AISEC Unit 2

Lecture "Machine Learning for Computer Security"
Prof. Dr. Christian Wressnegger
Artificial Intelligence & Security
Karlsruher Institute für Technologie (KIT)

1. **From Loss to Risk**
   (a) Define the "Expected risk" and the "Empirical risk"

   Solution:

   (b) What do we need the latter for?

   Solution:

2. **Kernel functions.** Kernel functions can be constructed by combining other kernels. Let us consider two kernels $k_a : X \times X \to \mathbb{R}$ and $k_b : X \times X \to \mathbb{R}$. Verify whether the following combinations yield valid kernel functions. Recall that a kernel needs to be symmetric and positive semi-definite.

   (a) $k_1(x, z) = k_a(x, z) + k_b(x, z)$
   (b) $k_2(x, z) = k_a(x, z) - k_b(x, z)$
   (c) $k_3(x, z) = k_a(z, z) + k_b(x, x)$

Solution:

3. **Kernalized distance.** Derive the kernalized version of the Euclidean distance between $\phi(x)$ and $\phi(z)$ with ϕ representing the implicit feature map.

Solution:

4. **Bag-of-Words.** Implement a *polynomial* bag-of-words kernel k for two strings x and z as follows

$$k(x, z) = \left(\sum_{w \in L} occ(w, x) \cdot occ(w, z) \right)^d .$$

where $occ(w, x)$ returns the number of occurrences of the word w in x. The language L is defined implicitly by splitting the strings using space and punctation characters.

Compute, (pretty) print and plot 4×4 kernel matrices for the following strings with $d \in \{1, 2, 3, 4\}$.

- `They call it a Royale with cheese.`
- `A Royale with cheese.  What do they call a Big Mac?`
- `Well, a Big Mac is a Big Mac, but they call it le Big-Mac.`
- `Le Big-Mac.  Ha ha ha ha.  What do they call a Whopper?`

Solution:

Bonus: Why is it called a Royale with cheese?