Please send your solutions by May 16 2021. You may send a partial solution or ask for a hint. It is ok to work on a homework in a group, but everybody should contribute and everybody needs to write their solution themselves.

[**Assignment 2.1**] **6 points** Matrix multiplication testing: We are given three matrices $A, B, C \in \mathbb{R}^{n\times n}$ and wish to decide in time quadratic in n if $AB = C$. Let us use the following algorithm:

- pick uniformly at random a zero-one vector $x \in \{0,1\}^n$
- check if $Cx = A(Bx)$
- repeat several times

1. Determine the probability that a single test (without repetition – single vector x) detects inequality (given that $AB \neq C$).
2. How many repetitions do we need if we want error at most ε?
3. Which algorithm type is this? (ZPP, BPP, RP, coRP, ...)

[**Assignment 2.2**] **6 points** Coupling: Let us consider the following deck of cards shuffling:

- Pick two cards uniformly at random (where C is the set of all cards, we pick $(x, y) \in C \times C$).
- Switch the cards x, y (if $x = y$ nothing happens).

1. Show that it is the same as picking a uniformly at random a card $x \in C$ and a position $i \in \{1, 2, \ldots, |C|\}$ and switching the card x with the card on position i.
2. Consider the coupling where the card choice and the position choice is the same in both Markov chains (in both coordinates). Let X_t be the number of cards which position differs in the two decks of our coupling at time t. Show that X_t is nonincreasing sequence ($X_{t+1} \leq X_t$).
3. Show that
$$\Pr[X_{t+1} \leq X_t - 1 \mid X_t > 0] \geq \left(\frac{X_t}{|C|}\right)^2$$
4. Argue that the expected number of steps t before $X_t = 0$ is $\mathcal{O}(|C|^2)$ no matter the starting permutations of the two coordinates.

[**Assignment 2.3**] **6 points** Vain coupling: Let φ be a DNF formula in n variables (thus $\varphi(x_1, x_2, \ldots, x_n) = (x_3 \wedge \neg x_7 \wedge x_1) \vee (x_7 \wedge x_4) \vee \ldots)$ which has exactly $\alpha(n)$ satisfying assignments (for some fixed polynomial α). Show that sampling $2^{n/2}$ assignments independently uniformly at random gives us probability of finding at least one satisfying assignment that is just exponentially small.