Solutions 9

Exercise 9.1.

1. We know that C has minimum distance d if and only if every $d-1$ columns of H are linearly independent and some d columns are dependent. Thus if C is MDS, every $n-k$ columns are independent. Conversely, if every $n-k$ columns are independent, then $d \geq n-k+1$. By the Singleton bound, $d = n-k+1$ and C is MDS.

2. It is enough to show that if C is MDS, $C^{\perp}$ is MDS. H is a generator matrix for $C^{\perp}$. Since any $n-k$ columns of H are linearly independent, only the zero codeword can have zeros on $n-k$ coordinates (another way to put this is to note that any $n-k$ coordinates of a codeword of $C^{\perp}$ can be taken as message symbols, i.e., any $n-k$ coordinates generate the whole codeword). Thus the minimum distance of $C^{\perp}$ is at least $k+1$. By the Singleton bound and using the fact that the dimension of $C^{\perp}$ is $n-k$, we get that the minimum distance is exactly $k+1$ and $C^{\perp}$ is MDS.

3. Let C be MDS, so that $d = n-k+1$. We already know that any k columns of G are linearly independent, i.e., any k coordinates of a codeword generate the codeword. Given any $d = n-k+1$ coordinates, take one of them together with the remaining $k-1$ coordinates as message symbols. Set this single coordinate to 1 and the remaining $k-1$ to 0; this generates a codeword c which has weight at most $n-k+1$; hence c has weight exactly $d = n-k+1$ and its nonzero coordinates are exactly the d coordinates that we picked.

   Conversely, let C be such that for any d coordinates, there exists a codeword with support exactly equal to these coordinates. Take in particular the codewords which are not zero exactly on the first d coordinates, on the coordinates 2 to $d+1$, on the coordinates 3 to $d+2$, etc. There are $n-d+1$ such codewords, and they form an independent set. But there can be no more than k independent codewords, so that $n-d+1 \leq k$, i.e., $d \geq n-k+1$. Then by the Singleton bound, $d = n-k+1$ and C is MDS.

Exercise 9.2.

1. If there was a $\mathcal{K}_{k,2}$ subgraph, there would exist a pair of distinct codewords x, y that agree on at least k coordinates, i.e., their distance would be at most $n-k$. However, the distance of the code is $n-k+1$, which is a contradiction.

2. This is obtained by counting the number of edges as the summation of left degrees versus the summation of right degrees and equating the two quantities.

3. Define p_i as in the hint. Then C is the expected number of common neighbors that two randomly chosen and distinct codewords X and Y have. Define an indicator random variable I_i which takes the value 1 if the ith left node is a common neighbor of X and Y and zero otherwise. Thus,

$$C = \mathbb{E}\left[\sum_i I_i\right] = \sum_i \mathbb{E}[I_i],$$

by the linearity of expectation. On the other hand, we obviously have $\mathbb{E}[I_i] = p_i$. This means that $C = \sum_i p_i$. Now observe that

$$p_i = \frac{\binom{u_i}{2}}{\binom{\ell}{2}} = \frac{u_i(u_i-1)}{\ell(\ell-1)},$$

so that

$$C = \sum_{i=1}^{n} p_i = \sum_{i=1}^{n} \frac{u_i(u_i-1)}{\ell(\ell-1)} = \frac{1}{\ell(\ell-1)} \left(\sum_i u_i^2 - \ell t \right),$$

where we have used the fact that $\sum_i u_i = \ell t$.

4. By Cauchy-Schwarz, the expression for C found above can be bounded as

$$C \geq \frac{1}{\ell(\ell-1)} \left(\frac{(\ell t)^2}{n} - \ell t \right) = \frac{t}{n(\ell-1)} (\ell t - n).$$

On the other hand, $C \leq k-1$, thus

$$\frac{t}{n(\ell-1)} (\ell t - n) \leq k-1,$$

which after reordering gives the desired bound.

Exercise 9.3.

1. We show that S uniquely determines e. Suppose that there are two different choices e and e' of the error vector, each of weight at most τ such that $H(c+e) = H(c+e')$. This would imply that $H(e-e') = 0$, where $e-e'$ is a nonzero vector of weight at most $2\tau < d$. Then $e-e'$ would be a nonzero codeword of the code, which is a contradiction as we know that no nonzero codeword can have weight less than d.

2. We have $S^\top = H(c+e) = Hc + He = He$, as c is a codeword and thus $Hc = 0$.

3. This immediately follows from expanding the system of linear equations given by $S^\top = He$, and observing that $e_j = 0$ for every $j \notin J$.

4. First we note that the multiplicative inverse of $1 - \alpha_j x$ can be written as

$$\frac{1}{1-\alpha_j x} \equiv 1 + \alpha_j x + (\alpha_j x)^2 + \cdots + (\alpha_j x)^{d-2} \mod x^{d-1}.$$

Substituting this identity in the summation $\sum_{j \in J} \frac{e_j}{1-\alpha_j x}$ and we obtain

$$\sum_{j \in J} \frac{e_j}{1-\alpha_j x} = \sum_{\ell=0}^{d-2} x^\ell \left(\sum_{j \in J} e_j \alpha_j^\ell \right) \mod x^{d-1}$$

which combined with the previous part gives the required identity.

5. The degree bounds hold because of the bound on the number of errors, i.e., $|J| \le \tau$. Note that $\Lambda(x)$, by its definition, factorizes to linear factors. Thus $\Lambda(x)$ and $\Gamma(x)$ are relatively prime iff they do not share a root. This must be the case because if $\Lambda(\alpha_t^{-1}) = 0$, then $t \in J$ and
$$\Gamma(\alpha_t^{-1}) := e_t \prod_{m \in J \setminus \{t\}} (1 - \alpha_m \alpha_t^{-1})$$
which is nonzero because the α_i are distinct.

6. Using part 4 and the definition of $\Lambda(x)$, we get
$$\Lambda(x)S(x) \equiv \sum_{j \in J} \frac{e_j \prod_{j \in J}(1 - \alpha_j x)}{1 - \alpha_j x} \mod x^{d-1}$$
which is indeed $\Gamma(x)$.

7. As $\Lambda(0) = 1$, the polynomial $\Lambda(x)$ has a multiplicative inverse in the ring $\mathbb{F}_q[x]/x^{d-1}$ and we can write
$$S(x) \equiv \Gamma(x)(\Lambda(x))^{-1} \mod x^{d-1}.$$
Substituting this in the assumption, we get
$$\lambda(x)\Gamma(x)(\Lambda(x))^{-1} \equiv \gamma(x) \mod x^{d-1},$$
or,
$$\lambda(x)\Gamma(x) \equiv \gamma(x)\Lambda(x) \mod x^{d-1}.$$
Because the degree of both sides is already less than $d-1$, we have in fact
$$\lambda(x)\Gamma(x) \equiv \gamma(x)\Lambda(x),$$
and thus $\Lambda(x) \mid \lambda(x)\Gamma(x)$, which means $\Lambda(x) \mid \lambda(x)$ because $\gcd(\Lambda(x), \Gamma(x)) = 1$.

8. Let $\lambda(x) = \sum_{i=0}^{\tau} \lambda_i x^i$ and $\gamma(x) = \sum_{i=0}^{\tau-1} \gamma_i x^i$. Then the identity
$$\lambda(x)S(x) \equiv \gamma(x) \mod x^{d-1}$$
can be written in the matrix form
$$\left(\begin{array}{cccc} S_0 & 0 & \dots & 0 \\ S_1 & S_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ S_{\tau-1} & S_{\tau-2} & \dots & 0 \\ \hline S_\tau & S_{\tau-1} & \dots & S_0 \\ S_{\tau+1} & S_\tau & \dots & S_1 \\ \vdots & \vdots & \ddots & \vdots \\ S_{d-2} & S_{d-3} & \dots & S_{d-\tau-2} \end{array}\right) \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_\tau \end{pmatrix} = \left(\begin{array}{c} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{\tau-1} \\ \hline 0 \\ 0 \\ \vdots \\ 0 \end{array}\right)$$
And we know that any solution of this system for $\lambda(x)$ satisfies $\Lambda(x) \mid \lambda(x)$. Now if $\lambda(x)$ is nonzero, we know that the set of roots of λ determines a superset J' (of size at most τ) of the set of error locations J. Thus, using $\lambda(x)$, one can form and solve the system
$$(\forall i = 1, \dots, \tau)\colon \sum_{j \in J'} \alpha_j^i e_j = S_i$$
for unknowns e_j (which is known as *erasure decoding*) to find the error values.