

## Homework 8 Partial Solutions

### Question 2.19 in Coding Supplement

Let  $C$  be a Hamming code with parity check matrix  $H$  with  $r$  rows. By definition of a Hamming code,  $H$  consists the  $2^r - 1$  distinct nonzero columns containing only 0s and 1s. Since the all zero column is not in  $H$ , no single column in  $H$  is linearly dependent, and hence by theorem 2.6.1 the minimum distance of  $H$  is greater than 1. Furthermore, since all the columns of  $H$  are different, no two columns in  $H$  form a linearly dependent set, and hence by theorem 2.6.1, the minimum distance

of  $H$  is also not 2. The columns  $\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ ,  $\begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ , and  $\begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$  form a linearly dependent set. Therefore, by

theorem 2.6.1, the minimum distance of  $C$  is  $\leq 3$ , and hence exactly 3 by what we showed first.

### Question 15A # 12

For  $n > 2$ , chose the integer  $r$  such that  $2^r > n$ . Let  $M = p_1 p_2 \cdots p_r$ , where  $p_1, p_2, \dots, p_r$  are distinct odd primes. Let  $R = \mathbb{Z} \setminus M\mathbb{Z}$ . Note that  $R$  is a commutative ring. Let  $f(x) = x^2 - 1$ . We will now show that  $f(x)$  has at least  $n$  roots. If  $x^2 - 1 \equiv 0 \pmod{M}$ , then

$$\begin{aligned} x^2 - 1 &\equiv 0 \pmod{p_1} \\ x^2 - 1 &\equiv 0 \pmod{p_2} \\ x^2 - 1 &\equiv 0 \pmod{p_3} \\ &\vdots \\ x^2 - 1 &\equiv 0 \pmod{p_r} \end{aligned}$$

Equivalently,

$$\begin{aligned} x &\equiv \pm 1 \pmod{p_1} \\ x &\equiv \pm 1 \pmod{p_2} \\ x &\equiv \pm 1 \pmod{p_3} \\ &\vdots \\ x &\equiv \pm 1 \pmod{p_r} \end{aligned}$$

For each equation, we can choose either + or - for the sign before 1, so there are  $2^r$  sets of congruences. By the Chinese Remainder Theorem, there is a unique solution to each of these  $2^r$  sets of congruences, and hence there are at least  $2^r$  solutions to the congruence equation  $x^2 - 1 \equiv 0 \pmod{M}$ . Since  $r$  was chosen such that  $2^r > n$ , we have the  $n$  desired roots.