Theorem: $Var(X) = E[X^2] - (E[X])^2$. Let $\mu = E[X]$.

Proof: $Var(X) = E[(X-\mu)^2]$

$$= \sum_a (a-\mu)^2 p_X(a) = \sum_a (a^2 - 2\mu a + \mu^2) p_X(a)$$

$$= \sum_a a^2 p_X(a) - 2\mu \sum_a a p_X(a) + \mu^2 \sum_a p_X(a)$$

$$= E[X^2] - 2\mu^2 + \mu^2 = E[X^2] - (E[X])^2$$

Theorem: $Var(aX+b) = a^2 Var(X)$, where a, b constant.

Proof: ~~$Var(aX+b)$~~ Let $\mu = E[X]$.

$Var(aX+b) = E[((aX+b) - (a\mu+b))^2]$ (defn of Var)

$= E[(a(X-\mu))^2] = E[a^2(X-\mu)^2]$

$= a^2 E[(X-\mu)^2] = a^2 Var(X)$ (defn of Var)

In general, $Var(X+Y) \neq Var(X) + Var(Y)$.

For example, $Var(X+X) = Var(2X) = 4Var(X) \neq Var(X) + Var(X)$

Defn: R.V.'s X and Y are independent iff

$$\forall x \forall y \; P(X=x \cap Y=y) = P(X=x) P(Y=y).$$

Ex: Flip a fair coin $2n$ times independently.

Let X be # of heads in the first n flips,

Let Y be # of heads in the last n flips,

Let Z be # of heads in all $2n$ flips.

X and Y are independent.

X and Z are dependent: $P(X=0) > 0$, $P(Z=n+1) > 0$,

but $P(X=0 \cap Z=n+1) = 0$

<u>Theorem:</u> If X and Y are independent r.v.'s, then $E[XY] = E[X]E[Y]$.

<u>Proof:</u> $E[XY] = \sum_x \sum_y xy\, P(X=x \cap Y=y)$

$= \sum_x \sum_y xy\, P(X=x)P(Y=y)$ (independence)

$= \sum_x x P(X=x) \cdot \sum_y y P(Y=y) = E[X]E[Y]$

<u>Theorem:</u> If X and Y are independent, then
$$Var(X+Y) = Var(X) + Var(Y).$$

<u>Proof:</u> $Var(X+Y) = E[(X+Y)^2] - (E[X+Y])^2$

$= E[X^2 + 2XY + Y^2] - (E[X] + E[Y])^2$

$= E[X^2] + 2E[XY] + E[Y^2] - (E[X])^2 - 2E[X]E[Y] - (E[Y])^2$

$= E[X^2] - (E[X])^2 + E[Y^2] - (E[Y])^2 + 2E[X]E[Y] - 2E[X]E[Y]$

$= Var(X) + Var(Y)$

independence