CSE 5852: Problem Set 1
Due September 14, 2016 at 11:59 PM EST

August 29, 2016

1 Some facts about probability

In this problem we will learn how to manipulate probability by proving some simple results. You may use facts proved in class and previous problems. Anything else must be proved. Most of these statements are fairly simple but do require multiple steps to prove. Be clear why each step can be made.

1. **4 pts** Consider a finite σ-algebra $\mathcal{F}$. Show that for any $E_1, E_2 \in \mathcal{F}$, then $E_1 \cap E_2 \in \mathcal{F}$.

2. **4 pts** Consider a finite σ-algebra $\mathcal{F}$. Show that for any $E_1, E_2 \in \mathcal{F}$, then $E_1 \setminus E_2 \in \mathcal{F}$. Here $E_1 \setminus E_2$ is the set difference between E_1 and E_2.

3. **4 pts** Consider a finite σ-algebra $\mathcal{F}$. Show that for any $E_1, ..., E_n \in \mathcal{F}$, $\cup_i E_i \in \mathcal{F}$.

4. **8 pts** Recall a set of events $\mathcal{E}$ is a partition of Ω if $\forall E_1, E_2 \in \mathcal{E}, E_1 \cap E_2 = \emptyset$ and $\cup_i E_i = \Omega$. Consider the set $\mathcal{F}$ that consists of all unions of sets in the partition and the emptyset. Show that $\mathcal{F}$ is a σ algebra.[1]

5. **8 pts** Consider two σ-algebras $\mathcal{F}, \mathcal{G}$. Show that $\mathcal{F} \cap \mathcal{G}$ is a σ-algebra.

6. **4 pts** Consider a σ-algebra $\mathcal{F}$ with an associated probability measure. For any event $E \in \mathcal{F}$, show that $\Pr[E] = 1 - \Pr[E^c]$.

7. **8 pts** Show that for *any* E_1, E_2,

$$\Pr[E_1 \cup E_2] = \Pr[E_1] + \Pr[E_2] - \Pr[E_1 \cap E_2].$$

2 Alternate Security Definitions

A company asks you to design an encryption scheme. They say they care that an attacker cannot learn the message from the ciphertext.

[1] Important note that we won't prove, every σ-algebra is the "closure" of a partition of the space. There is a 1-1 mapping between σ-algebras and partitions.

a) **10 pts** Formalize this definition. Consider an experiment between the cryptosystem and an attacker. We'll call this definition **message unpredictability**. Assume a uniform message distribution (each message is equally likely). **Hint:** Your definition may have a parameter ϵ that specifies the "unpredictability" of the scheme.

b) **15 pts** Is this definition weaker, equivalent, or stronger than perfect secrecy (or Shannon secrecy)?

   (a) If it is weaker, show that perfect secrecy implies this message unpredictability. Also give an example of something that could be revealed to the attacker under this definition that isn't possible under perfect secrecy.

   (b) If it is stronger, show that message unpredictability implies perfect secrecy. Also give an example of something that could be revealed to the attacker under perfect secrecy that isn't possible under message unpredictability.

   (c) If it is equivalent show a proof (in both directions).

   If you need an assumption or condition on your proof, that is okay, just state it clearly.

c) **5 pts** What happens if the message distribution is not uniform? State how the definition is different in words (you don't need to rewrite the definition).

3 Extending the One-Time Pad

We showed the one-time pad is perfectly secure over binary strings. In this problem we will consider some basic extensions to the one-time pad.

1. **10 pts** Consider an arbitrary message space $\mathcal{M}$ where it is not possible to represent messages as binary strings. Assuming no algebraic properties, how can you construct a one-time pad? What is the "key" for your construction?

2. **20 pts** A crucial part of the name is "one-time" pad. In this section we consider the consequences of reusing keying material. Consider two messages m_1, m_2 that are both encrypted under the same key. Answer the following questions:

   (a) **10 pts** Assume both messages M_1, M_2 are uniformly distribution from the message space.

   - What does the adversary know about the messages after seeing c_1, c_2?
   - Is it possible to recover k?

   (b) **10 pts** Assume each message has two possible values (uniformly selected) $m_1^1, m_1^2, m_2^1, m_2^2$.

   - What information does the adversary know about the messages after seeing c_1, c_2?

- What information (if any) is revealed about the key after seeing c_1? Why doesn't this information violate the definition of perfect secrecy?
- What condition on the messages is necessary and sufficient for the adversary to completely recover the key with probability 1?