Part 1: Elements of Probability Calculus

Mieke Massink
CNR-ISTI, Via Moruzzi 1, Pisa

Probabilistic Model Checking AA. 2020-2021

Elements of Probability Calculus

Def: Random Experiment ($\mathcal{C}$)

Every experiment that can manifest itself in a number of different alternatives or elementary events

For example:
- Throwing a dice, or two dices etc.
- Taking an exam...

result = elementary event = alternative = elementary random event

Elements of Probability Calculus

Def: Sampling Space ($\Omega$) of $\mathcal{C}$ or fundamental space

Set of all elementary events of $\mathcal{C}$ where $\omega \in \Omega$. 
Elements of Probability Calculus

Def: Sampling Space (Ω) of C or fundamental space

Set of all elementary events of C where ω ∈ Ω.

For example:
- the six faces of a dice
- passing or failing the exam

Observation:

E contains subsets of Ω

E ⊆ 2Ω

Question:

E ⊆ 2Ω?
Imagine $\Omega$ infinite and non-denumerable. The elements $\Omega = \{0, \ldots, 9\}^\omega$.

For example:

\[
\Omega = \{0, \ldots, 9\}^\omega
\]

This could be interpreted as an infinite series of throwing a dice with 10 faces (these represent all real numbers in $[0, 1)$).

Every single series is infinite.

The probability that a certain series $\sigma$ occurs is:

\[
Prob(\sigma) = \frac{1}{10} \cdot \frac{1}{10} \cdot \frac{1}{10} \cdot \cdots \lim_{n \to \infty} \left(\frac{1}{10}\right)^n = 0
\]

But:

\[
Prob(\Omega) = 1
\]

There does not exist an analytic tool of measurement that is valid for all elements of the powerset of any given set, outside the class of finite sets or denumerable sets.

But do we need a probability measure on infinite or non-denumerable sets?

Elements of Probability Calculus

Model-checking

Models based on transition systems, for example:

- pa: processor available
- ps: process suspended
- rse: external service request
- fse: end external service

Let’s call ‘Ready’ state 1 (initial state), ‘Run’ state 2 and ‘Wait’ state 3.

(Example taken from operating systems)

A typical model-checking example (CTL): $\Box(tt \land wait)$?

“Always eventually reaching state ‘Wait’?”

Executions:

- $1, 2, 3, \{(1, 2), 3\}^\omega$
- $1, 2, 1, 2, 3, \{(1, 2), 3\}^\omega$
- $\vdots$
- $(1, 2)^\ast, 3, \{(1, 2), 3\}^\omega$

all (infinite sets of) infinite executions

Only the trace $(1, 2)^\omega$ does not satisfy the formula.
**Elements of Probability Calculus**

**Probabilistic Model-checking**

Consider: \( P \geq 0.5 (\text{tt} \cup \text{wait}) \)?

'With probability greater than or equal to 0.5 we end up in state Wait sooner or later?'

**Elements of Probability Calculus**

This means: the probability (measure) of an infinite set of infinite series. For example:

\[
P(1, 2, 3, (1, 2)^\omega) = 1 \times \frac{2}{3} \times 1 \times \frac{1}{3} \times 1 \times \frac{1}{3} \times \cdots
\]

\[
= \lim_{n \to \infty} (1 \times \frac{2}{3} \times (\frac{1}{3})^n)
\]

\[= 0\]

and so on, for every sequence that satisfies: \{\text{tt} \cup \text{wait}\}

But we also know that only one sequence \((1, 2)^\omega\) does not satisfy the formula. Therefore we also have that:

\[
P((1, 2)^\omega) = 0
\]

But:

\[
P(\Omega) = 1 \text{ and also } P(\{\text{tt} \cup \text{wait}\}) = 1 - P((1, 2)^\omega) = 1 - 0 = 1
\]

This clearly leads to a contradiction!

**Elements of Probability Calculus**

**Borel set**

Given any set, it is possible to construct an analytical instrument of measure that is valid for all elements of a Borel set

\( \mathcal{E} \) is restricted to the Borel set (or the \( \sigma \)-algebra of Borel) of \( \Omega \)
Elements of Probability Calculus

Construction of a Borel algebra

Def: $\sigma$-algebra

Given a Sample Space $\Omega$ (of $\mathcal{C}$)

$\mathcal{F} \subseteq 2^\Omega$ is a $\sigma$-algebra iff:

1. $\Omega \in \mathcal{F}$
2. $A \in \mathcal{F} \implies \overline{A} \in \mathcal{F}$
3. $\bigwedge_{i=1}^{\infty} A_i \in \mathcal{F} \implies \bigcup_{i=1}^{\infty} \in \mathcal{F}$

Elements of Probability Calculus

Terminology:

- The elements of a $\sigma$-algebra are called: measurable sets
- $(\Omega, \mathcal{F})$ is called measurable space

It is required that:

- $\mathcal{E}$ is a $\sigma$-algebra
- $A \in \mathcal{E} \implies A \subseteq \Omega$

Probability

Def $P$

Given a measurable space $(\Omega, \mathcal{F})$, a probability measure on this space is a function:

$$P : \mathcal{F} \to \mathbb{R}_{\geq 0} \text{s.t.}$$

1. $P(\emptyset) = 0$
2. $P(\Omega) = 1$
3. For every family $\{A_i | A_i \in \mathcal{F}, i \in \mathbb{N}\}$ with $k \neq h \implies A_k \cap A_h = \emptyset$ it holds that:

$$P\left(\bigcup_{i=0}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i)$$
Elements of Probability Calculus

Discrete probability measure

Given a probability space \((\Omega, \mathcal{F}, P)\), if there exists a denumerable set \(A \subseteq \Omega\) such that

\[
\sum_{a \in A} P\{a\} = 1
\]

then

- \(P\) is a discrete probability measure
- \((\Omega, \mathcal{F}, P)\) is a discrete probability space

Elements of Probability Calculus

Cylindersets

A path that starts in an initial state is an infinite sequence \(s_0, s_1, \ldots\) of states with \(s_0\) as initial state and with \(P(s_i, s_{i+1}) > 0\).

If \(\sigma\) is a path, \(\sigma \uparrow n\) is a finite prefix \(s_0, s_1, \ldots, s_n\) of \(\sigma\) and \(\sigma[i]\) is the element (state) \(s_i\) of the path \(\sigma\).

A cylinderset is defined as:

\[
\{\sigma \in \text{paths} | \sigma \uparrow n = s_0, s_1, \ldots, s_n\}
\]

A cylinderset

\[
\{\sigma \in \text{paths} | \sigma \uparrow n = s_0, s_1, \ldots, s_n\}
\]

Set of all sequences with the same prefix.

The cylindersets form a \(\sigma\)-algebra (Borel space) and therefore they can be used as the base for the definition of a probability measure.
Elements of Probability Calculus

Probability measure on sets of paths: \( P \)

- For any sequence \( s_0, \ldots, s_n \) that starts in \( s_0 \)
  \[
  P \{ \sigma \in \text{paths} | \sigma \uparrow n = s_0, \ldots, s_n \} = P(s_0, s_1) \cdot P(s_1, s_2) \cdot \cdots \cdot P(s_{n-1}, s_n)
  \]
  where \( P \) is the probability function for the transitions
- For \( n = 0 \)
  \[
  P \{ \sigma \in \text{paths} | \sigma \uparrow 0 = s_0 \} = 1
  \]

Elements of Probability Calculus

Properties of \( P \)

Given the probability space \( (\Omega, \mathcal{F}, P) \) the following holds:

- \( \forall A \in \mathcal{F} : P(A) + P(\bar{A}) = 1 \)
- \( \forall A, B \in \mathcal{F} : A \subseteq B \implies P(A) \leq P(B) \)
- \( \forall A \in \mathcal{F} : P(A) \leq P \mathbb{1} \)
- \( \forall A, B \in \mathcal{F} : P(A \cup B) \geq \max\{P(A), P(B)\} \)
- \( \forall A, B \in \mathcal{F} : P(A \cap B) \leq \min\{P(A), P(B)\} \)
- \( \forall A, B \in \mathcal{F} : P(A \cup B) = P(A) + P(B) - P(A \cap B) \)
- \( \forall A, B \in \mathcal{F} : A \subseteq B \implies P(B \setminus A) = P(B) - P(A) \)
- \( \forall A_i \in \mathcal{F} : P(\bigcup_{i=0}^{\infty} A_i) \leq \sum_{i=0}^{\infty} P(A_i) \)

where \( \bar{A} \) denotes the complement of \( A \).

Elements of Probability Calculus

Probabilistic Model Checking

Executions seen as cylindric sets:

- \( \{ \sigma | \sigma \uparrow 3 = 1, 2, 3 \} \quad 1 * 2/3 = 2/3 \)
- \( \{ \sigma | \sigma \uparrow 5 = 1, 2, 1, 2, 3 \} \quad 1 * 1/3 * 1 * 2/3 = 1/3 * 2/3 \)
- \( \{ \sigma | \sigma \uparrow 7 = 1, 2, 1, 2, 1, 2, 3 \} \quad \vdots \)
- \( \vdots \)
More generally we obtain:
\[ X = \bigcup_{n=1}^{\infty} \{ \sigma | \sigma \uparrow 2n + 1 = (1, 2)^n, 3 \} \]

And the probability of this set is:
\[ P(X) = \frac{2}{3} \sum_{n=1}^{\infty} \left( \frac{1}{3} \right)^n = 2/3 \left( \frac{1}{1-1/3} \right) = 2/3 \times 3/2 = 1 \]

Which is the probability that the system never passes by state 3.
Elements of Probability Calculus

Stochastically independent events

Given \((\Omega, \mathcal{F}, P)\) and \(A, B \in \mathcal{F}\) random events

Def.: \(A\) and \(B\) are stochastically independent iff.
\[
P(A \cap B) = P(A) \cdot P(B)
\]

Properties

Given \((\Omega, \mathcal{F}, P)\) and \(A, B \in \mathcal{F}\) independent random events

- \(\bar{A}, B\) are stochastically independent
- \(A, \bar{B}\) are stochastically independent
- \(\bar{A}, \bar{B}\) are stochastically independent
- \(P(A \cup B) = 1 - P(\bar{A} \cdot \bar{B})\)