Problem Set 3

Deadline: July 16

Problem 1. Consider a new learning model which we call EQ. In EQ, the teacher and learner agree on a sample space $\mathcal{X} = \{0,1\}^n$ and a hypothesis class $\mathcal{C}$, and the teacher chooses some unknown target function $f \in \mathcal{C}$. Then they proceed in rounds as follows. In each round, the learner proposes a hypothesis $h \in \mathcal{C}$ and makes an equivalence query to the teacher. If h is identical to f, the teacher says YES and the learning game is over. Otherwise, the teacher says NO and provides a counterexample, which is any $x \in \mathcal{X}$ for which $h(x) \neq f(x)$. Notice that there is no random sampling anywhere in this model. We say that L is an efficient learner for C in the EQ model if L identifies the correct hypothesis $h \equiv f$ after $\text{poly}(n)$ rounds.

Show that if $\mathcal{C}$ is efficiently learnable in the EQ model then it is also efficiently PAC learnable. In other words, show how to convert a black-box EQ learner into a PAC learner.

Problem 2. Let T be a table consisting of 99 rows and 99 columns. You need to fill 9801 numbers, from 1 to 9801, in table T such that the sum of each row, each column, and each of diagonal elements is the same. Victor has tried to solve this problem but failed. Paula claimed that she solved this problem. Design a protocol, and help Paula convince Victor that Paula has a solution without showing it to Victor.

Problem 3. Let a, b be integers and $a > b$. Prove that

$$\gcd(a,b) = \gcd(b, a \bmod b).$$

Problem 4. We look at the RSA algorithm. Let $p = 11$ and $q = 13$ be two prime numbers used in the RSA algorithm. Let $r = 7$, the number that is used in the public key.

- Compute the private key.
- Let $x \in \{1, \ldots, 9\}$ be the last non-zero number of your student ID. Encrypt x and show the ciphertext.
- Decrypt the ciphertex above.