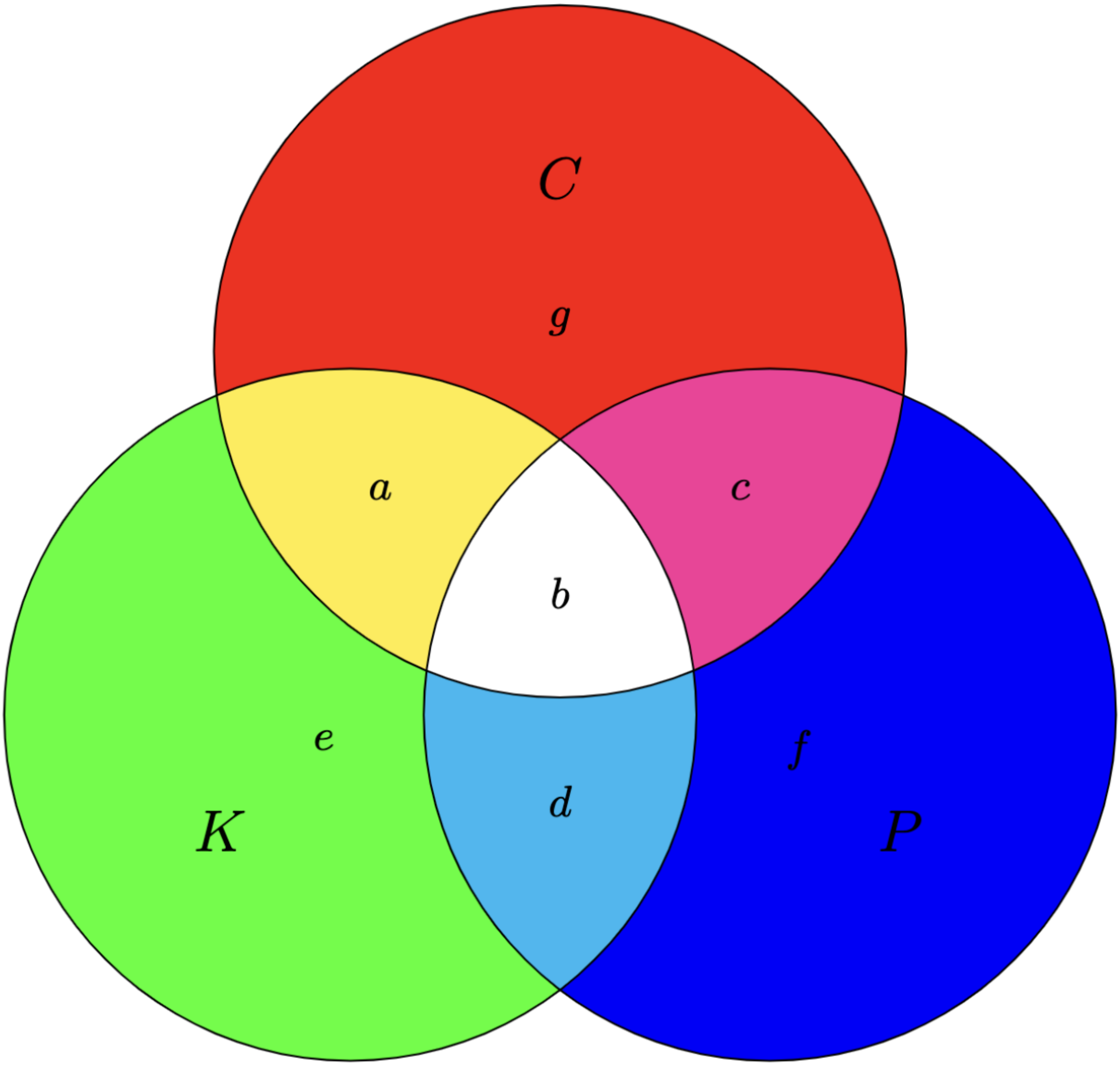
Exercise 5.4 Entropy of the key

Task

Show that, in any cryptosystem, it holds that $H(K|C) \geq H(P|C)$. Under which condition do we have equality?

Solution

We'll be using the diagram provided in the course notes



Using the diagram $H(K|C) = e + d$ and $H(P|C) = f + d$.

$$H(K|C) \overset{?}{\geq} H(P|C)$$

$$e + d \overset{?}{\geq} f + d$$

$$e \overset{?}{\geq} f$$

But we know that $f = 0$ always, so the above equation becomes $e \geq 0$ which is always true, so we get that indeed $H(K|C) \geq H(P|C)$.

We'll get equality if and only if $e = 0$, which is in the case when $H(K|C,P) = 0$. Or in other words: The key is always independent of the plaintext, so that means the key is fully dependent on the ciphertext.

Exercise 5.5 Entropies in the affine cipher

Task

Compute $H(K|C)$ and $H(K|P,C)$ for the Affine cipher when used to encrypt a single letter from the English alphabet. Assume that keys and plaintexts are uniformly chosen.

Solution

H(K|C)

Since we work with the English alphabet we have 26 characters. The keys in the Affine cipher are chosen from $K = Z^{*}{26} \times Z{26}.(a,b) \in K.bcanfreelytakeall26values,howevera needstobesuchthatgcd(a, 26) = 1.Therefore,a \in A = {1,3,4,7,9,11,15,17,19,21,23,25}.|A| = 13 .Sowehave13valuesforaand26forb.Therefore,|K| = 13 \times 26 = 312$.

Because we know the keys are uniformly chosen, each key has $\frac{1}{312}$ probability. From this we can say that

$$H(K) = \sum_{i=1}^{312} \frac{1}{312} log(312) = log(312)$$

As the plaintext is also uniformly chosen it would have the following entropy:

$$H(P) = \sum_{i=1}^{26} \frac{1}{26} log(26) = log(26)$$

Since the Affine cipher is 1:1 map, we can also say that:

$$H(C) = \sum_{i=1}^{26} \frac{1}{26} log(26) = log(26) = H(P)$$

Therefore

$$H(K|C) = H(K) + H(P) - H(C) = H(K) = log(312)$$

H(K|P,C)

Using the diagram above we can see that $H(K|C,P) = e$. Another way of writing this would be

$$e = H(K) - H(P) - H(C|P) + H(C|K) = H(K|C,P)$$

We already know $H(K)$ and $H(P)$. Also, because $H(K|C) = H(K)$ (from the previous step) we know that K and C are independent, hence $H(C|K) = H(C)$, which we also know the value of. What's left is $H(C|P)$. We will show that $H(C|P) = H(C)$, or in other words C is independent of P. We can see this because of the encryption function of the Affine cipher and the uniform distribution of keys. $C = a \times P + b$, but a and b are uniformly distributed and similarly to the way we prove that the Shift cipher is perfectly secure if the key is used only once, we can see that this would be perfectly secure as well, i.e. C does not depend on P. Then $H(C|P) = H(C)$.

So finally we get:

$$H(K|C,P) = H(K) - H(P) - H(C|P) + H(C|K) = H(K) - H(P) - H(C) + H(C) = log(312) - log(26) = log(\frac{312}{26}) = log(12)$$