

## Homework 9

*Lecturer: Ronitt Rubinfeld**Due Date: May 9, 2017*

**Homework guidelines:** You may work with other students, as long as (1) they have not yet solved the problem, (2) you write down the names of all other students with which you discussed the problem, and (3) you write up the solution on your own. No points will be deducted, no matter how many people you talk to, as long as you are honest. It's ok to look up famous sums and inequalities that help you to solve the problem, but don't look up an entire solution.

1. Do one of the following two problems (the same idea solves both):
  - (a) You are given  $n \times n$  matrices  $A, B, C$  whose elements are from  $\mathcal{Z}_2$  (integers mod 2). Show a (randomized) algorithm running in  $O(n^2)$  time which verifies  $A \cdot B = C$ . The algorithm should always output "pass" if  $A \cdot B = C$  and should output "fail" with probability at least  $3/4$  if  $A \cdot B \neq C$ . Assume the field operations  $+, \times, -$  can be done in  $O(1)$  steps.
  - (b) Given two linear functions  $f, g$  mapping  $\{0, 1\}^d \rightarrow \{0, 1\}$ . Show that either  $f = g$  or  $f$  and  $g$  differ on exactly half of the inputs.