Exercise Sheet 9

(Solutions)

Exercise 9.1. We are looking for a matrix

$$H_{\mathcal{C}} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^k & \alpha_2^k & \dots & \alpha_n^k \end{pmatrix} \begin{pmatrix} v'_1 & & & 0 \\ & v'_2 & & \\ & & \ddots & \\ 0 & & & v'_n \end{pmatrix}$$

such that $G_{\mathcal{C}} H_{\mathcal{C}}^{\top} = 0$. Thus we want that for each $i = 0, \dots, k-1$ and $j = 0, \dots, n-k-1$,

$$\sum_{\ell=1}^{n} v_\ell v'_\ell \alpha_\ell^{i+j} = 0,$$

or equivalently,

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \dots & \alpha_n^{n-2} \end{pmatrix} \begin{pmatrix} v_1 & & & 0 \\ & v_2 & & \\ & & \ddots & \\ 0 & & & v_n \end{pmatrix} \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_n \end{pmatrix} = 0,$$

meaning that the set of solutions for $(v'_1, \dots, v'_n)$ is the set of codewords of an $[n, 1, n]$ Generalized Reed-Solomon code. As the distance of this code is n, there is always a nonzero codeword that satisfies $v'_1 \neq 0, \dots, v'_n \neq 0$.

Exercise 9.2.

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 an 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., $|J| \leq \tau$. 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.