CSE 16 5-30-24

Recorded Lecture

(Continue 7.1 ....)

<u>Exercise</u>

Find a formula for the probability that a random string of length k from an alphabet of size n has no repeated letters.

<u>Note</u>: if $k > n$, then this prob. is 0 by Pigeonhole Principle.

7.2 Probability Theory

Let S be a finite sample space.

A Probability Law

$$P : \mathbb{P}(S) \to \mathbb{R}$$

must satisfy the following axioms.

(1) for all $E \subseteq S$: $P(E) \geq 0$

(2) $P(S) = 1$

(3) for all $E, F \subseteq S$, if $E \cap F = \phi$,

then $P(E \cup F) = P(E) + P(F)$.

If S is infinite, more care is needed.

Exercise

Prove

(a) $P(\phi) = 0$

(b) for any $E \subseteq S$: $P(E) \le 1$.

(c) for $E_1, E_2, \dots, E_k$ Pairwise disjoint,

$$P(E_1 \cup E_2 \cup \dots \cup E_k) = P(E_1) + P(E_2) + \dots + P(E_k).$$

called <u>additivity Property</u>.

Theorem

Given $E \subseteq S$, The Probability of $\overline{E}$

$= S - E$ is

$$P(\overline{E}) = 1 - P(E).$$

Proof

note $E \cap \bar{E} = \phi$, and $E \cup \bar{E} = S$, so

$$
\begin{aligned}
1 &= P(S) && \text{axiom (2)} \\
&= P(E \cup \bar{E}) \\
&= P(E) + P(\bar{E}) && \text{axiom (3)}
\end{aligned}
$$

$\therefore P(\bar{E}) = 1 - P(E)$. ■

Theorem

Given events $A, B \subseteq S$:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Proof

First: $A = A \cap S = A \cap (B^c \cup B)$

$$= (A \cap B^c) \cup (A \cap B)$$

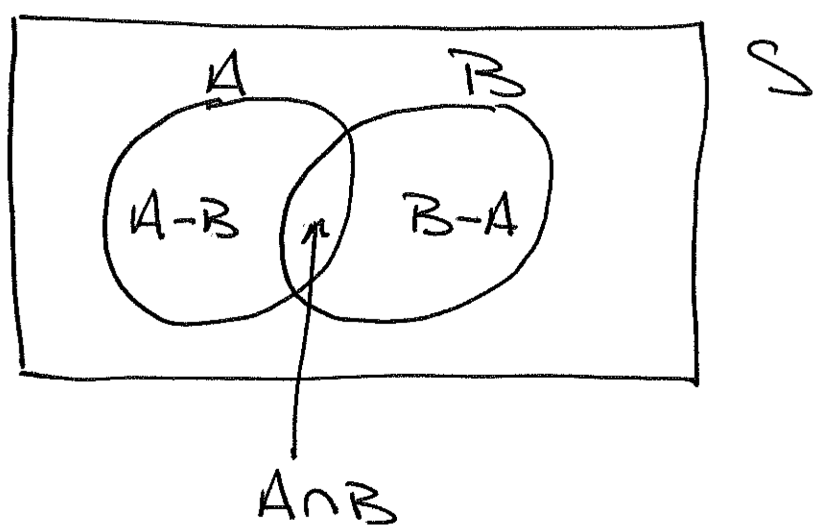
$$= (A - B) \cup (A \cap B)$$

likewise $B = (B - A) \cup (A \cap B)$.

furthermore,

$$A - B, \; B - A, \; A \cap B$$

are pairwise disjoint (Prove this).



and $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ (Prove.)

Thus

$$P(A \cup B) = P(A - B) + P(B - A) + P(A \cap B)$$

$$= \left[P(A-B)+P(A\cap B)\right]+\left[P(B-A)+P(A\cap B)\right]$$
$$- P(A\cap B)$$

$$= P(A)+P(B)-P(A\cap B). \qquad \blacksquare$$

<u>Notation</u>

for any $x \in S$
$$P(x) = P(\{x\})$$

By the additivity property of P, we have for any event $E \subseteq S$:

$$E = \bigcup_{x \in E} \{x\}$$

$$\therefore \quad P(E) = \sum_{x \in E} P(x).$$

Ex.

Define $P(x) = \frac{1}{|S|}$ for all $x \in S$.

i.e. each outcome is equally likely.

Then

$$P(E) = \sum_{x \in E} P(x)$$

$$= \sum_{x \in E} \frac{1}{|S|}$$

$$= |E| \cdot \frac{1}{|S|}$$

$$= \frac{|E|}{|S|}$$

This recovers the uniform Prob. law.

Ex.

A loaded die is thrown in which the Prob. of 3 is twice the Prob. of each other outcome, which are all equal. Find the Prob. of each outcome.

Let

$$P(1) = P(2) = P(4) = P(5) = P(6) = a$$

then $P(3) = 2a$. Thus

$$1 = P(S) = P(\{1, 2, 3, 4, 5, 6\})$$

$$= 5a + 2a = 7a$$

$\therefore \quad a = \frac{1}{7}$

$\therefore$

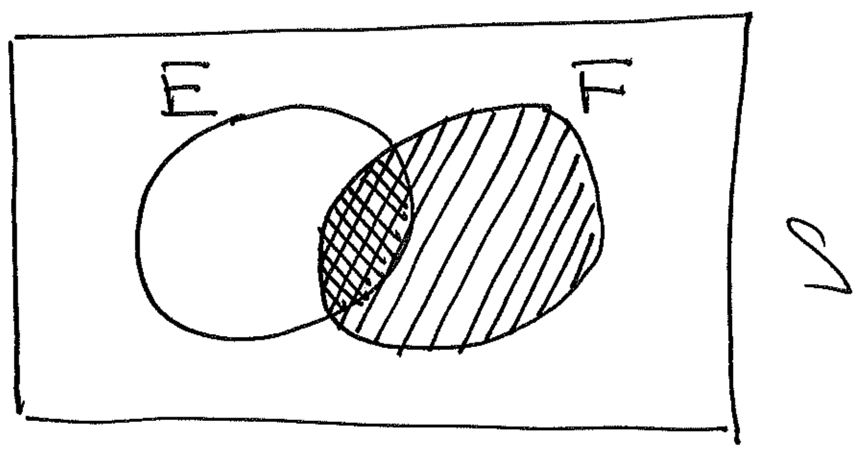
K	1	2	3	4	5	6
P(K)	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$

Defn

Let $E, F \subseteq S$ with $P(F) \neq 0$.

The <u>conditional Probability</u> of E given F is

$$P(E|F) = \frac{P(E \cap F)}{P(F)}$$



Interpretation

Given the knowledge that F occurs, $P(E|F)$ is the prob. that E occurs.

Ex.

The loaded die from last example is thrown. Let $k \in S = \{1, 2, 3, 4, 5, 6\}$ be the outcome. Let

$$E = \{k \geq 2\} = \{2, 3, 4, 5, 6\}$$
$$F = \{k \leq 4\} = \{1, 2, 3, 4\}$$

then

$$E \cap F = \{2, 3, 4\}$$

and

$$P(E) = \frac{6}{7}, \quad P(F) = \frac{5}{7}, \quad P(E \cap F) = \frac{4}{7}$$

Thus

$$P(E|F) = \frac{P(E \cap F)}{P(F)} = \frac{4/7}{5/7} = \boxed{\frac{4}{5}}$$

and

$$P(F|E) = \frac{P(E \cap F)}{P(E)} = \frac{4/7}{6/7} = \boxed{\frac{2}{3}}$$

Ex.

A bit string of len. 3 is selected at random (uniform law). Given that the 1^{st} bit is 0, what is Prob. that there are exactly 2 1's ?

$S = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$F = \{000, 001, 010, 011\}$, $P(F) = \frac{4}{8} = \frac{1}{2}$

$E = \{011, 101, 110\}$, $P(E) = \frac{3}{8}$

$E \cap F = \{011\}$, $P(E \cap F) = \frac{1}{8}$

$$P(E|F) = \frac{P(E \cap F)}{P(F)} = \frac{1/8}{4/8} = \boxed{\frac{1}{4}}$$

Defn

Events $E, F \subseteq S$ are said to be independent iff

$$P(E \cap F) = P(E) \cdot P(F)$$

If $P(F) \neq 0$, this is equiv. to

$$P(E|F) = P(E)$$

If $P(E) \neq 0$, this is equiv. to

$$P(F|E) = P(F)$$

i.e. the knowledge that F occurs does not change Prob. that E occurs

<u>Ex.</u>

A permutation of $\{1,2,3\}$ is selected at random (i.e. uniform law). Is the event that 1 precedes 2 independent of the event that 3 is not first?

$S = \{\underline{123}, \underline{132}, 213, 231, \underline{312}, 321\}$

$E = \{123, 132, 312\}$, $P(E) = \frac{3}{6} = \frac{1}{2}$

$F = \{123, 132, 213, 231\}$, $P(F) = \frac{4}{6} = \frac{2}{3}$

$E \cap F = \{123, 132\}$, $P(E \cap F) = \frac{2}{6} = \frac{1}{3}$

So $P(E \cap F) = \frac{1}{3} = \frac{1}{2} \cdot \frac{2}{3} = P(E) \cdot P(F)$

$\therefore$ E and F are independent.

<u>Check</u>: $P(E|F) = P(E)$ and $P(F|E) = P(F)$

Ex.

Let $S=\{1,2,3,4,5\}$ and define

$$P: \mathbb{P}(S) \to \mathbb{R}$$

by

x	1	2	3	4	5
$P(x)$	.1	.2	.2	.4	.1

Let $E=\{1,2,3\}$, $F=\{3,4,5\}$ and $G=\{1,5\}$

- Are E and F independent?

$$P(E)\cdot P(F) = (.5)(.7) = .35$$

$$P(E\cap F) = P(3) = .2 \neq .35$$

$\therefore$ E, F are not independent.

- are E and G independent?

$P(E)\cdot P(G) = (.5)(.2) = .1$

$P(E\cap G) = P(1) = .1 = P(E)\cdot P(G)$

$\therefore$ E, G are independent.

Defn

A Bernoulli Trial is an experiment with 2 possible outcomes

$$S = \{0, 1\}$$

$$\begin{cases} 1 = \text{success} = \text{heads} = \text{true} \\ 0 = \text{failure} = \text{tails} = \text{false} \end{cases}$$

notation

$p = P(\text{success})$

$q = 1-p = P(\text{failure})$

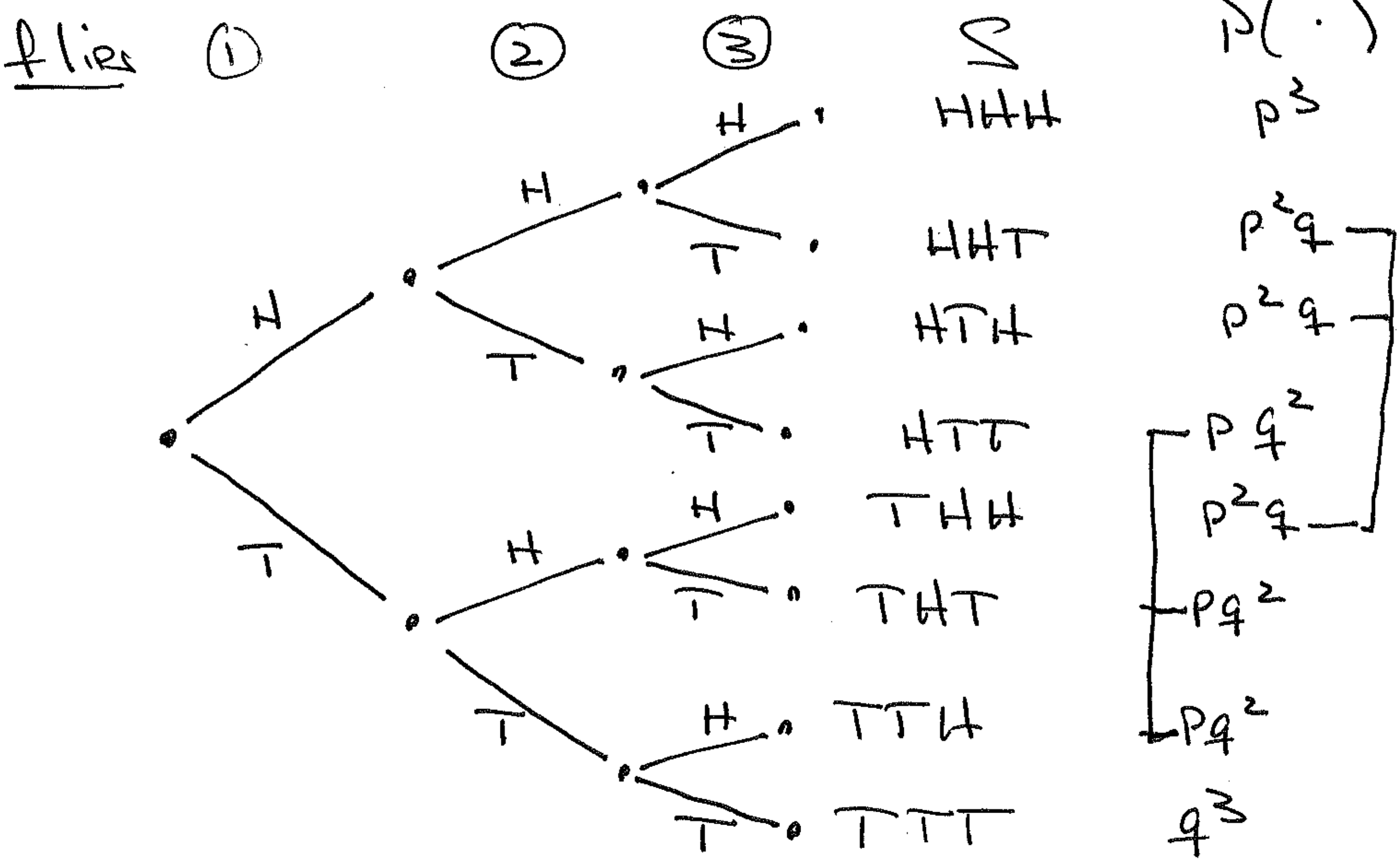
usually consider sequences of Bernoulli trials.

Ex.

A weighted coin is flipped 3 times

$P(H) = p$ and $P(T) = q = 1 - p$

Assume individual flips are independent.



- what is Prob. that exactly 2 flips are Heads?

$$P(\#\text{heads} = 2) = 3p^2q \quad \checkmark$$

- check the probabilities of all outcomes add to 1

$$p^3 + \underline{\underline{3p^2q}} + 3pq^2 + q^3 = (p+q)^3 = 1^3 = 1 \quad \checkmark$$

Theorem

The Prob. of exactly k successes in n independent Bernoulli trials is

$$P(k \text{ successes in } n \text{ ind. trials})$$

$$= \binom{n}{k} p^k q^{n-k}$$

$$= \binom{n}{k} p^k (1-p)^{n-k}$$