1. Let $\mathcal{C}$ be the linear code with basis 10001010, 01001001, 00100110, 00010101. Find a check matrix for this code, and determine the parameters (length, message length, distance) of this code.

2. Let $\mathcal{C}$ be the Hamming code of length 7 (with the parameter $r = 3$). Find a basis of this code.

3. For positive integers $d \leq n$, let $\mathcal{C}$ be the code of length n constructed as follows: Let $\mathcal{C}_0$ contain only the zero vector in $\mathbb{Z}_2^n$. For $i = 1, 2, \ldots$, if there exists a vector $w_i \in \mathbb{Z}_2^n$ whose Hamming distance from all codewords of $\mathcal{C}_{i-1}$ is at least d, then let

$$\mathcal{C}_i = \mathcal{C}_{i-1} \cup \{w + w_i : w \in \mathcal{C}_{i-1}\}.$$

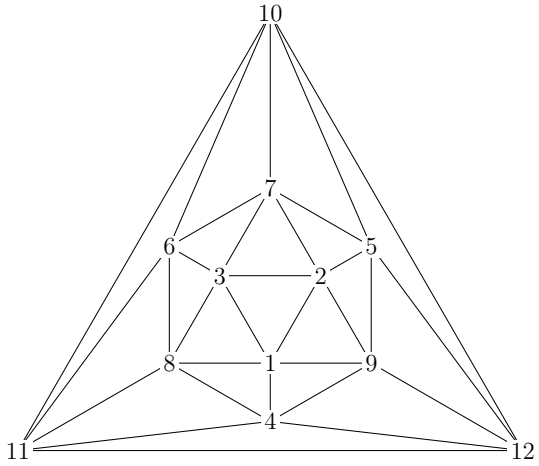
   Otherwise, we let $\mathcal{C} = \mathcal{C}_{i-1}$ and the construction is finished.

   - Show that $\mathcal{C}$ is a linear code.
   - Show the distance of $\mathcal{C}$ is at least d.
   - Show that the message length of $\mathcal{C}$ is at least $n - \log_2 \binom{n}{\leq d}$.

4. Let A be the check matrix of a linear code $\mathcal{C}$ of length n and distance d.

   - Let $w_1, w_2 \in \mathcal{C}$ be two codewords and let w_1' and w_2' be the words obtained from them by flipping the same bits (i.e., when computing in $\mathbb{Z}_2^n$, we have $w_1' - w_1 = w_2' - w_2$). Show that $A(w_1')^T = A(w_2')^T$. How does this expression depend on which bits are flipped?
   - Let $e_1, e_2 \in \mathbb{Z}_2^n$ be distinct vectors such that $\omega(e_1) + \omega(e_2) < d$. Show that $Ae_1^T \neq Ae_2^T$.
   - Design an algorithm that for $t < d/2$, given a word w' obtained from a codeword $w \in \mathcal{C}$ by flipping at most t bits, correctly determines the original word w. The algorithm is allowed to use a precomputed table containing at most $O(n^t)$ entries.

5. The *icosahedron* is the following graph G:



Let A be the *non-adjacency* matrix of this graph, i.e., $A_{i,j} = 0$ if the vertices i and j are adjacent and $A_{i,j} = 1$ otherwise (and in particular, $A_{i,i} = 1$ for every i). The *extended Golay code* $\mathcal{G}$ is the linear code (of length 24) whose check matrix is $C = (I_{12}|A)$, i.e., the concatenation of the 12×12 identity matrix I_{12} with A.

- Show that $CC^T = 0$, and that this implies that the rows of C also form a basis of this linear code $\mathcal{G}$.
- Show that this implies that $w_1 w_2^T = 0$ for all codewords $w_1, w_2 \in \mathcal{G}$, and thus the number of bits which are 1 both in w_1 and w_2 is divisible by 2.
- Observe that the number of 1's in each row of C is 8, and use this and the previous point to show that $\omega(w)$ is divisible by 4 for every $w \in \mathcal{G}$. What does this tell you about the distance of $\mathcal{G}$?
- The distance of the extended Golay code $\mathcal{G}$ is actually 8. What would you need to prove about the icosahedron graph to show that this is indeed true?

6. The *Golay code* is the truncation of the extended Golay code. Determine the parameters (length, message length, distance) of the Golay code and show that this code is perfect.