Statistics Part I

Cryptographic Hardware for Embedded Systems
ECE 3170

Fall 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

©Georgia Institute of Technology, 2018-2025

Gaussian (a.k.a. Normal) Distribution

- $f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-1}{2}(\frac{x-\mu}{\sigma})^2}$
- $\mu = E(X)$
- $\sigma^2 = Var(X) = E((X - E(X))^2)$
- $X \sim N(\mu, \sigma)$ means that X is normally distributed (has a Gaussian distribution) with mean value μ and standard deviation σ
- The “standard normal distribution” has μ = 0 and σ = 1

©Georgia Institute of Technology, 2018-2025

Expected Value

- $E(X)$ is just the arithmetic average of the possible values of X
- For example, consider nine measurements 111.9, 117.6, 123.2, 128.7, 134.0, 139.5, 145.1, 151.2 and 159.6 (all in mV)
- Assign random variable X to represent the power measured (recall we are assuming that the milliVolts measured across a one Ohm resistor is proportional to power = Watts = Joules per second = J/s)
- $E(X)$ = (111.9 + 117.6 + 123.2 + 128.7 + 134.0 + 139.5 + 145.1 + 151.2 + 159.6)/9 = 1210.8 / 9 = 134.5333
  - Note that the *median* value is 134
- Note that $E(X+Y)$ = $E(X) + E(Y)$
- If X and Y are independent, then $E(XY)$ = $E(X)E(Y)$

©Georgia Institute of Technology, 2018-2025

Empirical Equivalents

- We can estimate $\mu = E(X)$ with the average calculated empirically:
  - $\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$
- We can estimate $\sigma = \sqrt{Var(X)}$ with the square root of the variance also calculated empirically:
  - $s^2 = \frac{1}{n-1}\sum_{i=1}^{n}(x_i - \bar{x})^2$

©Georgia Institute of Technology, 2018-2025

Variance of a Sum

- $Var(X) = E((X - E(X))^2)$
- $Var(X + Y) = E((X + Y - E(X + Y))^2)$
- $= E(((X - E(X)) + (Y - E(Y)))^2)$
- $= E((X - E(X))^2 + 2(X - E(X))(Y - E(Y)) + (Y - E(Y))^2)$
- $= Var(X) + 2E((X - E(X))(Y - E(Y))) + Var(Y)$
- The middle term is defined to be the $Covariance$ of X and Y or $Cov(X, Y)$
  - $Cov(X, Y) = E((X - E(X))(Y - E(Y)))$
- $Cov(X, Y) = E((X - E(X))(Y - E(Y)))$
- $= E(XY - YE(X) - XE(Y) + E(X)E(Y))$
- $= E(XY) - E(Y)E(X) - E(X)E(Y) + E(X)E(Y) = E(XY) - E(Y)E(X)$

©Georgia Institute of Technology, 2018-2025

What Does Covariance Tell Us?

- If X and Y are independent, then $Cov(X, Y) = 0$
  - If X and Y are independent, then $E(XY) = E(X)E(Y)$
  - $Cov(X, Y) = E(XY) - E(Y)E(X) = E(X)E(Y) - E(Y)E(X) = 0$
- If X and Y are dependent (interrelated), then $Cov(X, Y) \neq 0$
  - If X and Y are dependent, then $E(XY) \neq E(X)E(Y)$
  - $Cov(X, Y) = E(XY) - E(Y)E(X)$

©Georgia Institute of Technology, 2018-2025

Correlation and Covariance

- Two points are correlated if they vary together in a related way
- Statistical measure: covariance
- *Cov(X,Y) = E[(X-E(X))*(Y-E(Y))] = E(XY) – E(X)E(Y)*
- Theoretical and empirical formulas:
- $\rho(X,Y) = \frac{Cov(X,Y)}{\sqrt{Var(X)*Var(Y)}}$
- $r = \frac{\sum_{i=1}^{n}(x_i-\overline{x_i})*(y_i-\overline{y_i})}{\sqrt{\sum_{i=1}^{n}(x_i-\overline{x_i})^2*\sum_{i=1}^{n}(y_i-\overline{y_i})^2}}$
- As defined, the correlation coefficient ρ varies between -1 and 1, i.e., $-1 \le \rho \le 1$ and also thus $-1 \le r \le 1$

©Georgia Institute of Technology, 2018-2025

Binomial Distribution

- Consider tossing a coin n times where heads occurs with probability p and tails occurs with probability (1-p)
- Let S_n denote the number of times the coin comes up heads
  - Then S_n is a random variable that can take on any value in the set {0,1,2,…,n}
  - P(S_n = k) = $\binom{n}{k} p^k (1-p)^{n-k}$
  - Recall $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
- For example, if p = 0.5 and we flip the coin three times
  - P(3 heads) = P(3 tails) = 1/8
  - P(2 heads and 1 tail) = P(2 tails and one head) = $\binom{3}{2} \frac{1}{2}^3$ = 3/8
- If p = 0.4 then P(3 heads) = 0.064, P(3 tails) = 0.216, P(2 heads and 1 tail) = 0.288, P(2 tails and one head) = 0.432

©Georgia Institute of Technology, 2018-2025