Selected Areas in Cryptology - Part 1: Post-quantum cryptography

Exercise sheet 4, 4 March 2024

1. The binary Hamming code with parameters $n = 15$ and $k = 11$ has the parity-check matrix

$$\mathbf{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

   Correct the word $(0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1)$.

2. Show that the (regular) decoding problem is equivalent to the syndrome decoding problem. **Hint:** We need to show the reduction both ways:

   (a) We assume that we have access to a syndrome decoder: given a syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, the syndrome decoder outputs $\mathbf{e}$ such that $\mathbf{s} = \mathbf{He}$ and $\mathrm{wt}(\mathbf{e}) = t$. How can we use the syndrome decoder to solve an instance of the decoding problem (given a word $\mathbf{y} \in \mathbb{F}_2^n$ with t errors and a generator matrix of the code $\mathbf{G} \in \mathbb{F}_2^{k\times n}$, find the codeword $\mathbf{c}$ and recover the message) ?

   (b) We assume that we have access to a regular decoder: given a word $\mathbf{y} \in \mathbb{F}_2^n$ with t errors and a generator matrix of the code $\mathbf{G} \in \mathbb{F}_2^{k\times n}$, the decoder outputs $\mathbf{c}$ such that $\mathbf{y} = \mathbf{c} + \mathbf{e}$. How can we use the regular decoder to solve an instance of the syndrome decoding problem (given a syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$ and a parity-check matrix $\mathbf{H} \in \mathbb{F}_2^{(n-k)\times n}$, find $\mathbf{e}$ such that $\mathbf{s} = \mathbf{He}$ and $\mathrm{wt}(\mathbf{e}) = t$) ?

3. Use Prange's algorithm to solve an instance of the syndrome decoding

problem with parameters $n = 10$, $k = 4$, $t = 2$ and input

$$\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \mathbf{s} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

Hint: This example can be solved, for instance, with a permutation that only swaps two columns.