MAT 148, Winter 2016
Solutions to HW 4

24. Prove that the dimension of the Reed-Muller code $R(r, m)$ equals

$$k = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$$

by induction using the identity $\binom{m}{i} + \binom{m}{i+1} = \binom{m+1}{i+1}$.

Solution: Let us prove it by induction in m. For $m = 0$ the only Reed-Muller code has generator matrix $G(0, 0) = (1)$ with 1 row. Assume that the formula for k holds for m, let us prove it for $m + 1$. Since

$$G(r + 1, m + 1) = \begin{pmatrix} G(r + 1, m) & G(r + 1, m) \\ 0 & G(r, m) \end{pmatrix},$$

one has

$$k(r + 1, m + 1) = k(r + 1, m) + k(r, m) =$$
$$\left[1 + \binom{m}{1} + \ldots + \binom{m}{r+1}\right] + \left[1 + \binom{m}{1} + \ldots + \binom{m}{r}\right] =$$
$$1 + \left[\binom{m}{1} + 1\right] + \left[\binom{m}{2} + \binom{m}{1}\right] + \ldots + \left[\binom{m}{r+1} + \binom{m}{r}\right] =$$
$$1 + \binom{m+1}{1} + \ldots + \binom{m+1}{r+1}.$$

25. Show that $R(r_1, m) \subset R(r_2, m)$ if $r_1 \le r_2$.

Solution: Let us prove by induction in m that the rows of the generator matrix $G(r_1, m)$ are contained in the set of rows for $G(r_2, m)$. For $m = 0$ the statement is clear. Assume that this holds for m, let us prove it for $m + 1$. One has:

$$G(r_1 + 1, m + 1) = \begin{pmatrix} G(r_1 + 1, m) & G(r_1 + 1, m) \\ 0 & G(r_1, m) \end{pmatrix} \subset$$
$$\subset \begin{pmatrix} G(r_2 + 1, m) & G(r_2 + 1, m) \\ 0 & G(r_2, m) \end{pmatrix} = G(r_2 + 1, m + 1).$$

26. Compute the dimensions and minimum weights of all the Reed-Muller codes of length 8.

Solution: The Reed-Muller code $R(r, m)$ has length 8 if $m = 3$. The dimension equals $1 + \binom{m}{1} + \ldots + \binom{m}{r}$, and the minimal weight equals 2^{m-r}. For $r = 0$ the dimension is 1 and the minimal weight is 8; for $r = 1$ the dimension equals $1 + \binom{3}{1} = 4$ and the minimal weight is 4; for $r = 2$ the dimension equals $1 + \binom{3}{1} + \binom{3}{2} = 7$ and the minimal weight is 2; for $r = 3$ the dimension equals $1 + \binom{3}{1} + \binom{3}{2} + \binom{3}{3} = 8$ and the minimal weight is 1.

Remark: Although it was not a part of the problem, let us list all the generator matrices for the codes $R(r, 3)$. We will do it inductively:

$$G(0,0) = G(1,0) = (1);\ G(0,1) = (1\ 1),$$

$$G(1,1) = \begin{pmatrix} G(1,0) & G(1,0) \\ 0 & G(0,0) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix};$$

$$G(0,2) = (1\ 1\ 1\ 1),\ G(1,2) = \begin{pmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix};$$

$$G(2,2) = \begin{pmatrix} G(2,1) & G(2,1) \\ 0 & G(1,1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$G(0,3) = (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1),$$

$$G(1,3) = \begin{pmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix};$$

$$G(2,3) = \begin{pmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix};$$

$$G(3,3) = \begin{pmatrix} G(3,2) & G(3,2) \\ 0 & G(2,2) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that one can also use the procedure described in p. 33 to generate $G(r,3)$ (with slightly different order of rows) directly.

C: Prove that for all k and t there exist n and a linear $[n,k]$ code correcting t errors. *Hint: Use Varshamov-Gilbert Bound.*

Solution: A code corrects t errors if its minimal weight is at least $d = 2t+1$. The Varshamov-Gilbert bound states that there is an $[n,k]$ code with minimal weight at least d as long as the following inequality is satisfied:

$$1 + \binom{n-1}{1} + \ldots + \binom{n-1}{d-2} < 2^{n-k}. \tag{1}$$

Therefore it is sufficient to prove that for fixed k and d one can find n satisfying (1). To simplify a problem, consider n very large. The left hand side of (1) is a polynomial in n of degree $d-2$, while the right hand side is proportional to 2^n. Since 2^n grows faster than any polynomial of fixed degree, for large n the inequality (1) is satisfied.