Problem 1. Show that, if $H$ is the parity-check matrix of a code of length $n$, then the code has minimum distance $d$ iff every $d - 1$ columns of $H$ are linearly independent and some $d$ columns are linearly dependent.

Problem 2. (a) Using Problem 5 part (c) of Homework 10, show that the minimum distance of a binary linear code of length $N$ and $2^L$ codewords satisfies

$$d_{\min} \leq \frac{N}{2} \left( \frac{2^L}{2^L - 1} \right).$$

(b) The above bound is effective when $L$ is small relative to $N$. Assume now that the code is systematic, namely, each codeword consists of $L$ information bits followed by $N - L$ check/parity bits. For larger values of $L$, the following bound is tighter: Show that for all $j$, $1 \leq j \leq L$,

$$d_{\min} \leq \frac{N - L + j}{2} \left( \frac{2^j}{2^j - 1} \right).$$

Hint: Consider the $2^j$ codewords in the code with the first $L - j$ information bits constrained to be zero. Remove the first $L - j$ bits from these $2^j$ codewords, obtaining a new code of blocklength $N - L + j$. Apply the bound in (a) to this new code. Bonus: show that the bound is valid for any (not necessarily linear) binary code of block length $N$ and $2^L$ codewords.

(c) Now consider $N$ and $d_{\min}$ as fixed, $N \geq 2d_{\min} - 1$, and show that the number of check digits $N - L$ must satisfy

$$N - L \geq 2d_{\min} - 2 - \lfloor \log_2 d_{\min} \rfloor.$$

Hint: choose $j = 1 + \lfloor \log_2 d_{\min} \rfloor$ and remember that $N - L$, $d_{\min}$ and $j$ are integers.

Problem 3. In this problem we will show that there exists a binary linear code which satisfies the Gilbert-Varshamov bound. In order to do so, we will construct a $r \times n$ parity-check matrix $H$ and we will use Problem 1.

(a) We will choose columns of $H$ one-by-one. Suppose $i$ columns are already chosen. Give a combinatorial upper-bound on the number of distinct linear combinations of these $i$ columns taken $d - 2$ or fewer at a time.

(b) Provided this number is strictly less than $2^r - 1$, can we choose another column different from these linear combinations, and keep the property that any $d - 1$ columns of the new $r \times (i + 1)$ matrix are linearly independent?

(c) Conclude that there exits a binary linear code of length $n$, with at most $r$ parity-check equations and minimum distance at least $d$, provided

$$1 + \binom{n - 1}{1} + \cdots + \binom{n - 1}{d - 2} < 2^r. \quad (1)$$

(d) Show that there exists a binary linear code with $M = 2^k$ distinct codewords of length $n$ provided $M \sum_{i=0}^{d-2} \binom{n-1}{i} < 2^n$. 