Prob. 1	Prob. 2

Team members: Küng, Pirelli, Schubert, Dousse, Vu

Problem 1.

a) Let z be a word in $\{0,1\}*$, and z^R its reverse. L_1 must not include zz^R since $(zz^R)^R = zz^R$. But, by the pigeonhole principle, there has to be a z' != z such that a DFA for L_1 cannot distinguish between z and z'. This means that a DFA is unable of both rejecting all palindromes (including zz^R) and accepting all non-palindromes (including $z'z^R$), therefore L_1 must be irregular.

b) Again, by the pigeonhole principle, there has to exist a k and a k' such that a DFA recognizing L_2 cannot distinguish between k 1s and k' 1s. But if the y that follows has Y 1s where $k < Y < k'$, k 1s followed by y must be rejected while k' 1s followed by y must be accepted. This is not possible, we cannot build such a DFA, therefore L_2 is irregular.

c) Same as... oh, wait, it's actually not the same thing, there's a trick! We can freely move 1s from the prefix to the last part, and the last part can match a lot of things. L_3 is equivalent to $L_3' := \{1y' | y' contains at least one 1\}$. Let's prove it. L_3' is trivially a subset of L_3 since it's equivalent to $L_3 with k = 1$. L_3 is a subset of L_3': the prefix in L_3 can be "split" into two parts: one 1, and zero or more 1s. The first part corresponds to the prefix in L_3', the second part is absorbed into y'. Since y contains at least k 1s and $k >= 1$, the condition for y' (at least one 1) is met. Thus, surprisingly, L_3 is a subset of L_3'. Since L_3 is a subset of L_3' and vice-versa, $L_3 = L_3'$. L_3' - in English, the set of words beginning by 1 and containing another 1 somewhere - is regular, here's a DFA that matches it:

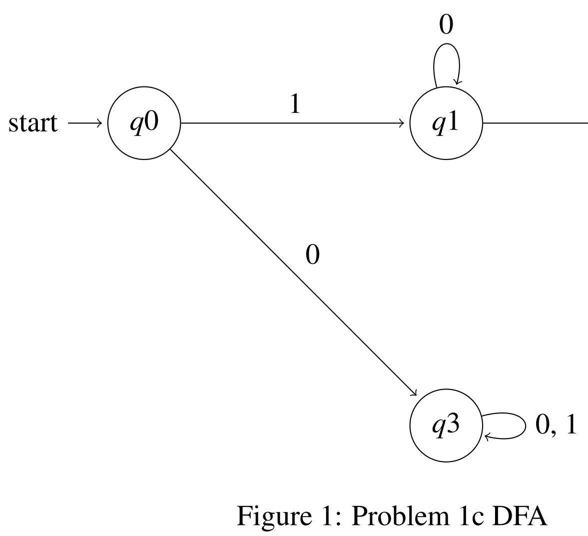

Figure 1: Problem 1c DFA

Problem 2.

a) The start state of our DFA is a state which can go to itself on any input, or go on a 0 to a second state that belongs to a bloc of K states, with each state going to the next one on any input (0 or 1), and a last state that is accepting and has no transitions.

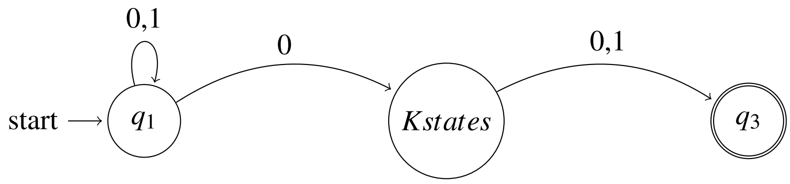

Figure 2: DFA A

b) Let us consider the set K of all words of length $k+1$ in $\{0,1\}^*$. We want to prove that all of these words are pairwise distinguishable by L_k. Let w_1, w_2 be two different words in K. Since they are different, there has to be at least one bit that is not the same between them, which also implies that one of these words will have a 0 where the other has a 1. Let's say w_1 is the one with a 0 and w_2 the one with a 1, and the last change bit is named B. We can construct a suffix u of length X (whether its bits are 0 or 1 doesn't matter), where X is $k-$ number of bits after B in w_1 (thus $0 <= X <= k$). This means that w_1u will be accepted while w_2u will be refused, therefore w_1 and w_2 are distinguishable by L. We juste proved that there exists a set K of $2^{(k+1)}$ words which are pairwise distinguishable by L_k. Using Theorem 1, we conclude that any DFA that implements L_k has to have at least $2^{(k+1)}$ states.