

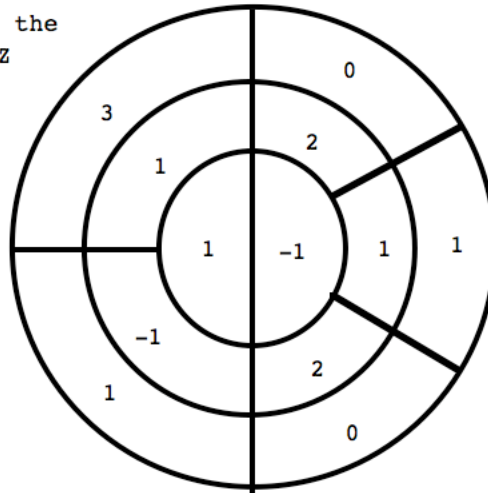
4. You cast a pair of dice: die #1 shows X and #2 shows Y but you only record $X + Y$.
- How much information have you lost in doing this?
 - What is the expected number of bits you need to store 300 samples of $X + Y$?
6. Verbally explain why your intuition tells you that we must have $H(Y|X) \leq H(X)$ and when should we have equality.

- (2) Random words are created by choosing the first letter using the following table of single letter statistics then each subsequent letter is chosen using the table of billetter statistics shown to the right.

A	4
B	1
C	2
D	3

	A	B	C	D
A	4	0	1	5
B	3	1	0	6
C	7	3	0	0
D	1	0	9	0

- How much information do you learn on average when you are told a two letter word given that you know that the word begins with the letter A?
 - How much information do you learn on average when you are told a two letter word given that you know that the word ends with the letter D?
 - How much information do you learn on average when you are told a two letter word given that you know at least one of the letters is a D?
3. Let X, Y, Z be produced by spinning the attached fortune wheel, with X, Y, Z given by the inner, middle and outer circles respectively. Calculate:



- $H(Y|X, Z)$
 - $H(X \times Z)$
 - The expected amount of information about Z you get when you are told the values of X and Y .
4. Suppose a random cryptosystem is obtained as follows:
The message consists of two independent random variables X_1, X_2 both generated by spinning a wheel with arcs labelled 0, 1 of lengths $1/4$ and $3/4$ respectively. Let there be four equiprobable keys with the following corresponding encrypting transformations:

- k1: $(X_1, X_2) \rightarrow (X_1, X_2)$
k2: $(X_1, X_2) \rightarrow (X_2, X_1)$
k3: $(X_1, X_2) \rightarrow (X_1, (X_1 + X_2) \bmod 2)$
k4: $(X_1, X_2) \rightarrow ((X_1 + X_2) \bmod 2, X_1)$

Calculate the entropy of the cyphertext.