Question 4

4.1

We show equivalence by showing that having an oracle solver for one problem allows us to solve the other problem.

In the forward direction, let $G \in \mathbb{F}_2^{n \times k}$ but a generator matrix, $c \in \mathbb{F}_2^n$ be some partially corrupted codeword, and $\mathcal{O}^S$ be the syndrome decoding oracle. If we can find a corresponding parity-check matrix H, then $y \leftarrow Hc \in \mathbb{F}_2^{n-k}$ is a syndrome. We can then feed H, y to $\mathcal{O}^S$ and obtain the error term e. Solving the linear system $Gm = c - e$ allows us to recover the message m.

To compute the parity check matrix, we assume that the generator matrix G has the following form:

$$G = \begin{bmatrix} I_k \\ G' \end{bmatrix}$$

where $G' \in \mathbb{F}_2^{(n-k) \times k}$. This is a reasonable assumption because if G does not have this form, we can column-reduce G to have this form. Column-reducing G is guaranteed to produce I_k on the top G has column rank k (otherwise the code will map distinct messages onto the same codeword, which cannot happen). Column-reducing G is equivalent to right-multiplication by an invertible matrix, which does not affect the set of codewords in the code $\mathcal{C}$.

Let $H = [-G' \mid I_{n-k}]$, then H is a rank-$(n-k)$ matrix such that $HG = 0$, meaning that H is a parity check matrix that corresponds with G.

In the backward direction, let $H \in \mathbb{F}_2^{(n-k) \times n}$ be a parity check matrix, $y \in \mathbb{F}_2^{n-k}$ be a syndrome, and $\mathcal{O}^C$ be a codeword decoding oracle. We can row reduce H to have the form $H = [I_{n-k} \mid H_0]$ where $H_0 \in \mathbb{F}_2^{(n-k) \times k}$. Since row reducing H is equivalent to left multiplication by an invertible matrix, the row-reduced $[I_{n-k} \mid H_0]$ is also a parity check matrix for the same code.

Let G be as follows:

$$G = \begin{bmatrix} -H_0 \\ I_k \end{bmatrix}$$

Then $G \in \mathbb{F}_2^{n \times k}$ is a rank-k matrix such that $HG = 0$. In other words, H is the parity check matrix of a linear code generated by G. If we solve the linear system $Hz = y$ for z, then z is some partially corrupted codeword in the linear code. Let $m \leftarrow \mathcal{O}^C(G, z)$. By the definition of the codeword decoding problem $e = z - Gm$ is the error term.

4.2

Again, we will show equivalence by showing that a solver for one problem allows us to solve the other problem.

In the forward direction, let $A \in \mathbb{F}_2^{n \times k} = PGS$ and $c \in \mathbb{F}_2^n = Am + e$ be what they are in the McEliece codeword decoding problem. Let $\mathcal{O}^S$ be a McEliece syndrome decoding oracle. If we can find the corresponding H_0 such that $[I_{n-k} \mid H_0] = SHP$ for some parity check matrix H, then we can compute $y \leftarrow [I_{n-k} \mid H_0]c$, feed H_0, y to $\mathcal{O}^S$ to obtain the error term e, then solve the linear system $Am = c - e$ to recover the message m, which is the solution to the McEliece codeword decoding problem.

To compute H_0, we first column-reduce A such that

$$A = \begin{bmatrix} I_k \\ A' \end{bmatrix}$$

where $A' \in \mathbb{F}_2^{(n-k) \times k}$. Column-reducing A is equivalent to right multiplication by an invertible matrix, so the column-reduced A still corresponds to the same generator matrix G. In addition, both P, S are invertible, so A is guaranteed to have rank k.

Let $\tilde{H} = [-A' \mid I_{n-k}]$, then $\tilde{H}A = \tilde{H}PGS = 0$, which means that $H = \tilde{H}P$ is a parity check matrix for G. If we then row reduce $\tilde{H} = HP^{-1}$:

$$\tilde{S}\tilde{H} = \tilde{S}HP^{-1} = [I_{n-k} \mid H_0]$$

Since $\tilde{S}$ is invertible and P^{-1} is also a permutation, H_0 is indeed the matrix used in the McEliece syndrome decoding.

In the other direction, let $H_0 \in \mathbb{F}_2^{(n-k)\times k}$ and $y \in \mathbb{F}_2^{n-k}$ be what they are in the McEliece syndrome decoding problem. Let $\mathcal{O}^C$ be a McEliece codeword decoding oracle. Let $\tilde{H} = [I_{n-k} \mid H_0]$, then solve the linear system $\tilde{H}z = y$ for z.

Let $\tilde{A}$ be as follows:

$$\tilde{A} = \begin{bmatrix} -H_0 \\ I_k \end{bmatrix}$$

Then $\tilde{H}\tilde{A} = 0$. By the definition of the McEliece syndrome decoding problem, we know that $\tilde{H} = SHP$ for some permutation P and some invertible matrix S, which means that $SHP\tilde{A} = 0$. Since $\tilde{A}$ has k-rank and P is invertible, $P\tilde{A}$ has rank-k. In other words, $P\tilde{A} = G$ for some generator matrix G that corresponds with H. Re-arranging this equation: $\tilde{A} = P^{-1}GI_k$ is a valid McEliece codeword decoding public key.

Let $m \leftarrow O^C(\tilde{A}, z)$, then $e = z - Gm$ is the error term and the solution to the McEliece syndrome decoding problem.