

# Probability

---

## Quantifying Uncertainty

# Quiz Scores

---

- poor (average = 76, st dev = 19)
- many, many small mistakes
- Diffie-Hellman was supposed to be easy
- just like sample quiz.
- find errors in lectures and book for points!

# Definitions

---

- A probability is a real number between 0 and 1, inclusive, that measures the uncertainty of what is to happen.
- If an event has probability 0, then it is certain to not happen. If an event has probability 1, it is certain to happen.
- What is the probability that a coin comes up heads?
- What is the probability that an icosahedron comes up 20?
- If there are  $N$  conceivable outcomes, and  $X$  is a set of  $n$  outcomes, then

$$P[X] = n/N.$$

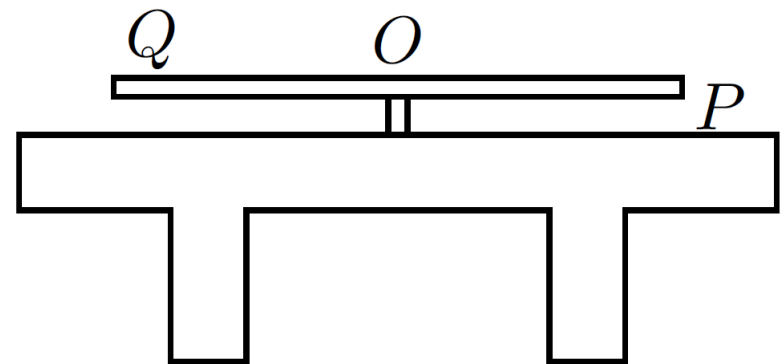
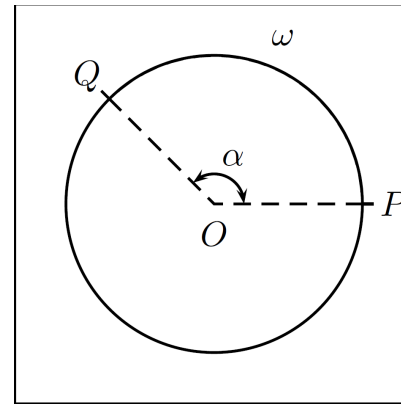
This assumes that all conceivable outcomes are equally conceivable. This is a huge assumption.

- What is the probability that it will rain tomorrow in San Diego?
- What is the probability that an icosahedral die will come up a multiple of 7?

# Roulette Wheels

---

- Imagine a roulette wheel, but one in which the sectors are not all the same size.
- An "event" is a set of angles. The probability of the event is the proportion of all angles that are in the set.
- $\omega = \alpha / (2\pi)$



# Roulette

---

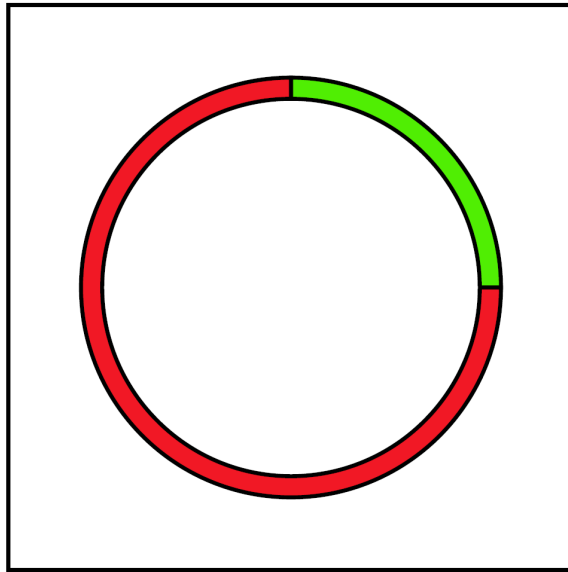


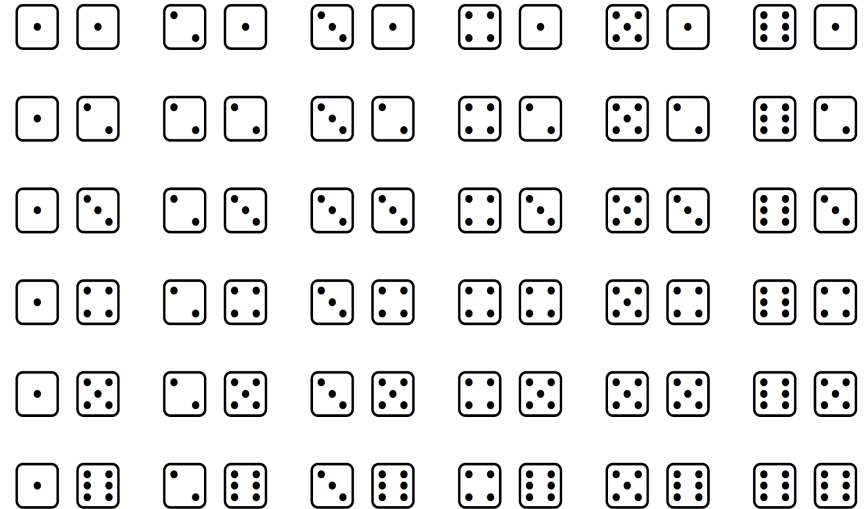
Figure 5.5: A fortune wheel with  $p_1 = 1/4$  and  $p_2 = 3/4$

If this wheel is spun, it will output "green" with probability  $1/4$ .  
If this wheel is spun 1000 times, it will output "green" about 250 times

# Dice

---

- Suppose that you throw two dice. What is the probability that the sum is 7?
- 11 possibilities: 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. So probability is  $1/11$ .
- 36 possibilities, and 6 of them lead to a sum of 7. So probability is  $6/36$ .
- This is not a matter of logic! You must experiment.



# Dice Roulette

---

- Experiments confirm “6/36” interpretation: the dice are independent.
- If you roll N times, you will get 2 approximately  $(1/36)N$  times, 3 approx  $(2/36)N$  times, .... The average outcome will be
- $(\text{total sum})/N =$   
 $((1/36)N*2+(2/36)N*3+(3/36)N*4+(4/36)N*5+(5/36)N*6+(6/36)N*7+(5/36)N*8+(4/36)N*9+(3/36)N*10+(2/36)N*11+(1/36)N*12)$
- The “N” cancels out! We define the expected value of “throw two dice and add them” to be

$$\sum_{k=2}^{12} P[X=k] k$$

- If X is a fortune wheel with outcomes  $x_1, x_2, \dots, x_n$ , its expected value is

$$E[X] = \sum_{k=1}^n P[X = x_k] x_k$$

the expected value of a wheel is the estimated outcome of spinning the wheel many times, and averaging the output.

# Independent Events

---

- An event  $E$  is a set of possible outcomes. The probability of an event  $P[E]$  is the probability that the actual outcome will be in the event  $E$ .
- A random variable  $X$  is a number which depends on the outcome. An equation like  $X=3$  defines an event. Events have probabilities, random variables have expectations.

$$E[X] = \sum_{k=1}^n P[X = x_k] x_k$$

- If  $E, F$  are two events,  $P[E|F]$  denotes the probability that the outcome will be in  $E$ , if you are guaranteed that the outcome will be in  $F$ .
- $P[E|F] = P[E \text{ and } F] / P[F]$
- Two events are independent if, upon learning the outcome of either event, it does not allow you to adjust the probability of the other event. That is, if  $P[E|F]=P[E]$  and  $P[F|E] = P[F]$ .
- Equivalently,  $E$  and  $F$  are independent if  $P[E \text{ and } F] = P[E] P[F]$ .

# Random Variables

---

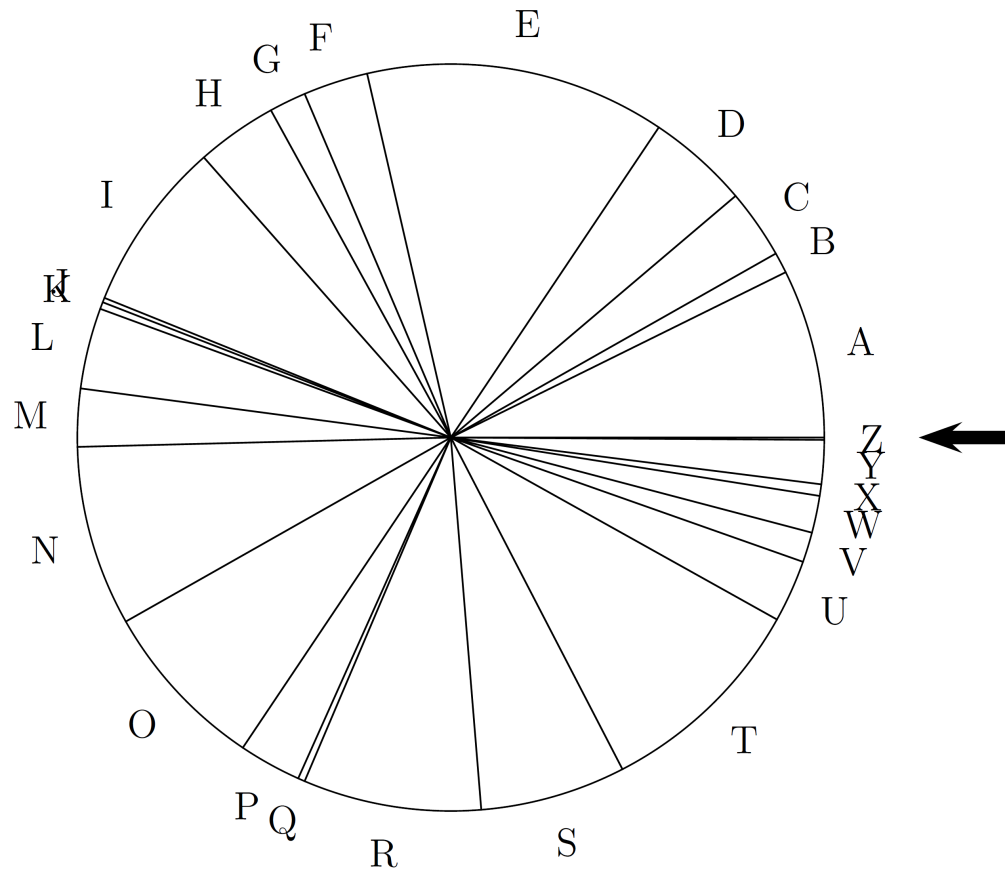
Let  $X$  be a random variable, and  $F$  and event.

$$E[X | F] = \sum_{k=1}^n x_k P[X = x_k | F]$$

- We will work later to define conditional expectation of random variables in various combinations.

# Text Roulette

---



# Index Of Coincidence

---

- The index of coincidence of a text is the probability that a pair of letters (chosen uniformly from the text) are equal.
- IOC for random text =  $1/26 = 3.9\%$
- IOC for English text =  $6.5\%$
- IOC for Caesar ciphertext?
- IOC for Monoalphabetic ciphertext?
- IOC for Vigenere ciphertext?