

DEF 5.6 CORRELATION COEFFICIENT

THE CORRELATION COEFFICIENT OF TWO RANDOM VARIABLES OF TWO RANDOM VARIABLES G & H IS,

$$\rho_{G,H} = \frac{\text{COV}[G, H]}{\sqrt{\text{VAR}[G] \text{VAR}[H]}} = \frac{\sigma_{G,H}}{\sigma_G \sigma_H}$$

($\rho_{G,H}$ HAS NO UNIT (DIMENSIONS))

PREVIOUS EXAMPLE, $\rho_{G,H} = \rho_{G',H'}$

PROPERTIES OF $\rho_{G,H}$ & $\sigma_{G,H}$

(A) LINEAR COMBINATIONS

THM 5.13 IF $G' = aG + b$ & $H' = cH + d$ THEN

$$(A) \quad \rho_{G',H'} = \rho_{G,H}$$

$$(B) \quad \sigma_{G',H'} = a \cdot c \cdot \sigma_{G,H}$$

EACH GRAPH HAS 200 SAMPLES, EACH MARKED BY A DOT OF THE RANDOM VARIABLE PAIR (G, H) SUCH THAT $E[G] = E[H] = 0$

BIVARIANCE GAUSSIAN RANDOM VARIABLES

Definition 5.10 — **Bivariate Gaussian Random Variables**
 Random variables X and Y have a **bivariate Gaussian PDF** with parameters $\mu_X, \mu_Y, \sigma_X > 0, \sigma_Y > 0$, and $\rho_{X,Y}$ satisfying $-1 < \rho_{X,Y} < 1$ if

$$f_{X,Y}(x,y) = \frac{\exp\left[-\frac{\left(\frac{x-\mu_X}{\sigma_X}\right)^2 - \frac{2\rho_{X,Y}(x-\mu_X)(y-\mu_Y)}{\sigma_X\sigma_Y} + \left(\frac{y-\mu_Y}{\sigma_Y}\right)^2}{2(1-\rho_{X,Y}^2)}\right]}{2\pi\sigma_X\sigma_Y\sqrt{1-\rho_{X,Y}^2}},$$

MARGINALS ARE GAUSSIAN THM 5.10, IT CAN BE SHOWN THAT MARGINALS ARE GAUSSIAN

$$f_G(g) = \frac{1}{\sqrt{2\pi\sigma_G^2}} e^{\left(\frac{-(g-\mu_G)^2}{2\sigma_G^2}\right)} \quad \& \text{SIMILAR FOR } H$$

THIS "PROVES" THAT σ_G^2 & σ_H^2 ARE THE VARIANCE OF G & H

UNCORRELATED IMPLIES INDEPENDENT (GAUSSIAN ONLY)

ALWAYS TRUE THAT

INDEP \Rightarrow UNCORRELATED

UNCORRELATED \Rightarrow INDEP

PROOF: LET $\rho_{G,H} = 0$ IN BIVARIATE GAUSSIAN

$$\begin{aligned} f_{G,H}(g,h) &= \frac{\exp\left[\frac{-(g-\mu_G)^2}{2\sigma_G^2} - \frac{(h-\mu_H)^2}{2\sigma_H^2}\right]}{2\pi\sigma_G\sigma_H} \\ &= \frac{e^{\left(\frac{-(g-\mu_G)^2}{2\sigma_G^2}\right)}}{\sqrt{2\pi\sigma_G^2}} \cdot \frac{e^{\left(\frac{-(h-\mu_H)^2}{2\sigma_H^2}\right)}}{\sqrt{2\pi\sigma_H^2}} = f_G(g) \cdot f_H(h) \end{aligned}$$

THUS $f_{G,H}(g,h) = f_G(g) \cdot f_H(h)$

THM 5.2 BIVARIATE GAUSSIAN RANDOM VARIABLES G & H ARE UNCORRELATED IFF THEY ARE INDEP.

THM 5.21 IF G & H ARE BIVARIATE GAUSSIAN RANDOM VARIABLES WITH PDF GIVEN BY DEFINITION OF 5.10, K_1 & K_2 ARE GIVEN BY LINEARLY INDEPENDENT EQ.

$$K_1 = a_1 G + b_1 H \quad K_2 = a_2 G + b_2 H$$

THM 5.21 IF G & H ARE BIVARIATE GAUSSIAN RANDOM VARIABLES WITH PDF GIVEN BY DEFINITION OF 5.10, K_1 & K_2 ARE GIVEN BY LINEARLY INDEPENDENT EQ, THEN K_1 & K_2 ARE BIVARIATE GAUSSIAN RANDOM VARIABLES

$$K_1 = a_1 G + b_1 H \quad K_2 = a_2 G + b_2 H$$

$$\begin{cases} E[K_i] = a_i \mu_G + b_i \mu_H \\ \text{VAR}[K_i] = a_i^2 \sigma_G^2 + b_i^2 \sigma_H^2 + 2a_i b_i \rho_{G,H} \sigma_G \sigma_H \quad ; \quad i=1,2 \\ \text{COV}[K_1, K_2] = a_1 a_2 \sigma_G^2 + b_1 b_2 \sigma_H^2 + (a_1 b_2 + a_2 b_1) \rho_{G,H} \sigma_G \sigma_H \end{cases}$$

THIS ALSO IMPLIES THAT K_1 & K_2 ARE INDIVIDUALLY GAUSSIAN

EXAMPLE

$$G \text{ is } N(1, 4) \quad \sigma_G^2 \quad \downarrow \quad \text{AND} \quad H \sim N(2, 16) \quad \sigma_H^2 \quad \downarrow \quad \text{INDEPENDENT}$$

FIND PDF OF $L = 3G + 2H$; $a_1 = 3$, $b_1 = 2$

$$\begin{aligned} E[L] &= (3)(1) + (2)(2) = 7 \\ &= a_1 \mu_G + b_1 \mu_H \end{aligned}$$

SINCE THEY ARE INDEPENDENT $\Rightarrow \rho_{G,H} = 0$

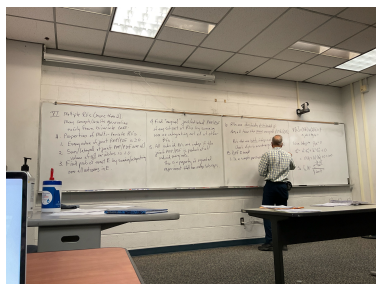
$$\begin{aligned} \sigma_L^2 &= a_1^2 \sigma_G^2 + b_1^2 \sigma_H^2 + 0 \\ &= 3^2(4) + 2^2(16) + 0 \\ &= 100 \end{aligned}$$

$$\text{THUS} \quad f_L(l) = \frac{e^{\left(\frac{-(l-7)^2}{200}\right)}}{\sqrt{200\pi}}$$

MULTIPLE RANDOM VARIABLES (RAND > 2)

MANY CONCEPTS / RESULTS GENERALIZE EASILY FROM BIVARIATE CASE

A. PROPERTIES



THE TOOLS OF PROBABILITY & STOCHASTIC PROCESSES
FOR PSEUDO RANDOM PASSWORD GENERATOR SYSTEM INTEGRITY
MORGAN BERGEN

MULTIVARIATE PROBABILITY MODELS STATE IF X_1, \dots, X_N ARE DISCRETE RANDOM VARIABLES WITH JOINT PMF $P_{X_1, \dots, X_N}(x_1, \dots, x_N)$
(1) THEN ITS $P_{X_1, \dots, X_N}(x_1, \dots, x_N) \geq 0$

$$(2) \sum_{x_1 \in S_{X_1}} \dots \sum_{x_N \in S_{X_N}} P_{X_1, \dots, X_N}(x_1, \dots, x_N) = 1 \Rightarrow$$

RANDOM VARIABLES ARE IDENTICALLY DISTRIBUTED IF THEY ALL HAVE THE SAME MARGINAL PMF/PDF
RVs THAT ARE BOTH INDEPENDENT & IDENTICALLY DISTRIBUTED ARE DESIGNATED iid

PMF PASSWORD GENERATOR EX

IN A SIMPLE PASSWORD SYSTEM, PASSWORDS CAN BE 6, 7, OR 8 CHARACTERS & EITHER \forall CHARS OR MIX OF CHARS A. THUS LET G REPRESENT AN \mathbb{Z}^+ TOTAL OF \forall CHARS

H REPRESENT THE \mathbb{Z}^+ QUANTITY OF NUMERALS

J REPRESENTS FAIL(0) OR SUCCESS(1) OF A USERS 1ST LOGIN ATTEMPT OF A GIVEN SESSION

2 JOINT PMF MODEL IS AS FOLLOWS,

G	H	J	PROB
6	0	0	0.02
6	0	1	0.30
6	1	0	0.01
6	1	1	0.08
7	0	0	0.02
7	0	1	0.25
7	1	0	0.01
7	1	1	0.07
8	0	0	0.03
8	0	1	0.15
8	1	0	0.01
8	1	1	0.05

NOW LETS FIND THE $P[G > 6, \text{SUCCESS}(1) \text{ ON 1ST ATTEMPT}]$

$$P[G > 6, \text{SUCCESS}(1)] = P_{G,H,J}(7,0,1) + P_{G,H,J}(7,1,1) + P_{G,H,J}(8,0,1) + P_{G,H,J}(8,1,1) \\ = 0.25 + 0.07 + 0.15 + 0.05 = 0.52$$

FIND $P_{G,H}(g,h)$ & $P_J(j)$

$P_{G,H}(g,h)$ PAIR, SUM OVER j VALUES, CAN EASILY GET P_G & P_H

g \ h	6	7	8	$P_H(h)$
0	0.32	0.27	0.18	0.77
1	0.09	0.08	0.06	0.23
$P_G(g)$	0.41	0.35	0.24	1.00

FOR $P_J \forall j$ VAL \sum_s OVER $\forall(G,H)$

$$P_J(0) = 0.02 + 0.01 + 0.02 + 0.01 + 0.03 + 0.01 \\ \therefore P_J(0) = 0.10$$

$$P_J(1) = 0.30 + 0.08 + 0.25 + 0.07 + 0.15 + 0.05 \\ \therefore P_J(1) = 0.90$$

NOW ARE G, H, J INDEPENDENT? WELL, WE MUST CHECK FOR $P_{G,H,J}(6,0,0)$ AND IN DOING SO WE DETERMINE THEY ARE NOT INDEPENDENT. \nexists INDEPENDENCE FOR $P_{G,H,J}(g,h,j)$

$$P_G(6) = 0.41 \quad P_H(0) = 0.77 \quad P_J(0) = 0.10 \quad \& \quad P_{G,H,J}(6,0,0)$$

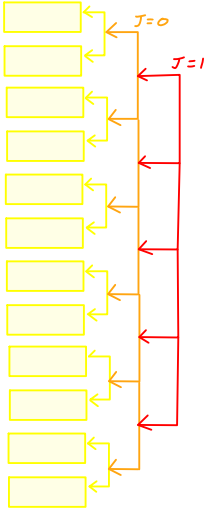
$$P_{G,H,J}(6,0,0) \neq P_G(g) P_H(h) P_J(j) \Leftrightarrow (0.41)(0.77)(0.10) \neq 0.02$$

THUS IMPLIES

THUS THE HIGHER THE CARDINALITY OF $G, H, \parallel J$ THEN THE LOWER THE PROBABILITY

MULTIVARIATE PROBABILITY MODELS STATE IF X_1, \dots, X_N ARE DISCRETE RANDOM VARIABLES WITH JOINT PMF P_X

OR
= IDENTICALLY DISTRIBUTED IF THEY ALL HAVE THE SAME MARGINAL PMF/PDF
INDEPENDENT & IDENTICALLY DISTRIBUTED ARE DESIGNATED iid



PROPERTIES OF RANDOM VARIABLES

RANDOM VARIABLES ARE IDENTICALLY DISTRIBUTED IF THEY ALL HAVE THE SAME MARGINAL PMF/PDF
 RVS THAT ARE BOTH INDEPENDENT & IDENTICALLY DISTRIBUTED ARE DESIGNATED iid

PMF EXAMPLE

IN A SIMPLE PASSWORD SYSTEM, PASSWORDS CAN BE 6, 7, OR 8 CHARACTERS & EITHER \forall CHARS OR MIX OF CHARS A

LET G REPRESENT AN \mathbb{Z}^+ TOTAL OF \forall CHARS

H REPRESENT THE \mathbb{Z}^+ QUANTITY OF NUMERALS

J REPRESENTS FAIL(0) OR SUCCESS(1) OF A USER'S 1ST LOGIN ATTEMPT OF A GIVEN SESSION

2 JOINT PMF MODEL:

G	H	J	PROB
6	0	0	0.02
6	0	1	0.30
6	1	0	0.01
6	1	1	0.08
7	0	0	0.02
7	0	1	0.25
7	1	0	0.01
7	1	1	0.07
8	0	0	0.03
8	0	1	0.15
8	1	0	0.01
8	1	1	0.05

NOW LETS FIND THE $P[G > 6 \text{ \& SUCCESS}(1) \text{ ON 1ST ATTEMPT}]$

$$P[G > 6, \text{SUCCESS}(1)] = P_{G,H,J}(7,0,1) + P(7,1,1) + P(8,0,1) + P(8,1,1) \\ = 0.25 + 0.07 + 0.15 + 0.05 \\ = 0.52$$

FIND $P_{G,H}(g,h)$ & $P_J(j)$

$P_{G,H}(g,h)$ PAIR, SUM OVER j VALUES, CAN EASILY GET P_G & P_H

$h \backslash g$	6	7	8	$P_H(h)$
0	0.32	0.27	0.18	0.77
1	0.09	0.08	0.06	
$P_G(g)$	0.41			

FOR P_J $\forall j$ VAL \sum_s OVER $\forall(G,H)$

$$P_J(0) = 0.02 + 0.01 + 0.02 + 0.01 + 0.03 + 0.01 \\ \therefore P_J(0) = 0.10$$

$$P_J(1) = 0.30 + 0.08 + 0.25 + 0.07 + 0.15 + 0.05 \\ \therefore P_J(1) = 0.90$$

NOW ARE G, H, J INDEPENDENT? WELL, WE MUST CHECK FOR $P_{G,H,J}(6,0,0)$

$$P_G(6) = 0.41 \quad P_H(0) = 0.77 \quad P_J(0) = 0.10$$

$$P_{G,H,J}(G,H,J) =$$