

1. Let  $S$  be a set of strings (not necessarily binary ones, i.e., the letters appearing in them can be arbitrary). Show that the Hamming distance is a metric on  $S$ .
2. A code  $\mathcal{C}$  of length  $n$  is *distance- $d$  maximal* if it has distance at least  $d$  and every string in  $\{0, 1\}^n$  is at Hamming distance less than  $d$  from a codeword of  $\mathcal{C}$ . That is,  $\mathcal{C}$  is any code that cannot be enlarged while preserving its distance. Show that  $\mathcal{C}$  has message length at least  $n - \log_2 \binom{n}{\leq d-1}$  and that if  $d \leq n/2$ , then the rate of this code is at least  $1 - H(d/n)$ .
3. For a binary string  $w$ , let  $\bar{w}$  be the string obtained from  $w$  by exchanging 0's and 1's. Let  $H_1 = \{00, 01\}$  and for  $t \geq 2$ , let  $H_t = \{ww, w\bar{w} : w \in H_{t-1}\}$ . Determine the length, size, message length, rate, distance, and relative distance of the code  $H_t$ . Hint: Once you guess what the distance  $d_t$  of  $H_t$  is, show by induction on  $t$  that  $d(w_1, w_2) \geq d_t$  and  $d(w_1, \bar{w}_2) \geq d_t$  holds for all distinct  $w_1, w_2 \in H_t$ .
4. Let  $\mathcal{C}$  be an  $(n, k, d)$ -code, where  $d$  is odd. Let  $\mathcal{C}'$  be the code obtained from  $\mathcal{C}$  by appending to each string  $w$  in  $\mathcal{C}$  the parity bit, i.e., the bit 1 if  $w$  contains odd number of 1's and the bit 0 otherwise. Show that  $\mathcal{C}'$  is a  $(n+1, k, d+1)$ -code.
5. You wrote data to a disk using a code of length  $n$  and distance  $d$ . After some time, you tried to read the data, but realized that a part of the disk failed and you cannot read bits whose indices belong to a set  $B \subseteq \{1, \dots, n\}$  (you know this set). Show that if  $|B| \leq d-1$ , then you can still recover the original message.
6. You are playing the game of "guess a word" with your friend: He chooses one of  $m$  possible words, and you can ask him a series of  $n$  yes / no questions to determine which word he chose. You are very good at this game, and so for any set  $W$  of words, you can formulate a question which has positive answer exactly for the words belonging to  $W$ . However, your friend can lie up to  $\ell$  times. Prove that following claims are equivalent:
  - There exists a strategy that allows you to win every time.
  - There exists an  $(n, k, 2\ell + 1)$ -code such that  $m \leq 2^k$ .
7. Use the bounds from the lecture (and from the second exercise) to obtain (as good as possible) statements of the following form:
  - If  $\ell \leq \dots$  (a bound depending on  $n$  and  $m$ ), then there definitely exists a winning strategy for the game from the previous task.
  - If  $\ell \geq \dots$ , then there definitely does not exist a winning strategy.