Solution 4.2

(a) Let e_j be the single-bit error on bit j. The $(n-k)$-dimensional vectors He_j are the n columns of H; they are the syndromes for single-bit errors. By assumption, any $d-1$ of these single-bit-error syndromes are linearly independent, but there exists a set of d of these syndromes that are linearly dependent.

1. Consider two codewords y_1 and y_2, and let $e = y_1 \oplus y_2$ be the error that connects them. e is also a codeword. The Hamming distance between y_1 and y_2 is

$$d(y_1, y_2) = w(y_1 \oplus w_2) = w(e) \ .$$

Suppose $w(e) < d$. Then e is a linear combination of $< d$ single-bit errors e_j, and He is a linear combination of $< d$ single-bit-error syndromes He_j. Since these He_j are linearly independent, their sum, He, cannot be zero, contradicting the fact that $He = 0$, since e is a codeword. We conclude that for any pair of codewords, $d(y_1, y_2) = w(e) \geq d$, implying that the distance of the code is $\geq d$.

2. Consider the set of d e_j's whose corresponding syndromes He_j are linearly dependent. The sum of all these He_j's must be zero for the following reason: some subset of the He_j's must sum to zero by the linear dependence of the whole set, but no subset with less than d members can sum to zero by the linear independence of all such subsets; this leaves only the sum of all the vectors to sum to zero. We conclude that sum of all d of the e_j's is a codeword having weight d. Thus the distance of the code is $\leq d$.

Putting these two results together, we find that the code has distance d.

(b) The only way two binary numbers can sum bitwise to zero is if they are identical, so any two of the binary numbers from 1 to $2^r - 1$ are linearly independent. But the first three binary numbers are not linearly independent. Thus all Hamming codes have distance $d = 3$.

This implies that Hamming codes can correct all single-bit errors. This is not surprising since Hamming codes are constructed so that single-bit errors fill up the syndrome space, meaning that single-bit errors, but nothing more, can be corrected.