Homework 3 Solutions

E2-205, Aug–Dec 2017

Solutions to Homework Assignment 3

1. (a) Let \( \sim \) be the relation on \( G \) defined by \( a \sim b \) if and only if \( a - b \in H \). It can be easily checked that \( \sim \) is an equivalence relation. (Reflexivity, symmetry and transitivity of the relation easily follow from the properties of a subgroup.) Now, by definition of an equivalence class, \( a \) and \( b \) in \( G \) belong to the same equivalence class of \( \sim \) iff \( a - b \in H \). On the other hand, it can also be readily verified that for all \( a \) and \( b \) in \( G \), we have \( a - b \in H \) iff \( a \) and \( b \) belong to the same coset of \( H \) in \( G \). Hence, \( a \) and \( b \) belong to the same equivalence class of \( \sim \) iff they belong to the same coset of \( H \) in \( G \). This is the same as saying that the equivalence classes of \( \sim \) are precisely the cosets of \( H \) in \( G \).

Since the equivalence classes of the relation \( \sim \) form a partition of \( G \), the cosets of \( H \) form a partition of \( G \). Moreover, each coset has size equal to \(|H|\), since there is a bijection (one-to-one correspondence) between \( H \) and any coset \( g + H \). (Indeed, the function that maps \( h \in G \) to \( h + g \in h + G \) is a bijection.) Hence, \( |G| = (\text{number of distinct cosets}) \times |H| \). Therefore, number of distinct cosets = \( |G| / |H| \).

(b) For this part, the following observation is useful: for binary words \( x = (x_1, \ldots, x_n) \) and \( y = (y_1, \ldots, y_n) \), the Hamming weight of \( x + y \) (taken over \( \mathbb{F}_2 \)) can be expressed as

\[
 w_H(x + y) = w_H(x) + w_H(y) - 2w_H(x \land y),
\]

where \( x \land y \) refers to the coordinatewise AND of \( x \) and \( y \) (i.e., \( x \land y = (z_1, \ldots, z_n) \in \{0, 1\}^n \) such that \( z_i = 1 \) iff \( x_i = y_i = 1 \)). Thus, if \( x \) and \( y \) are both of even Hamming weight, then so is \( x + y \). Moreover, if \( x \) and \( y \) are both of odd Hamming weight, then \( x + y \) has even Hamming weight.

Let \( C \) be a binary linear code and \( C_{\text{even}} \) be the set of codewords having even weight. By the above observation, \( C_{\text{even}} \) is a linear code in itself, i.e., it forms a subspace of \( C \). Viewing \( C \) as an abelian group under the + operation, we see (by part (a) above) that the cosets of \( C_{\text{even}} \) in \( C \) form a partition of \( C \).

Now, either \( C \) has no codewords of odd weight, in which case \( C_{\text{even}} = C \), or \( C \) has codewords of odd weight. In the latter case, let \( C_{\text{odd}} \) denote the set of codewords having odd weight. Observe that \( C_{\text{odd}} \) is a coset of \( C_{\text{even}} \) in \( C \): for \( x, y \in C_{\text{odd}} \), the difference (which over \( \mathbb{F}_2 \) is the sum \( x + y \)) is a codeword of even weight, i.e., \( x + y \) is in \( C_{\text{even}} \), again by the observation made at the beginning. Thus, \( C_{\text{even}} \) and its coset \( C_{\text{odd}} \) together form a partition of \( C \). By part (a), \( |C| = 2 \times |C_{\text{even}}| \).

In summary, either \( C \) has no codewords of odd weight, in which case \( |C| = |C_{\text{even}}| \), or \( C \) has codewords of odd weight, in which case \( |C| = 2 \times |C_{\text{even}}| \).
There are 10 single-error patterns, and \( \binom{5}{2} = 10 \) double-error patterns in which both errors are in the first five positions. In order to be correctable, these 20 error patterns must give rise to distinct non-zero syndromes. The number of distinct non-zero syndromes that can be obtained from the parity-check matrix of a binary \([10, k]\) linear code is \(2^{10-k} - 1\). So we must have \(2^{10-k} - 1 \geq 20\). Therefore, \(k \leq 10 - \log_2 21 \approx 5.6\), which shows that the maximum dimension that such a code can have is \(k = 5\).

To construct a code that meets the requirements of the problem, we need to construct a parity-check matrix with 10 distinct nonzero columns, such that

- the sum of any two of the first five columns is distinct from the sum of any other pair of columns from the first five; and
- the sum of any two of the first five columns is also distinct from any of the ten columns of the matrix.

It may be verified that the following construction does the trick: let \(C\) be the binary linear code with parity-check matrix

\[
H = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0
\end{bmatrix}
\]

Clearly all columns of the matrix are nonzero and distinct, so the code can correct all single-error patterns. The sum of any two of the first five columns gives a vector of weight 2, which is distinct from any of the columns of \(H\), and it is also clear that distinct pairs of columns (from the first five) have distinct sums. Thus, any double-error pattern with both errors in the first five positions gives rise to a syndrome that is distinct from any syndrome due to a single-error pattern, as well as from any syndrome due to another such double-error pattern.

If we choose the 21 to-be-corrected error patterns (including the “no-error” pattern) as the coset leaders of their respective cosets, then a syndrome decoder for \(C\) will have the required error-correction properties.

Note that \(C\) has dimension \(k = 10 - \text{rank}(H) = 5\). As shown above, this is the maximum dimension that such a code can have.

Remark: The code \(C\) is in fact capable of doing a lot more than what is required. On top of correcting all the required single- and double-error patterns, it can also correct all weight-3 and weight-5 error patterns in which all errors occur in the first five positions. (What about weight-4 error patterns?)
3. (a) The required standard array is as shown below:

<table>
<thead>
<tr>
<th>Coset</th>
<th>Syndrome</th>
<th>Coset Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C$</td>
<td>$[0 \ 0 \ 0]^T$</td>
<td>00000 10110 01101 11011</td>
</tr>
<tr>
<td>$10000 + C$</td>
<td>$[1 \ 1 \ 0]^T$</td>
<td>10000 00110 11101 01011</td>
</tr>
<tr>
<td>$01000 + C$</td>
<td>$[1 \ 0 \ 1]^T$</td>
<td>01000 11110 00101 10011</td>
</tr>
<tr>
<td>$00100 + C$</td>
<td>$[1 \ 0 \ 0]^T$</td>
<td>00100 10010 01001 11111</td>
</tr>
<tr>
<td>$00010 + C$</td>
<td>$[0 \ 0 \ 0]^T$</td>
<td>00010 10100 01111 11001</td>
</tr>
<tr>
<td>$00001 + C$</td>
<td>$[0 \ 0 \ 1]^T$</td>
<td>00001 10111 01100 11010</td>
</tr>
<tr>
<td>$00011 + C$</td>
<td>$[0 \ 1 \ 1]^T$</td>
<td>00011 10101 01110 11000</td>
</tr>
<tr>
<td>$10001 + C$</td>
<td>$[1 \ 1 \ 1]^T$</td>
<td>10001 00111 11100 01010</td>
</tr>
</tbody>
</table>

(b) The probability that $c$ is decoded correctly is equal to the probability that the error vector added by the BSC corresponds to one of the coset leaders. Thus, the probability that $c$ is decoded correctly is

$$p_{\text{corr}}(c) = (1 - \epsilon)^5 + 5\epsilon (1 - \epsilon)^4 + 2\epsilon^2 (1 - \epsilon)^3,$$

and

$$p_{\text{err}}(c) = 1 - p_{\text{corr}}(c).$$

(c) An error vector $e$ added by the BSC goes undetected if and only if $e$ is a non-zero codeword (or equivalently, the received vector $y = c + e$ is a codeword distinct from $c$). There are three non-zero codewords in the given code: 10110, 01101, and $10110 + 01101 = 11011$. Thus, the probability that channel errors go undetected is

$$2\epsilon^3 (1 - \epsilon)^2 + \epsilon^4 (1 - \epsilon).$$

(d) The two-bit message vector $u = [u_1 \ u_2]$ is encoded as $c = uG = [u_1 \ u_2 \ p_3 \ p_4 \ p_5]$, and transmitted across the channel. Suppose that $y = c + e$ is received. Then, the first message bit, $u_1$, is incorrectly decoded (under standard array decoding) if and only if the first bit of $e$ is not equal to the first bit of the leader of the coset to which $e$ belongs. Looking through the standard array, we identify all vectors $e$ which have this property:

10110, 11011, 00110, 01011, 11110, 10011, 10010, 11111, 10100, 11001, 10111, 11010, 10101, 11000, 00111, 01010.

The required probability is equal to the probability that the error vector $e$ is one of the above vectors, which is

$$5\epsilon^2 (1 - \epsilon)^3 + 7\epsilon^3 (1 - \epsilon)^2 + 3\epsilon^4 (1 - \epsilon) + \epsilon^5.$$