Problem 1

(a) Hamming bound:

$$|C| \leq \frac{2^n}{\binom{n}{0} + \ldots + \binom{n}{t}}.$$

Here $n = 19$ and $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{5-1}{2} \rfloor = 2$.
So

$$|C| \leq \frac{2^{19}}{\binom{19}{0} + \binom{19}{1} + \binom{19}{2}} = \frac{2^{19}}{191} < \frac{2^{19}}{2^7} = 2^{12}.$$

Therefore we get the bound $k \leq 11$.
(b) Since $n = 2k$, we have that n must be even.
The Gilbert Varshamov bound says there exists an (n, k, d) code if

$$\binom{n-1}{0} + \binom{n-1}{1} + \ldots + \binom{n-1}{d-2} < 2^{n-k}.$$

With $d = 3$ and $k = \frac{1}{2}n$ this gives

$$\binom{n-1}{0} + \binom{n-1}{1} < 2^{n-\frac{1}{2}n}.$$

$$1 + (n-1) < 2^{\frac{1}{2}n}$$

$$n < 2^{\frac{1}{2}n}$$

This is true for all $n \geq 6$, which can be proven for instance by induction.

From the hamming bound we get

$$2^{\frac{1}{2}n} \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1}} = \frac{2^n}{n+1}.$$

So we get $n+1 \leq 2^{\frac{1}{2}n}$. This excludes the possibilities $n = 2$ and $n = 4$.

So the answer is that there exists such a code when n is an even number ≥ 6.

(c) The singleton bount says $d-1 \leq n-k$. Here $k \geq \frac{2}{3}n$ and $d = \frac{1}{2}n$, so

$$\frac{7}{6}n - 1 = \frac{1}{2}n + \frac{2}{3}n - 1 \leq \frac{1}{2}n + k - 1 = d - 1 - k \leq n.$$

If $n \geq 6$, then this gives $1 < \frac{1}{6}n \leq 1$, which is not possible, so there does not exist such a code.

Problem 2

The received word is $w = 100\ 101\ 011\ 000\ 111\ 000\ 100\ 00$. We add the bit 0 so we get a word of length 24 with odd weight. $w' = w0 = 100\ 101\ 011\ 000\ 111\ 000\ 100\ 000$. We decode this word using the decoding algorithm for the extended Golay code.

First we calculate the syndrome $s = w'H = (100\ 101\ 011\ 000)I + (111\ 000\ 100\ 000)B = 100\ 101\ 011\ 000 + 000\ 000\ 110\ 110 = 100\ 101\ 101\ 110$.

We get $\operatorname{wt} s > 3$, so we continue the algorithm.

Next we check whether $\operatorname{wt}(s + b_i) \leq 2$ for some row b_i of B. After some computations we find $s + b_7 = 100\ 000\ 000\ 001$, so $\operatorname{wt}(s + b_7) = 2$. Therfore the most likely error pattern is $u = 100\ 000\ 000\ 001\ 000\ 000\ 100\ 000$ and the codeword is $v = w' + u = 000\ 101\ 011\ 001\ 111\ 000\ 000\ 000$. The most likely sent word of length 23 is

$$000\ 101\ 011\ 001\ 111\ 000\ 000\ 00.$$

Problem 3

We have $d = \delta = 5$, so C can correct $\lfloor \frac{5-1}{2} \rfloor = 2$ errors.

The received word is $w = \beta^3\beta^{11}\beta^5 00\ 10000\ 00000$. The corresponding polynomial is $w(x) = \beta^3 + \beta^{11}x + \beta^5 x^2 + x^5$. To decode the word we use algorithm 6.3.2.

Step 1.

$$\begin{aligned}
s_1 = w(\beta) &= \beta^3 + \beta^{12} + \beta^7 + \beta^5 = 0001 + 1111 + 1101 + 0110 &&= 0101 = \beta^9 \\
s_2 = w(\beta^2) &= \beta^3 + \beta^{13} + \beta^9 + \beta^{10} = 0001 + 1011 + 0101 + 1110 &&= 0001 = \beta^3 \\
s_3 = w(\beta^3) &= \beta^3 + \beta^{14} + \beta^{11} + 1 = 0001 + 1001 + 0111 + 1000 &&= 0111 = \beta^{11} \\
s_4 = w(\beta^4) &= \beta^3 + 1 + \beta^{13} + \beta^5 = 0001 + 1000 + 1011 + 0110 &&= 0100 = \beta
\end{aligned}$$

Step 2.

$$M' = \begin{bmatrix} s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{bmatrix} = \begin{bmatrix} \beta^9 & \beta^3 & \beta^{11} \\ \beta^3 & \beta^{11} & \beta \end{bmatrix} \sim \begin{bmatrix} 1 & \beta^9 & \beta^2 \\ 1 & \beta^8 & \beta^{13} \end{bmatrix}$$

The rank of this matrix is two, so $e = \operatorname{Rank} M' = 2$.

Step 3. We continue with the row operations.

$$\sim \begin{bmatrix} 1 & \beta^9 & \beta^2 \\ 0 & \beta^{12} & \beta^{14} \end{bmatrix} \sim \begin{bmatrix} 1 & \beta^9 & \beta^2 \\ 0 & 1 & \beta^2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \beta^9 \\ 0 & 1 & \beta^2 \end{bmatrix}$$

So $\sigma_0 = \beta^9$ and $\sigma_1 = \beta^2$.

Step 4. The error locator polynomial is $\sigma_A = \sigma_0 + \sigma_1 x + x^2 = \beta^9 + \beta^2 x + x^2$.

We try to solve $\sigma_A = 0$.

$$\beta^9 + \beta^2 x + x^2 = 0$$

Let $x = \beta^2 y$.

$$\begin{aligned} \beta^9 + \beta^4 y + \beta^4 y^2 &= 0 \\ \beta^5 + y + y^2 &= 0 \\ y(y+1) &= \beta^5 \end{aligned}$$

Solving this, for instance looking up in the table, we get solutions $y = \beta$ or $y = \beta^4$. As values for x we get $x = \beta^3$ or $x = \beta^6$.

So we let $a_1 = \beta^3$ and $a_2 = \beta^6$.

Step 5. We need to solve the linear system

$$\begin{bmatrix} a_1 & a_2 \\ {a_1}^2 & {a_2}^2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$

$$\begin{bmatrix} \beta^3 & \beta^6 \\ \beta^6 & \beta^{12} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} \beta^9 \\ \beta^3 \end{bmatrix}$$

Row operations give

$$\begin{bmatrix} \beta^3 & \beta^6 & \beta^9 \\ \beta^6 & \beta^{12} & \beta^3 \end{bmatrix} \sim \begin{bmatrix} 1 & \beta^3 & \beta^6 \\ 1 & \beta^6 & \beta^{12} \end{bmatrix} \sim \begin{bmatrix} 1 & \beta^3 & \beta^6 \\ 0 & \beta^2 & \beta^4 \end{bmatrix} \sim \begin{bmatrix} 1 & \beta^3 & \beta^6 \\ 0 & 1 & \beta^2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & \beta^9 \\ 0 & 1 & \beta^{12} \end{bmatrix}$$

Therefore we get $b_1 = \beta^9$ and $b_2 = \beta^2$. The most likely error is $000\beta^9 0\ 0\beta^2 000\ 00000$. The most likely sent word is $c = w + e = \beta^3\beta^{11}\beta^5\beta^9 0\ 1\beta^2 000\ 00000$.

Step 6. Checking the solution (not necessary, but might be a good idea).

We have $(\beta^3 + \beta^{11}x + \beta^5 x^2 + \beta^9 x^3 + x^5 + \beta^2 x^6) \colon g(x) = \beta^2 x^2 + \beta^8$, so c is a codeword.

Problem 4

We can use Algorithm 7.1.11 to find such a pattern.

The syndrome polynomial is

$$s(x) = w(x) \operatorname{\underline{mod}} g(x) = 1 + x + x^5$$

We get

$$\begin{aligned}
s_0(x) &= 1 + x + x^5 \\
s_1(x) &= x(1 + x + x^5) \operatorname{\underline{mod}} g(x) = 1 + x^3 \\
s_2(x) &= x^2(1 + x + x^5) \operatorname{\underline{mod}} g(x) = x + x^4 \\
s_3(x) &= x^3(1 + x + x^5) \operatorname{\underline{mod}} g(x) = x^2 + x^5 \\
s_4(x) &= x^4(1 + x + x^5) \operatorname{\underline{mod}} g(x) = 1 + x + x^2
\end{aligned}$$

Here we get $\deg s_4 < l = 3$. So the most likely cyclic burst error pattern is

$$e(x) = x^{15-4} s_4(x) \operatorname{\underline{mod}}(1+x^{15}) = x^{11}(1+x+x^2) \operatorname{\underline{mod}}(1+x^{15}) = x^{11}+x^{12}+x^{13}.$$

The corresponding word $e = 00000\ 00000\ 01110$ has cyclic burst length 3.

Problem 5

(a) If u and v are two words then

$$\operatorname{wt}(u + w) = \operatorname{wt} u + \operatorname{wt} v - 2 \operatorname{wt}(u \cap v),$$

where $u \cap v$ is the word having 1s exactly in those positions where both u and v have 1s.

If $u, v \in C'$, then $u, v \in C$ and both $\operatorname{wt} u$ and $\operatorname{wt} v$ are even. From the formula above we get that $\operatorname{wt}(u + v)$ is even. Since C is linear we have $u + v \in C$, so $u + v \in C'$.

Suppose C is cyclic and suppose $u \in C'$. Then $u \in C$ and also the cyclic shift $\pi(u) \in C$. Since $\operatorname{wt}(\pi(u)) = \operatorname{wt} u$ is even, we have $\pi(u)C'$. Since C' is closed under cyclic shifts, we have that C' is cyclic.

(b) One way to argue is as follows.

If all words in C have even weight, then $C = C'$ and therefore $\dim C = \dim C'$.

Suppose there is a word $u \in C$ with odd weight. Then there is a function $\phi\colon C \to C$ defined by $\phi(v) = v + u$. This function is $1-1$ and onto. Furthermore $\phi(\phi(v)) = v$. From the weight formula in (a) we get that $\operatorname{wt}(\phi(v))$ is even if $\operatorname{wt}(v)$ is odd and that $\operatorname{wt}(\phi(v))$ is odd if $\operatorname{wt}(v)$ is even. In this way we get a $1-1$ correspondence between words with odd weight and words with even weight. So there are equally many words of even weight and of odd weight. This gives $|C'| = \frac{1}{2}|C|$, so $\dim C' + 1 = \dim C$.

(c) Since there are words in C with odd weight, we know from part (b) that $\dim C' = \dim C - 1 = 3$. So we have to find 3 linearly independent words in C'. ROW 1 = 1000111 has even weight Another word in C with even weight is ROW 2 + ROW 3 = 0110011 We have

to find a third word in C with even weight that is linearly independent to $\{1000111, 0110011\}$. One such word is $\mathrm{ROW}\,2 + \mathrm{ROW}\,4 = 0101101$. So one possible generator matrix for C' is

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

(d) The polynomial corresponding to 010001100 is $x + x^5 + x^6$. The generator polynomial of C is $\gcd(1 + x^9, x + x^5 + x^6) = x^2 + x + 1$. This means that $\dim C = 9 - 2 = 7$. Since C contains words with odd weight, we have $\dim C' = \dim C - 1 = 6$.

If $g'(x)$ denotes the generator polynomial of C', then $\deg g'(x) = 9 - 6 = 3$

(Alternative 1:) We must have $g'(x) \mid 1 + x^9$. From the factorisation of $1 + x^9$ we see that the only factor of degree 3 is $1 + x^3$.

(Alternative 2:) Since $C' \subseteq C$, we must have $g'(x) = h(x)g(x)$ for some polynomial $h(x)$. Since $\deg g'(x) = \deg g(x) + 1$, we must have $\deg h(x) = 1$. If $h(x) = x$, then $g'(x) = x + x^2 + x^3$. Then C' contains words with odd weight, which is a contradiction. Therefore $h(x) = x+1$ and $g'(x) = (1 + x)(1 + x + x^2) = 1 + x^3$.