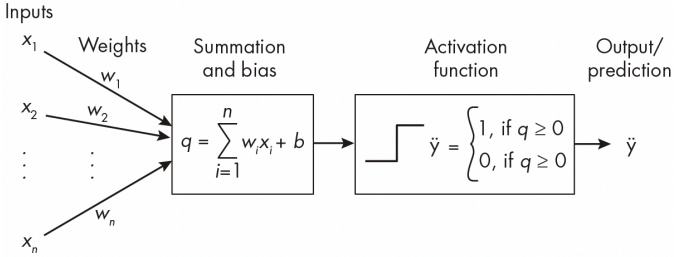
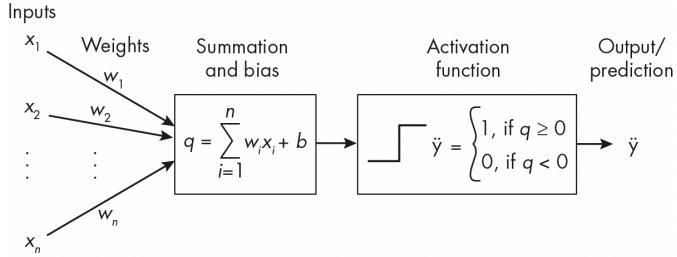


Practical AI Security

A Hands-on Guide to Attacking, Defending, and Securing Modern AI Systems

by Harriet Farlow

Errata updated to print 1

Page	Error	Correction	Print corrected
5	 <p>Inputs x_1, x_2, \dots, x_n are multiplied by weights w_1, w_2, \dots, w_n and summed with bias b to produce $q = \sum_{i=1}^n w_i x_i + b$. The activation function is a step function defined as $\hat{y} = \begin{cases} 1, & \text{if } q \geq 0 \\ 0, & \text{if } q \geq 0 \end{cases}$. The output is \hat{y}.</p> <p>Figure 1-2: The Perceptron</p>	 <p>Inputs x_1, x_2, \dots, x_n are multiplied by weights w_1, w_2, \dots, w_n and summed with bias b to produce $q = \sum_{i=1}^n w_i x_i + b$. The activation function is a step function defined as $\hat{y} = \begin{cases} 1, & \text{if } q \geq 0 \\ 0, & \text{if } q < 0 \end{cases}$. The output is \hat{y}.</p> <p>Figure 1-2: The Perceptron</p>	Pending