

## Cryptography Assignment 8

1. A Boolean function on  $r$  variables is a function from  $\{0, 1\}^r$  to  $\{0, 1\}$ . Let  $n$  be the number of all possible Boolean functions. What is  $n$  as a function of  $r$ .
2. Let  $f_1, \dots, f_n$  be a list of all the Boolean functions on  $r$  variables. A long code for  $q = 2$  has codewords  $x = x_1 \dots x_n$  where there is some  $y \in \{0, 1\}^r$  such that  $x_i = f_i(y)$  for all  $i$ .  
Is the long code a linear code? What are the values of  $m$  and  $d$  and what is the rate?
3. Describe the long code for general  $q$ . Answer the same questions as in 2 for the  $q$ -ary long code.
4. Let  $g$  be a function from  $\{0, 1\}^n$  to  $\{0, 1\}$ . Show there is an  $i$  such that  $g(x) = x_i$  for all Boolean long codes  $x$ .