities or communication relationships
  - Pseudonymity: anonymity plus link-ability
  - Data protection personal data is only used in certain ways
1.3 Mechanisms for Authentication

They are many mechanisms for authentication, the most used are

- Something that you know: eg. a PIN or a password
- Something that you have: eg. a smart-card
- Something that you are: eg. biometric characteristics like voice, eyes, fingerprints . . .
- Location: eg. in a secure building

Strong authentication combines multiple factors, indeed you can use both smart-card and biometric authentication . . .

1.4 Example

1.4.1 Banking

A bank may require

- Authenticity of clients (thanks to the card, the code etc.)
- Non-repudiation of transactions
- Integrity of accounts and other customer data
- Secrecy of customer data (address, tel . . . )
- Availability of logging.

The conjunction of these properties might constitute the bank’s (high-level) security policy.

1.4.2 E-voting

An e-voting system should ensure that

- Only registered voters can vote and only once
- Integrity of votes
- Privacy of voting information (only used for tallying), and availability of system during the vote
In practice, many policy aspects are difficult to formulate precisely.

**Exercice 1** give the security properties that in international airport should guarantee.

# 2 Probability theory: Basic definitions

## 2.1 Probability distribution

A **finite probability distribution** \( D = (P, U) \) is a finite and non-empty set \( U \), together with a function \( P \) that map \( u \in U \) to \( P[u] \in [0, 1] \) such that

\[
\sum_{u \in U} P[u] = 1
\]

The set \( U \) is called the **sample space** and the function \( P \) is called the **probability function**

**Example : Rolling a dice**

If we think of rolling a fair die, then \( U := 1, 2, 3, 4, 5, 6 \) and \( P[u] := \frac{1}{6} \) for all \( u \in U \) gives a probability distribution describing the possible outcomes of the experiment.

### 2.1.1 Probability distribution properties

An **event** is a subset \( A \) of \( U \) and the probability if \( A \) is

\[
P[A] = \sum_{u \in A} P[u]
\]

**Properties**

- For an event \( A \subseteq U \) let \( \bar{A} \) denote the **complement** of \( A \) in \( U \).
  
  \[
P[\emptyset] = 0
  
P[U] = 1
  
P[\bar{A}] = 1 - P[A]
  \]

- For any event \( (A, B) \subseteq U^2 \) if \( A \subseteq B \) then \( P[A] \leq P[B] \)

- For any events \( (A, B) \subseteq U^2 \) we also have
  
  \[
P[A \cup B] = P[A] + P[B] - P[A \cap B]
  \]
  
  \[
P[A \cup B] \leq P[A] + P[B]
  \]

In particular, if \( A \) and \( B \) are disjoint then

\[
P[A \cup B] = P[A] + P[B]
\]
More generally, for any events \((A_1, ..., A_n) \subseteq U^n\) we have

\[
P\left[ \bigcup_{i \in [1,n]} A_i \right] \leq \sum_{i \in [1,n]} P[A_i]
\]

And if the \(A_i\) are disjoint then

\[
P\left[ \bigcup_{i \in [1,n]} A_i \right] = \sum_{i \in [1,n]} P[A_i]
\]

2.1.2 DeMorgan’s law

Let \(A\) and \(B\) two events, then we have

- \(\overline{A \cup B} = \overline{A} \cap \overline{B}\)
- \(\overline{A \cap B} = \overline{A} \cup \overline{B}\)

**Proof**

1. Let \(x \in \overline{A \cup B}\)
   
   \(x \in \overline{A \cup B} \iff x \notin A \cup B\)
   \(\iff x \notin A \text{ and } x \notin B\)
   \(\iff x \in \overline{A} \text{ and } x \in \overline{B}\)
   \(\iff x \in \overline{A} \cap \overline{B}\)

2. Let’s use the first relation with \(\overline{A}\) and \(\overline{B}\). We have \(\overline{A \cup B} = A \cap B\)
   
   Thus \(A \cup B = \overline{\overline{A} \cap \overline{B}}\)
   
   So \(\overline{A \cup B} = \overline{A} \cap \overline{B}\)

2.1.3 Distributive law

Let \(A, B\) and \(C\) three events, then we have

- \(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\)
- \(A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\)

**Proof**

- \(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\)
  
  \(x \in A \cap (B \cup C)\)
  \(\iff x \in A \text{ and } (x \in B \text{ or } x \in C)\)
  \(\iff (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\)
  \(\iff x \in (A \cap B) \cup (A \cap C)\)

- \(A \cup (B \cap C) = (A \cup B) \cap (A \cup C)\)
  
  \(x \in A \cup (B \cap C)\)
  \(\iff x \in A \text{ or } (x \in B \text{ and } x \in C)\)
  \(\iff (x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C)\)
  \(\iff x \in (A \cup B) \cap (A \cup C)\)
2.2 Conditionnal distribution

Let \( D = (U, P) \) be a probability distribution. For any event \( B \subseteq U \) with \( P[B] \neq 0 \) and any \( u \in U \) let us define

\[
P[u \mid B] := \begin{cases} 
P[u] & \text{if } u \in B \\ 0 & \text{otherwise} \end{cases}
\]

For any event \( A \subseteq U \), the **conditional probability** of \( A \) given \( B \) is defined by

\[
P[A \mid B] = \sum_{u \in A} P[u \mid B] = \frac{P[A \cap B]}{P[B]}
\]

2.3 Bayes’s theorem

Suppose we have a collection \( B_1, ..., B_n \) of \( n \) events that partitions \( U \) (i.e. \( \bigcup_{i=1}^{n} B_i = U \)), such that each event \( B_i \) occurs with non-zero probability. The \( B_1, ..., B_n \) verify

\[
\bigcup_{i=1}^{n} B_i = U \quad \text{and} \quad \forall i \neq j, B_i \cap B_j = \emptyset
\]

It is easy to see that for any event \( A \)

\[
P[A] = \sum_{i=1}^{n} P[A \cap B_i] = \sum_{i=1}^{n} P[A \mid B_i] P[B_i]
\]

Furthermore, if \( P[A] \neq 0 \) then for any \( j \in [1, n] \) we have

\[
P[B_j \mid A] = \frac{P[A \cap B_j]}{P[A]} = \frac{P[A \mid B_j] P[B_j]}{\sum_{i=1}^{n} P[A \mid B_i] P[B_i]}
\]

This equality, known as **Bayes’ theorem** lets us compute the conditional probability \( P[B_j \mid A] \) in terms of the conditional probabilities \( P[A \mid B_i] \).

**Proof**

Suppose \( A \) is an event and \( B_1, ..., B_n \) is a partition of \( U \).
For all \( A \subseteq U \) we have \( A = A \cap U \), or \( U = \bigcup_{i=1}^{n} B_i \) so \( A = A \cap (\bigcup_{i=1}^{n} B_i) \).

\[
A = \bigcup_{i=1}^{n} (A \cap B_i)
\]

As \( \forall i \neq j B_i \cap B_j = \emptyset \)
we have \( \forall i \neq j (A \cap B_i) \cap (A \cap B_j) = \emptyset \) (the two events are incompatible).
So

\[
P[A] = P[\bigcup_{i=1}^{n} (A \cap B_i)] = \sum_{i=1}^{n} P[A \cap B_i] = \sum_{i=1}^{n} P[A \mid B_i] P[B_i]
\]

And

\[
P[B_j \mid A] = \frac{P[A \cap B_j]}{P[A]} = \frac{P[A \mid B_j] P[B_j]}{\sum_{i=1}^{n} P[A \mid B_i] P[B_i]} = \frac{\sum_{i=1}^{n} P[A \mid B_i] P[B_i]}{\sum_{i=1}^{n} P[A \mid B_i] P[B_i]}
\]

6
Fred picks a bowl at random, and then picks a cookie at random.

- The cookie turns out to be a plain one. How probable is it that Fred picked it out of bowl 1?
- What is the probability that Fred picked bowl 1, given that he has a plain cookie?

Solution

<table>
<thead>
<tr>
<th></th>
<th>Bowl 1</th>
<th>Bowl 2</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chocolate chips</td>
<td>1/8</td>
<td>1/4</td>
<td>3/8</td>
</tr>
<tr>
<td>Plain</td>
<td>3/8</td>
<td>1/4</td>
<td>5/8</td>
</tr>
<tr>
<td>Total</td>
<td>1/2</td>
<td>1/2</td>
<td>1</td>
</tr>
</tbody>
</table>

Relative frequency of cookies in each bowl by type of cookie

→ Let $P(A)$ be the probability that Fred picked bowl 1 regardless of any other information. Hence $P(A) = 1/2$.

→ Let $P(B)$ be the probability of getting a plain cookie regardless of any information on the bowls. $P(B) = (0.75 + 0.5)0.5 = 0.625$ or $P(B) = 50/80 = 0.625$.

- $P(B|A)$ = the probability of getting a plain cookie given that Fred has selected bowl 1. $P(B|A) = 30/40 = 0.75$

Given all this information, we can compute the probability of Fred having selected bowl 1 given that he got a plain cookie, as such: $P(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{0.75 \times 0.5}{0.625} = 0.6$. As we expected, it is more than half.

Exercice 2 The drug test

Suppose a certain drug test is 99% accurate, the test will correctly identify a drug user as testing positive 99% of the time and will correctly identify a non-user as testing negative 99% of the time. Let’s assume a corporation decides to test its employees for opium use and 0.5% of the employees are drug users. We want to know the probability that given a positive drug test an employee is actually a drug user.
Solution

Let A the event ”An employee is a drug user”.  
Let B the event ”The test is positif”.  
We want to know \(P(A|B)\). 

\[
P(A|B) = \frac{P(A \cap B)}{P(B)}
\]

\[
= \frac{P(B|A).P(A)}{P(B)}
\]

We know that \(P(B|A) = 0.99\) and \(P(A) = 0.005\) 
let’s calculate \(P(B)\) 

\[
P(B) = P(B|A).P(A) + P(B|\bar{A}).P(\bar{A})
\]

\[
\Rightarrow P(A|B) = \frac{P(B|A).P(A)}{P(B|A).P(A) + P(B|\bar{A}).P(\bar{A})}
\]

with \(P(B|\bar{A}) = 0.01\) and \(P(\bar{A}) = 0.995\) 

\[
\Rightarrow P(A|B) = \frac{0.99 \times 0.005}{0.99 \times 0.005 + 0.01 \times 0.995} \approx 33\%
\]

Thus the probability that given a positive drug test an employee is actually a drug user is about 33%.

2.4 Random variables

Let \(D = (U, P)\) be a probability distribution. A random variable \(X\) is a function from \(U\) into a set \(\chi\). 
If \(\chi\) is a subset of a real numbers then \(X\) is called a real random variable: \(X(U) = \{X(u) : u \in U\}\).

Properties

- If \(X : U \to \chi\) is a random variable, and \(f : \chi \to Y\) is a function, then \(f(X) := f \circ X\) is also a random variable.
- Let \(X : U \to X\) be a random variable. For \(x \in \chi\), we write ”\(X = x\)” as shorthand for the event \(\{u \in U : X(u) = x\}\).

2.4.1 Independent random variables

Definitions

- Two random variables \(X, Y\) defined on a probability distribution \(Z := (X, Y)\) is also a random variable whose distribution is called the joint distribution of \(X\) and \(Y\).
- Two random variables \(X, Y\) are independent if for all \(x\) in the image of \(X\) and all \(y\) in the image of \(Y\) the events \(X = x\) and \(Y = y\) are independent

\[
P[X = x \land Y = y] = P[X = x]P[Y = y]
\]

Equivalently, \(X\) and \(Y\) are independent if and only if their joint distribution is equal to the product of their individual distribution.

Exercice 3 Prove that \(X\) and \(Y\) are independant if and if for all values taken by \(X\) with non-zero probability the conditional distribution of \(Y\) given the event \(X = x\) is the same as the distribution of \(Y\).
Pairwise independent random variables

Let $X_1, ..., X_n$ be a collection of random variables and let $X_i$ be the image of $X_i$ for $i \in [1, n]$. We say that the $X_1, ..., X_n$ are **pairwise independent** if for all $(i, j) \in [1, n]^2$ with $i \neq j$ the variables $X_i$ and $X_j$ are independent.

Mutually independent random variables

We say that $X_1, ..., X_n$ are **mutually independent** if for all $x_1 = X_1, ..., x_n = X_n$ we have

$$P[X_1 = x_1 \land ... \land X_n = x_n] = \prod_{i=1}^{n} P[X_i = x_i]$$

More generally for $k \in [2, n]$ we say that $X_1, ..., X_n$ are $k$-wise independent if any $k$ of them are mutually independent.

Example

We toss three coins and set $X_i := 0$ if the $i^{th}$ coin is "tails" and $X_i := 1$ otherwise. Show that the variables $X_1, X_2, X_3$ are mutually independent.

Let us set $Y_{12} := X_1 \oplus X_2$, $Y_{13} := X_1 \oplus X_3$ and $Y_{23} := X_2 \oplus X_3$ where "$\oplus$" denotes "exclusive or" that is addition modulo 2.

Show that the variables $Y_{12}, Y_{13}, Y_{23}$ are pairwise independent but not mutually independent.

2.5 Expectation

Let $D = (U, P)$ be a probability distribution. If $X$ is a real random variable then its **expected value** is

$$E[X] := \sum_{u \in U} X(u)P[u]$$

Properties

- If $\chi$ is the image of $X$, we have

$$E[X] = \sum_{x \in \chi} \sum_{u \in X^{-1}(x)} xP[u] = \sum_{x \in \chi} xP[X = x]$$

- More generally

$$E[f(X)] = \sum_{x \in \chi} f(x)P[X = x]$$

- If $X$ is equal to a constant $c$ (i.e. $\forall u \in U \ X(u) = c$) then $E[X] = E[c] = c$.

- If $X$ takes only non-negative values (i.e. $\forall u \in U \ X(u) \geq 0$) then $E[X] \geq 0$. Similarly, if $X$ takes only positive values then $E[X] > 0$.
Example

Let $X$ be uniformly distributed over $1, \ldots, n$.

$$E[X] = \sum_{x=1}^{n} \frac{x}{n} = \frac{n(n+1)}{2} \frac{1}{n} = \frac{n+1}{2}$$

Let $X$ denote the value of a die toss. Let $A$ be the event that $X$ is even. $X$ is uniformly distributed over 2, 4, 6 and hence

$$E[X|A] = \frac{2 + 4 + 6}{3} = 4$$

Similarly, in the conditional probability space given $A$, we see that $X$ is uniformly distributed over 1, 3, 5 and hence

$$E[X|\overline{A}] = \frac{1 + 3 + 5}{3} = 3$$

Hence

$$E[X] = E[X|A]P[A] + E[X|\overline{A}]P[\overline{A}] = \frac{4}{2} \cdot \frac{1}{2} + \frac{3}{2} \cdot \frac{1}{2} = \frac{7}{2}$$

Linearity of expectation

For real random variables $X$ and $Y$ and a real number $a$, we have

$$E[X + Y] = E[X] + E[Y]$$

$$E[aX] = aE[X]$$

If $X$ and $Y$ are independent real random variables then

$$E[XY] = E[X]E[Y]$$
Proofs

Let \( a \in \mathbb{R} \), \( \Omega_X = \{x_1, x_2, \ldots\} \), \( \Omega_Y = \{y_1, y_2, \ldots\} \) and \( \Phi(x, y) = x + y \).

- \( E[X + Y] = E[\Phi(X, Y)] = \sum_i \sum_j (x_i + y_j) P(X = x_i, Y = y_j) \)
  \[= \sum_i \sum_j x_i P(X = x_i, Y = y_j) + \sum_i \sum_j y_j P(X = x_i, Y = y_j)\]
  \[= \sum_i x_i \sum_j P(X = x_i, Y = y_j) + \sum_j y_j \sum_i P(X = x_i, Y = y_j)\]
  because both sums exist, they are finite.

- \( E[aX] = \sum_j ax_j P(x_j) \)
  \[= a \sum_j x_j P(X = x_j) = aE[X] \]

- Let suppose now that \( X \) and \( Y \) are independent random variables.

  \( E[XY] = \sum_i \sum_j x_i y_j P(X = x_i, Y = y_j) \)
  \[= \sum_i x_i \sum_j y_j P(X = x_i, Y = y_j) \]
  \[= \sum_i x_i P(X = x_i) \sum_j y_j P(Y = y_j) = E[X]E[Y] \]

2.6 Variance

The variance of a real random variable \( X \) is

\[
Var[X] := E[(X - E[X])^2]
\]

It is a measure of the spread or dispersion of the distribution of \( X \) around its expected value \( E[X] \). Variance is always non-negative.

Properties

Let \( X \) be a real random variable and let \( a \) and \( b \) be real numbers. Then we have

- \( Var[X] = E[X^2] - (E[X])^2 \)
- \( Var[aX] = a^2 Var[X] \)
- \( Var[X + b] = Var[X] \)
Proofs

  indeed \( E[aX] = aE[X] \) and the expectation is linear.
  So \( \text{Var}(X) = E[X^2] - E[X]^2 \).
- Let \( a \in \mathbb{R} \).
  \( \text{Var}(aX) = E[a^2X^2] - E[aX]^2 = a^2(E[X^2] - E[X]^2) = a^2 \text{Var}(X) \)
- Let \( b \in \mathbb{R} \).
  \( \text{Var}(X + b) = E[(X + b - E[X + b])^2] = E[(X - E[X])^2] = \text{Var}(X) \)

Examples

Let \( X \) be uniformly distributed over \( 1, \ldots, n \).

\[
E[X] = \sum_{x=1}^{n} x \cdot \frac{1}{n} = \frac{n(n+1)}{2} \cdot \frac{1}{n} = \frac{n+1}{2}
\]

We also have

\[
E[X^2] = \sum_{x=1}^{n} x^2 \cdot \frac{1}{n} = \frac{n(n+1)(2n+1)}{6} \cdot \frac{1}{n} = \frac{(n+1)(2n+1)}{6}
\]

Therefore

\[
\text{Var}(X) = E[X^2] - (E[X])^2 = \frac{n^2 - 1}{12}
\]

2.7 Theorems

2.7.1 Markov’s inequality

Let \( X \) be a random variable that takes only non-negative real values. Then for any \( t > 0 \), we have

\[
P[X \geq t] \leq \frac{E[X]}{t}
\]
Proof

Let $f$ be the density of $X$. We have

$$E[X] \geq 0 = \int_0^t xf(x)dx + \int_t^{\infty} xf(x)dx$$

The function for any $x \in \mathbb{R}^+$, $xf(x) \geq 0$. And since $t \geq 0$ we have

$$\int_0^t xf(x)dx \geq 0$$

Thus we obtain

$$E[X] \geq \int_t^{\infty} xf(x)dx$$

For any $x \in [t, \infty]$, we obviously have $x \geq t$ and so

$$xf(x) \geq tf(x)$$

$$\int_t^{\infty} xf(x)dx \geq \int_t^{\infty} tf(x)dx$$

$$\int_t^{\infty} xf(x)dx \geq t \int_t^{\infty} f(x)dx$$

$$E[X] \geq tP[X \geq t]$$

$$\frac{E[X]}{t} \geq P[X \geq t]$$

2.7.2 Chebyshev’s inequality

Let $X$ be a real random variable. Then for any $t > 0$, we have:

$$P(\|X - E[X]\| \geq t) \leq \frac{Var[X]}{t^2}$$

Proof

in any $\lambda > 0$ we obtain

$$P(\|X \geq \lambda\|) \leq \frac{E[Y]}{\lambda}$$

$$P(\|X - E[X]\| \geq \sqrt{\lambda}) \leq \frac{E[(X - E[X])^2]}{\lambda}$$

Let $t$ such as $t = \sqrt{\lambda}$ to obtain

$$P(\|X - E[X]\| \geq t) \leq \frac{V[X]}{t^2}$$
2.7.3 Chernoff bound

Let $X_1, \ldots, X_n$ be mutually independent random variables, such that each $X_i$ is 1 with probability $p$ and 0 with probability $q := 1 - p$. Assume that $0 < p < 1$. Also, let $X$ be the sample mean of $X_1, \ldots, X_n$. We have $X = \sum_i X_i$ and $ar{X} = \frac{1}{n}X$.

Then for any $\varepsilon > 0$, we have:

- For any $\varepsilon > 0$

  $$P[\bar{X} - p \geq \varepsilon] \leq \left(\frac{e^{\varepsilon/p}}{(1 + \varepsilon/p)^{1+\varepsilon/p}}\right)^{np}$$

  For $0 < \varepsilon \leq 1$

  $$P[\bar{X} - p \geq \varepsilon] \leq \exp(-\frac{n\varepsilon^2}{3p})$$

- For any $\varepsilon > 0$

  $$P[\bar{X} - p \leq -\varepsilon] \leq \left(\frac{e^{-\varepsilon/p}}{(1 - \varepsilon/p)^{1-\varepsilon/p}}\right)^{np}$$

  For $0 < \varepsilon \leq 1$

  $$P[\bar{X} - p \leq -\varepsilon] \leq \exp(-\frac{n\varepsilon^2}{2p})$$

- For $0 < \varepsilon \leq 1$

  $$P[|\bar{X} - p| \geq \varepsilon] \leq 2\exp(-\frac{n\varepsilon^2}{3p})$$
Proofs

We want to prove for any $\varepsilon > 0$

$$P[\bar{X} - p \geq \varepsilon] \leq \left(\frac{e^{\varepsilon/p}}{(1 + \varepsilon/p)^{1+\varepsilon/p}}\right)^{np}$$

We have $X_1, \ldots, X_n$ which are mutually random variables.

$P(X_i = 1) = \mu$ and $P(X_i = 0) = \bar{\mu}$, $X = \sum_i X_i$ and $\bar{X} = \frac{1}{n}X$.

Let $t > 0$. $A = P(e^{tX} \geq e^{\mu(1+\delta)})$. Now we can use Markov’s inequality.

$$A \leq \frac{E[e^{tX}]}{e^{t(1+\delta)}}$$

We take $\ln t > 0 \{e^{t} - 1 - t(1+\delta)\}$, so $t = \ln(1+\delta)$

So

$$P[\bar{X} - p \geq \varepsilon] \leq \left(\frac{e^{\varepsilon/p}}{(1 + \varepsilon/p)^{1+\varepsilon/p}}\right)^{np}$$

Furthermore for $0 < \varepsilon \leq 1$ we can prove that

$$\frac{e^{\varepsilon/p}}{(1+\varepsilon/p)^{1+\varepsilon/p}} \leq e^{\exp(-\frac{\delta}{3})}$$

(by derivating a function and study its sign)

So

$$0 < \varepsilon \leq 1, P[\bar{X} - p \geq \varepsilon] \leq \exp(-\frac{n\varepsilon^2}{3p})$$

A similar proof strategy can be used to show the two others inequality.

3 Birthday Paradox

We search to know, how many people must be in a room such that the probability $p$ that one has your birthday is $p > 0.5$.

If we have $n$ people, $p(n) = 1 - \left(\frac{365-1}{365}\right)^n$.

We want to find $n$ such that $p(n) > 0.5$.

$$1 - \left(\frac{365-1}{365}\right)^n > 0.5$$
\[ n \ln \left( \frac{365 - 1}{365} \right) \geq \ln \left( \frac{1}{2} \right) \]
\[ n \geq \frac{\ln \frac{1}{2}}{\ln \frac{365 - 1}{365}} \simeq 253 \]

As stated above, the probability that no two birthdays coincide is:

\[ p(n) = \prod_{k=1}^{n-1} \left( 1 - \frac{k}{365} \right) \]

By convexity \( \forall x \in \mathbb{R}, 1 - X < e^{-X} \) it’s the tangent in 0.

\[ \bar{p}(n) < \prod_{k} e^{-\frac{k}{365}} = e^{-\frac{n(n+1)}{2 \cdot 365}} \]

We want \( p(n) < 0.5 \) so

\[ n^2 - n > 2.365 \cdot \ln 2 \]

We concluded that \( n \) need to be greater or equal to 23.

**Generalisation**

The setting is that we have \( q \) balls. View them as numbered, 1, \ldots, \( q \). We also have \( N \) bins, where \( N \geq q \). We throw the balls at random into the bins, one by one, beginning with ball 1. At random means that each ball is equally likely to land in any of the \( N \) bins, and the probabilities for all the balls are independent. A collision is said to occur if some bin ends up containing at least two balls. We are interested in \( C(N, q) \), the probability of a collision. The birthday paradox is the case where \( N = 365 \). We are asking what is the chance that, in a group of \( q \) people, there are two people with the same birthday, assuming birthdays are randomly and independently distributed over the days of the year.

First, we need to prove the two inequality:

\[ X - \frac{X}{e} \leq 1 - e^{-X} \leq X \]

By convexity \( \forall X \in \mathbb{R}, 1 - e^{-X} < X \), it’s the tangent in 0.

Let \( g(X) = 1 - e^{-X} - X(1 - e^{-1}) \)

We have \( g'(X) = e^{-X} - 1 + e^{-1} > 0, \forall X \in \mathbb{R}^+ \)

Or \( g(0) = 0 \) and \( \forall X \in \mathbb{R}^+, g'(X) > 0 \) meaning \( g \) is an increasing function, thus \( X - \frac{X}{e} \leq 1 - e^{-X} \).

We want to estimate the probability \( C(N, q) \)

\[ C(N, q) = 1 - A_q^N = 1 - \left( 1 - \frac{1}{N} \right) \cdot \left( 1 - \frac{2}{N} \right) \cdot \left( 1 - \frac{q-1}{N} \right) \]

But \( 1 - x < e^{-x} \), so

\[ C(N, q) > 1 - \prod_{i=1}^{q-1} e^{-\frac{i}{N}} = 1 - e^{-\frac{q(q-1)}{2N}} \]

We search \( q \) such that \( C(N, q) \geq 0.5 \).

\[ q(q - 1) = 2N\ln(0.5) \]

Since \( q \) is positive, \( q = \frac{1}{2} + \sqrt{N} \cdot \sqrt{\frac{1}{4N} - 2\ln(0.5)} \) So \( q \simeq 1.18\sqrt{N} \)

In the birthday case, we have \( N = 365 \) so \( q \simeq 1.18\sqrt{365} \simeq 23 \)
4 Negligible function

We call a function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ negligible if for every positive polynomial $p$ there exists an $N$ such that for all $n > N$

$$\forall n > N; \mu(n) < \frac{1}{p(n)}$$

Properties

Let $f$ and $g$ be two negligible functions then

- $f \cdot g$ is negligible
- For any $k > 0$, $f^k$ is negligible
- For any $(\lambda, \mu) \in \mathbb{R}^2$, $\lambda f + \mu g$ is negligible

Proofs

- Let be $p$ a positive polynome.
  We can find $q$ a positive polynome such as $\forall n \ q^q(n) \geq p(n)$ for example $\forall n \ q(n) = \sqrt{p(n)}$
  $f$ is negligible so $\exists N_1 \ \forall n > N_1, \ f(n) < \frac{1}{q(n)}$
  $g$ is negligible so $\exists N_2 \ \forall n > N_2, \ g(n) < \frac{1}{q(n)}$
  Let $N = \max(N_1, N_2)$ then we have $\forall n > N, \ f(n)g(n) < \frac{1}{q^2(n)}$
  So $\forall n > N, \ f(n)g(n) < \frac{1}{p(n)}$.

- Let be $p$ a positive polynome and $k$ a positive integer.
  We can find $q$ a positive polynome such as $\forall n \ q^k(n) \geq p(n)$ for example $\forall n \ q(n) = p^{\frac{1}{k}}(n)$
  $f$ is negligible so $\exists N \ \forall n > N, \ f(n) < \frac{1}{q(n)}$
  Thus $\exists N \ \forall n > N, \ f^k(n) < \frac{1}{q^k(n)}$ So $\exists N \ \forall n > N, \ f^k(n) < \frac{1}{p(n)}$

- Let be $p$ a positive polynome, $\lambda, \mu$ two positive real numbers and $f,g$ two negligible functions.
  First we proved that $\lambda f$ is a negligible function.
  Let be $q$ a positive polynome such as $q = \lambda p$.
  $f$ is negligible so $\exists N \ \forall n > N, \ f(n) < \frac{1}{q(n)}$ So $\exists N \ \forall n > N, \ \lambda f(n) < \frac{1}{p(n)}$ ie $\lambda f$ is a negligible function.
  Now we can prove that $(\lambda, \mu) \in \mathbb{R}^2, \ \lambda f + \mu g$ is negligible.
  Let be $q$ a positive polynome such as $q = 2p$.
  $f$ is negligible so $\exists N_1 \ \forall n > N_1, \ \lambda f(n) < \frac{1}{q(n)}$
  $g$ is negligible so $\exists N_2 \ \forall n > N_2, \ \mu g(n) < \frac{1}{q(n)}$
  Let $N = \max(N_1, N_2)$ then we have $\forall n > N, \ \lambda f(n) + \mu g(n) < \frac{2}{q(n)}$
  So $\exists N \ \forall n > N, \ \lambda f(n) + \mu g(n) < \frac{1}{p(n)}$

Exercice 4 Prove or disprove if the following functions are negligible

- $f(n) := (\frac{1}{2})^n$
- $f(n) := 2^{-\sqrt{n}}$
- $f(n) := n^{-n \ln n}$
5 Noticeable function

Instead of “there exists an N such as for all \( n > N \) ” we will in the following often say “for all sufficiently large \( n \)”. We call a function \( f : \mathbb{N} \to \mathbb{R}^+ \) noticeable if there exists a positive polynomial \( p \) such as for all sufficiently large \( n \) we have

\[
f(n) > \frac{1}{p(n)}
\]

Note: A function can be neither noticeable nor negligible.

Exercise 5 Prove or disprove the following statements

- If both \( f, g \geq 0 \) are noticeable then \( f - g \) and \( f + g \) are noticeable
- If both \( f, g \geq 0 \) are not noticeable then \( f - g \) is not noticeable
- If both \( f, g \geq 0 \) are not noticeable then \( f + g \) is not noticeable
- If \( f \geq 0 \) is noticeable and \( g \geq 0 \) is negligible then \( f \cdot g \) is negligible
- If both \( f, g > 0 \) are negligible then \( \frac{f}{g} \) is noticeable