# Coding Theory

## Sheet 8

### Spring 2014

1. In a binary linear code of length $n$ containing the codeword $z = 11\cdots 11$, show that the weight distribution $(A_0, A_1, \ldots, A_n)$ satisfies $A_i = A_{n-i}$ for $i = 0, 1, \ldots, n$.

2. In a linear code of length $n$ over $\mathbf{F}_q$ with weight distribution $(A_0, A_1, \ldots, A_n)$, show that $q - 1$ divides $A_i$ for $i = 1, 2, \ldots, n$.

3. Show that, for any $q$, the Reed–Solomon codes

$$\mathcal{N}_{q-1}(r, q),\ \mathcal{N}_q(r, q),\ \mathcal{N}_{q+1}(r, q),$$

defined over $\mathbf{F}_q$, are all MDS.

4. Show that the Reed–Solomon code $\mathcal{N}_{q+2}(3, q)$ is MDS for $q$ even but not for $q$ odd.

5. † Write out generator matrices for the codes $\mathcal{N}_5(3, 5)^\perp$ and $\mathcal{N}_5(3, 5)$. Reduce each to a standard form $[I\, B]$ or $[B\, I]$ and verify that every minor of $B$ is non-zero.

6. In an $[n, k]_q$ MDS code $C$, show that the number of words of minimum weight $d = n - k + 1$ is

$$(q - 1)\binom{n}{d}.$$

(Hint: Given a generator matrix $G$, put it in standard form and consider the number of words of weight $d$ with 0 in the first $k - 1$ positions.)

7. Factorise $X^n + 1$ into irreducible factors over $\mathbf{F}_2$ for $n = 3, 4, 5, 6, 7, 8, 9$.

8. In $R_7 = \mathbf{F}_2[X]/(X^7 + 1)$, calculate $f(X)g(X)$, where

   (a) $f(X) = 1 + X^3 + X^6,\ g(X) = 1 + X;$

   (b) $f(X) = 1 + X^4 + X^5,\ g(X) = 1 + X^3 + X^4.$

9. * Find a generator polynomial and a generator matrix for all binary cyclic codes of lengths $3, 4, 5$. In each case, write down $d$ and $k$.

10. Find a generator polynomial and a generator matrix for all ternary cyclic codes of length 5. In each case, write down $d$ and $k$ .

---

As part of the course assessment, hand in at the School Office a solution to the daggered question, namely 5, if you are doing the BSc course, and to the starred question, namely 9, if you are doing the M-level course, by 2.00 p.m. on Thursday, 3rd April. Solutions to all questions will be placed online on Friday, 4th April.